

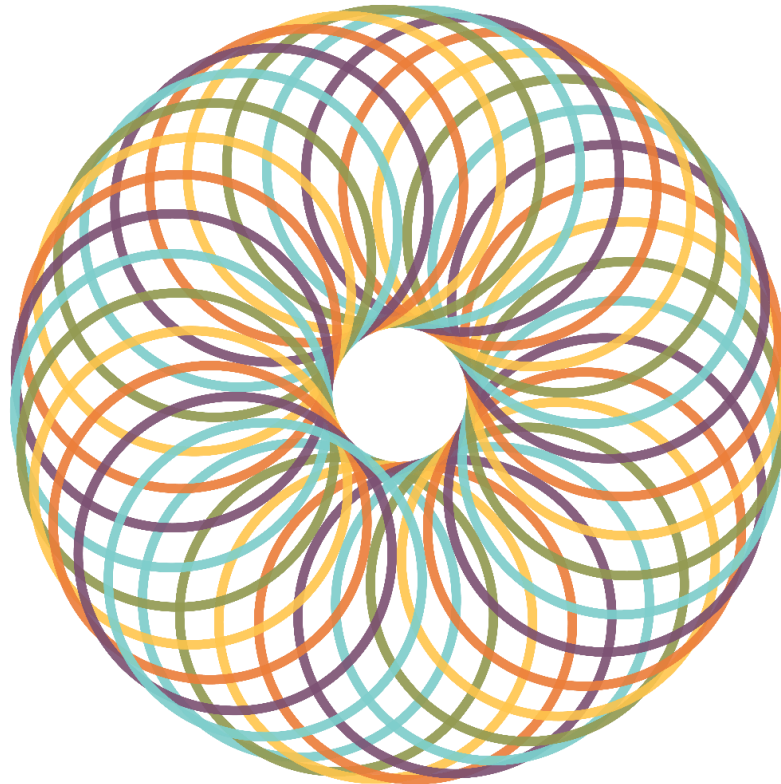
NOTICE

You and your company have obtained access to this report dated 4 July 2024, on certain Application Development, Maintenance, Production Support and the related General IT Controls services performed by Deloitte Haskins & Sells LLP (“DHSLLP”) as agreed with ZHO CORPORATION PVT. LTD. (herein referred to as “Client”) (“Report”), by accepting the terms of the Click Through Access Agreement that was attached to this Report and acknowledging that your company (“Recipient”) is a prospect customer of the Client/ or as per contractual agreement with the client eligible to receive this report.

The terms of the Access Agreement include, among other things, an agreement by you and your company not to further disclose, distribute, quote, or reference this Report and an agreement to release and indemnify DHSLLP for certain claims. By reading this Report, you agree that you and your company have agreed to the terms of such Access Agreement. If you are not the Recipient and you have not accessed this Report by agreeing to the terms of such Access Agreement then you are prohibited from having access to this Report and you must permanently delete it from your and your company’s computer and network systems.

This Report is intended only to be used by the Client solely for its internal purposes. DHSLLP and its subcontractors and their respective personnel shall have no liability, duties, responsibilities or other obligations to any one including Recipient who may obtain this Report.

DHSLLP, its subcontractors and their respective personnel do not have any obligation to advise or consult with any entity regarding their use of this Report. Any use of this Report by a party other than Client is at such party’s sole and exclusive risk. This Report is not to be further disclosed, distributed, quoted, or referenced to any third party or included or incorporated by reference in any other document.



SOC 2+ HIPAA Type 2 Examination

Zoho Corporation Private Limited ('Zoho')

Report on the description of system of Zoho related to Application Development, Production Support and the related IT General Controls for services provided to customers relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy Trust Services Criteria with mapping to the requirements of Security and Privacy rules of Health Insurance Portability and Accountability Act (HIPAA) and the suitability of the design and operating effectiveness of the controls stated in the description throughout the period December 01, 2022 through November 30, 2023

This report is intended solely for the information and use of Zoho Corporation Private Limited, user entities and other specified parties and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report.

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITOR’S REPORT	1
SECTION 2: MANAGEMENT OF ZOHO’S ASSERTION	7
SECTION 3: MANAGEMENT OF ZOHO’S DESCRIPTION OF ITS SYSTEM	10
SECTION 4: MANAGEMENT OF ZOHO’S DESCRIPTION OF ITS RELEVANT CRITERIA AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS	189

SECTION - 1

Independent Service Auditor's Report

Section 1: Independent Service Auditor's Report

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

To the Management of Zoho Corporation Private Limited

Scope

We have examined the description of the system of Management of Zoho Corporation Private Limited (the "Service Organization" or "Company" or "Zoho") related to Application Development, Production Support and the related Information Technology General Controls for the services provided to customers ("User entities" or "User Organizations" or "Clients"), from Zoho Facilities located at Chennai, Tenkasi and Renigunta in India included in Section 3 "Management of Zoho's Description of Its System" throughout the period December 01, 2022 to November 30, 2023 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report in AICPA Description Criteria and the security and privacy requirements set forth in the Health Insurance Portability and Accountability Act ("HIPAA") ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period December 01, 2022 to November 30, 2023, to provide reasonable assurance that Zoho's service commitments and system requirements would be achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust service criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy in AICPA Trust Services Criteria and the security and privacy requirements set forth in the HIPAA (collectively the "applicable criteria").

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited, Digital Realty Trust Inc., Equinix Inc. B.V., CtrlS Datacenters Limited, Equinix Asia Pacific Pte. Ltd for Datacenter Co-Location Services ("Subservice organizations"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable criteria. The Description presents Zoho's controls, the applicable criteria, and the types of complementary subservice organization controls assumed in the design of Zoho's controls. The Description does not disclose the actual controls at the subservice organizations Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable criteria. The Description presents Zoho's controls, the applicable criteria, and the complementary user entity controls assumed in the design of Zoho's controls. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Management of Zoho is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Zoho service commitments and system requirements would be achieved. Management of Zoho has provided the accompanying assertion in Section 2 titled "Management of Zoho's Assertion" (the "Assertion") about the Description and the suitability of design and operating effectiveness of controls stated therein. Management of Zoho is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that Zoho's service commitments and system requirements would be achieved based on the applicable criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based the applicable criteria.

- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Zoho achieved its service commitments and system requirements based on the applicable criteria.
- Evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and, therefore may not include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4, "Management of Zoho's Description of Its Relevant Criteria and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Emphasis of a Matter:

The service organization identified a bug during the change management process for 1 of the Zoho Products - Zoho Cliq and reported an incident on October 30th, 2023, where wrong meta data of chat ID was getting updated to different chat ID. However, as confirmed by the service organization management, the security incident did not impact the in scope products but impacted only Zoho Cliq, specifically for some customers in Europe, India, China, Australia and Japan Data Centers, which is not in scope of this report. The scope of this report is limited to controls related to in-scope products in Section 3 and hence we did not perform any additional procedures as regards the identified security incident.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Therefore, the HIPAA Security and Privacy requirements 164.404(a)(1), 164.406(1)(a), 164.408(a), 164.504, 164.506, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, 164.530, 164.532 were not applicable for Zoho. The reasons for non-applicability have been included in Section 3 of this report.

Opinion

In our opinion, in all material respects,

- a. The Description presents Zoho's system related to Application Development, Production Support and the related Information Technology General Controls that was designed and implemented throughout the period December 01, 2022 to November 30, 2023 in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed throughout the period December 01, 2022 to November 30, 2023 to provide reasonable assurance that Zoho's service commitments and systems requirements would be achieved based on the applicable criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls throughout that period.
- c. The controls stated in the Description operated effectively throughout the period December 01, 2022 to November 30, 2023, to provide reasonable assurance that Zoho's service commitments and system requirements would be achieved based on the applicable criteria, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Zoho, user entities of Zoho's system related to Application Development, Production Support and the Information Technology General Controls during some or all of the period December 01, 2022 to November 30, 2023, business partners of Zoho subject to risks arising from interactions with Zoho's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following :

- The nature of the service provided by Zoho.
- How Zoho's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at Zoho to achieve Zoho's commitments and system requirements.
- User entity responsibilities and how they may affect the user entities' ability to effectively use Zoho's services.

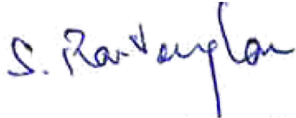
- The applicable criteria.
- The risks that may threaten the achievement of Zoho's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Deloitte Haskins & Sells LLP

Chartered Accountants

Firm Registration No: 117366W/W- 100018



S. Ravi Veeraraghavan

Partner

M. No. 29935

July 04, 2024

SECTION - 2

MANAGEMENT OF ZOHO'S

ASSERTION



Section 2: MANAGEMENT OF ZOHO'S ASSERTION

MANAGEMENT OF ZOHO CORPORATION PRIVATE LIMITED'S ASSERTION

For the period from December 01, 2022 through November 30, 2023

The signed Management assertion has been provided by Zoho Corporation Private Limited via letter dated July 04, 2024. The extract of the letter is as under:

We have prepared the description of the system of Management of Zoho Corporation Private Limited (the "Service Organization" or "Company" or "Zoho") related to Application Development, Production Support and the related Information Technology General Controls for the services provided to customers ("User entities" or "User Organizations" or "Clients"), from Zoho Facilities located at Chennai, Tenkasi and Renigunta in India included in Section 3 "Management of Zoho's Description of Its System" throughout the period December 01, 2022 to November 30, 2023 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report in AICPA Description Criteria and the security and privacy requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) ("description criteria"). The Description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Zoho's system, particularly information about system controls that Zoho has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy in AICPA Trust Services Criteria and the security and privacy requirements set forth in the HIPAA (collectively the "applicable criteria").

Zoho uses Sabey Data Center Properties LLC, Databank Holdings Limited, Digital Realty Trust Inc., Equinix Inc. B.V., CtrlS Datacenters Limited, Equinix Asia Pacific Pte. Ltd for Datacenter Co-location Services ("Subservice organizations"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable criteria. The Description presents Zoho's controls, the applicable criteria, and the types of complementary subservice organization controls assumed in the design of Zoho's controls. The Description does not disclose the actual controls at the subservice organization. The Description does not extend to controls of the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zoho, to achieve Zoho's service commitments and system requirements based on the applicable criteria. The Description presents



Zoho's controls, the applicable criteria, and the complementary user entity controls assumed in the design of Zoho's controls. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- a. The Description presents Zoho's system that was designed and implemented throughout the period December 01, 2022 to November 30, 2023 in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed throughout the period December 01, 2022 to November 30, 2023, to provide reasonable assurance that Zoho's service commitments and system requirements would be achieved based on the applicable criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls throughout that period.
- c. The controls stated in the Description operated effectively throughout the period December 01, 2022 to November 30, 2023 to provide reasonable assurance that Zoho's service commitments and system requirements were achieved based on the applicable criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of Zoho's controls operated effectively throughout that period.

Zoho identified a bug during the change management process for 1 of the Zoho Products - Zoho Cliq and reported an incident on October 30th, 2023, where wrong meta data of chat ID was getting updated to different chat ID. However, as confirmed by Zoho, the security incident did not impact the in scope products but impacted only Zoho Cliq, specifically for some customers in Europe, India, China, Australia and Japan Data Centers, which is not in scope of this report. The scope of this report is limited to controls related to in-scope products in Section 3 and hence we did not perform any additional procedures as regards the identified security incident.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Therefore, the HIPAA Security and Privacy requirements 164.404(a)(1), 164.406(1)(a), 164.408(a), 164.504, 164.506, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, 164.530, 164.532 were not applicable for Zoho. The reasons for non-applicability have been included in Section 3 of this report.

For Zoho Corporation Private Limited

Sd/-

Name: N Jai Anand

Title: Chief Financial Officer

Date: July 04, 2024

SECTION - 3

MANAGEMENT OF ZOHO'S

DESCRIPTION OF ITS SYSTEM

Section 3: MANAGEMENT OF ZOHOO'S DESCRIPTION OF ITS SYSTEM

3.1 Zoho Business Overview

Incorporated in 1996, Zoho Corporation provides SaaS solutions, IoT platform and IT management software (on premise) to organizations of all sizes across the globe. Zoho comes with a suite of software that brings together collaboration, productivity, and communications tools and integrates them into other business processes. From network, and IT infrastructure management applications, software maintenance and support services for enterprise IT, networking, and telecom clients to enterprise IT management software for network performance management, IT service desk and desktop management, datacenter and server management, and log analysis and security management.

Zoho's primary facilities are based from India - Chennai, Tenkasi and Renigunta. Zoho also has a global presence in Netherlands (Utretch), Singapore (Cecil Street), China, Japan, Mexico and Australia (Varsity Lakes). The sales, marketing and customer support activities are specifically carried out in secondary facilities in Netherlands, Australia, China, Japan and Singapore.

Zoho hosts the data in datacenters across the globe. When an organization (customer who wants to subscribe to Zoho) signs up with Zoho, the default datacenter location is chosen by Zoho based on the user/organization's IP address. The customer does not have the option to choose the hosting location. In order to make it easier for the organization, that field is selected by default based on the organizations IP address. Based on the country chosen there, the corresponding datacenter is chosen for the organization's account. Listed below are the locations Zoho services and their associated datacenters:

- United States Of America – Quincy, Dallas (www.zoho.com)
- Europe – Amsterdam, Dublin (www.zoho.eu)
- India – Mumbai, Chennai (www.zoho.in)
- Australia – Sydney, Melbourne (www.zoho.com.au)
- Japan – Tokyo (www.zoho.jp)
- China – Shanghai (www.zoho.com.cn)
- Canada – Toronto (www.zohocloud.ca)
- Saudi Arabia – Riyadh (www.zoho.sa)

Zoho's range of products are internally classified under the following verticals:

- **Zoho** - offers a comprehensive suite of online business, productivity & collaboration applications to assist user entities manage their business processes and information.
- **ManageEngine** - offers enterprise IT management software for service management, operations management, Active Directory, and security needs.

- **Site24x7** - an all-in-one monitoring tool for DevOps and IT Operations from the cloud. Monitor the performance of websites, servers, network, cloud resources, and APM application on-the-go.
- **Qntrl** - A workflow orchestration software that helps you gain visibility and control over your business processes by automating them.
- **TrainerCentral** - A comprehensive platform to help you build engaging online courses, nurture a learning community and turn your expertise into a successful training business.
- **Zakya** - Running a retail business is easier with Zakya. We help you sell better, manage your entire business, and join the digital revolution.
- **MedicalMine** - Charmhealth Suite of Products are developed for MedicalMine Inc. to be used by healthcare professionals in the Ambulatory Clinic Care. The Charmhealth helps to providers to manage Electronic Health Record, Patient Health Record, Medical Billing, etc.

System Overview

Zoho operates in a well-defined system to provide services to its clients. This system consists of multiple components such as policies and procedures, governance structure, support functions, and application systems. The policies and procedures provide guidance to the users regarding the process to be followed for providing the services and assistance in the consistent implementation of the same. The governance structure establishes a structure for operating the system and assists in demonstrating Management's commitment towards the same. The defined processes for information systems including Software development, Quality and Security testing, Incident Management, Change Management, and Service Delivery are implemented by Zoho to support the processes followed for providing services to its clients.

Zoho has established an internal controls framework that reflects:

- The overall control environment within the organization and its various processes
- The Risk Assessment procedure
- Control activities that help in meeting the overall applicable criteria.
- Information and communication and
- Monitoring components of internal control

The components mentioned above are described in detail in the succeeding sections. There is synergy and linkage amongst these components, forming an integrated system that responds dynamically to changing conditions. The internal control system is intertwined with Zoho's operating activities and exists for fundamental business reasons.

Overview of Services

Zoho products are developed, maintained and supported by the following teams:

a. Product Teams

Product teams perform the following activities:

- Development, design, research and analysis of new features and enhancements
- Application Patch management
- Issue fixing
- Quality and security testing before deploying in production environment
- Release management (where applicable)
- Overall management of product (including assessments, documentation, training programs for associates etc.)

b. Customer Support Team

Zoho Customer Support has several tiers of Customer support depending upon the support plan the customer is entitled to Zoho does provide both complementary and paid customer support. Clients report clarifications or bugs via phone/chat/email to the Client Support team. The team coordinates with Product teams to resolve reported issues.

c. Zorro and NOC team

The Zorro team handles the management of components such as servers, databases and network devices within the data center hosting Cloud services.

The Network Operations Center (NOC) team monitors Local Area Networks (LAN) / Wide Area Networks (WAN) and network devices for faults, failures, errors, usage and performance from a centralised location based out of Zoho's Corporate Office in Estancia, Chennai. The scope of work for NOC and Zorro team includes- analysing problems in network devices, troubleshooting issues, reporting incidents, communicating with site technicians and tracking problems to resolution.

d. Sysadmin team

The Sysadmin team is responsible for management of Zoho's internal Corporate Infrastructure components such as servers, databases and network devices. Corporate Infrastructure supports non-production instances of Zoho products used for development and testing purposes, and other internal tools used by teams to support the Zoho products.

e. Compliance team

The Compliance team is responsible for the overall Information Security Governance and compliance within the organization and also ensuring the service commitments and system requirements as per the Master Service agreement and Terms of Service or any other agreements between Zoho and the user entities.

f. Security and privacy team

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They engineer and maintain our defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

g. Configuration Management Team

Zoho has a centralized Configuration Management team. They are responsible for maintaining the source code and enforce code check standards for the builds which needs to be deployed.

h. Service Delivery team

The Service Delivery team is responsible for the deployment of builds into local, pre-production and production environments of Zoho products. The service delivery team takes care of SD tool, which in turn takes care of automation related activities related to deployment of builds into local, pre-production and production environments of Zoho Cloud products.

Zoho Products

Zoho provides multiple products across its different divisions to customers. The below products which are provided by Zoho form part of the description criteria in relation to this SOC2+HIPAA examination:

Table 1: Inscope Products

Product Name	Product Category	Product Description	Product Scale	Division
Zoho CRM	Sales and Marketing	It is a tool which acts as a single repository to bring your sales, marketing, customer support activities together, and streamlines your process, policy, and people in one platform.	Large	Zoho Cloud Services
Zoho SalesIQ	Sales and Marketing	Zoho SalesIQ offers your marketing, sales, and support teams the digital customer engagement tools to communicate with every site visitor at every stage of the customer lifecycle.	Large	Zoho Cloud Services
Zoho Forms	Sales and Marketing	Build forms for lead generation and customer engagement	Medium	Zoho Cloud Services
Zoho Bigin	Sales and Marketing	Pipeline management solution for small customer-facing teams	Medium	Zoho Cloud Services
Zoho Bookings	Sales and Marketing	Zoho Bookings syncs your calendars while letting customers self-schedule and pay for appointments.	Small	Zoho Cloud Services
Zoho Campaigns	Sales and Marketing	Create responsive designs, customize messages, deliver emails to inboxes, trigger automated workflows, and connect with new customers—Zoho Campaigns provides the toolkit to meet your email marketing needs.	Large	Zoho Cloud Services
Zoho Backstage	Marketing	Zoho Backstage is an event management software that empowers event organizers to plan and run conferences, meetups, and product launches with greater efficiency and impact.	Small	Zoho Cloud Services
Zoho Survey	Marketing	Create your survey in minutes. Reach the audience on every device. View results graphically and in real-time.	Medium	Zoho Cloud Services

Product Name	Product Category	Product Description	Product Scale	Division
Zoho Commerce	Marketing	Zoho Commerce contains all the tools you need to build a website, accept orders, track inventory, process payments, manage shipping, market your brand, and analyze your data.	Small	Zoho Cloud Services
Zoho Meeting and Webinar	Marketing	Zoho Meeting and Webinar is a secure online meeting platform and webinar solution that helps people find new ways to collaborate and work remotely with efficacy.	Medium	Zoho Cloud Services
Zoho Sites	Marketing	Quickly build professional websites.	Medium	Zoho Cloud Services
Zoho Pagesense	Marketing	Optimize your web pages for engagement and conversion.	Medium	Zoho Cloud Services
Zoho Marketing Automation	Marketing	Zoho Marketing Automation is an all-in-one marketing automation software that helps you successfully manage your marketing activities across multiple channels.	Small	Zoho Cloud Services
Zoho Assist	Help Desk	Troubleshoot customer issues remotely for quick resolutions.	Small	Zoho Cloud Services
Zoho Desk	Help Desk	Support customers across multiple channels with one tool.	Large	Zoho Cloud Services
Zoho Lens	Help Desk	Train, troubleshoot, and collaborate with AR tech turning mobile cameras in to remote eyes.	Small	Zoho Cloud Services
Zoho Books	Finance	Zoho Books is online accounting software that manages your finances, keeps you GST compliant, automates business workflows, and helps you work collectively across departments.	Large	Zoho Cloud Services
Zoho Invoice	Finance	Zoho Invoice is online invoicing software that helps you craft professional invoices, send payment reminders, keep track of expenses, log your work hours, and get paid faster.	Medium	Zoho Cloud Services
Zoho Expense	Finance	Zoho Expense will turn receipts into expense reports for quick approval.	Medium	Zoho Cloud Services
Zoho Inventory	Finance	Manage orders. Track inventory. Handle GST billing. Oversee	Medium	Zoho Cloud Services

Product Name	Product Category	Product Description	Product Scale	Division
		warehouses. One inventory management software to run all your inventory operations.		
Zoho Billing	Finance	Handle your customer subscription billing life cycle from end to end. Automate recurring billing, manage subscriptions, send professional GST-compliant invoices, and get paid on time, every time.	Medium	Zoho Cloud Services
Zoho Checkout	Finance	Build a custom, branded payment page in a matter of minutes and start accepting payments right away.	Medium	Zoho Cloud Services
Zoho People	People and Culture	It is a tool that acts as an HR management system for managing the employee, hiring, onboarding and attendance management to time tracking and appraisals.	Large	Zoho Cloud Services
Zoho Recruit	People and Culture	Zoho Recruit is a cloud-based applicant tracking system that's built to provide diverse, end-to-end hiring solutions for staffing agencies, corporate HRs and temporary workforce.	Medium	Zoho Cloud Services
Zoho Connect	People and Culture	Zoho Connect is a private social network for team discussion and sharing resources.	Small	Zoho Cloud Services
Zoho Creator	Customer Solutions	Zoho Creator is a low-code platform that turns the unique business processes into custom applications.	Large	Zoho Cloud Services
Zoho Vault	IT	Zoho Vault is a secure password manager that safely manages your passwords and autofills them across websites and applications.	Medium	Zoho Cloud Services
Zoho Catalyst	IT	Catalyst by Zoho is a highly scalable serverless platform that lets developers build and deploy world-class solutions without managing servers.	Medium	Zoho Cloud Services
Zoho Contracts	IT	Contracts is a comprehensive contract life cycle management software.	Small	Zoho Cloud Services

Product Name	Product Category	Product Description	Product Scale	Division
Zoho Flow	IT	Visually build integration between apps and it automate business workflows by connecting your apps with Zoho Flow.	Small	Zoho Cloud Services
Zoho Office Integrator	Customer Solution	Zoho Office Integrator is a built-in document editor for web apps	Small	Zoho Cloud Services
Zoho Analytics	BI & Analytics	Get insights about every aspect of your business.	Medium	Zoho Cloud Services
Zoho DataPrep	BI & Analytics	DataPrep is an augmented self-service data preparation and pipeline service where we can Connect, explore, transform, and enrich data for analytics, machine learning, migration, and data warehousing.	Medium	Zoho Cloud Services
Zoho Notebook	Email & Office	Make note of what matters in this beautiful note-taking application.	Small	Zoho Cloud Services
Zepto Mail	Email & Office	ZeptoMail is an email service that is built exclusively to send transactional emails from applications or websites such as welcome emails, password reset emails, invoice emails etc.	Medium	Zoho Cloud Services
Zoho Writer	Email & Office	Write and collaborate in a clean interface.	Large	Zoho Cloud Services
Zoho Calendar	Email & Office	Zoho Calendar is an online business calendar that makes scheduling easy for you. You can use it to stay on top of your schedule and share calendars with your team to keep everyone on the same page.	Small	Zoho Cloud Services
Zoho Mail	Email & Office	Host your business email on a secure, encrypted, privacy-guaranteed, and ad-free email service.	Large	Zoho Cloud Services
Zoho Show	Email & Office	Design professional slides, collaborate with your team, and deliver visually engaging presentations.	Medium	Zoho Cloud Services
Zoho Learn	Email & Office	Zoho Learn is a complete knowledge and learning management platform that helps you capture and retain your team's knowledge, build training	Small	Zoho Cloud Services

Product Name	Product Category	Product Description	Product Scale	Division
		programs, and measure the results of your training.		
Zoho Sheet	Email & Office	Create, edit and share spreadsheets online, using Zoho Sheet.	Large	Zoho Cloud Services
Zoho Sprints	Project Management	It is an Agile project management application that will effectively manage and track agile projects.	Small	Zoho Cloud Services
Zoho Projects and BugTracker	Project Management	Zoho Projects, our cloud-based project management software, helps you plan your projects, track work efficiently, and collaborate with your team.	Large	Zoho Cloud Services
Zoho Workdrive	Collaboration	It is a File Management application that will store, organize and manage team files securely.	Large	Zoho Cloud Services
Zoho Voice	Collaboration	Zoho Voice is a cloud-based telephony software for business.	Large	Zoho Cloud Services
Zoho Sign	Collaboration	Sign documents digitally and request signatures.	Medium	Zoho Cloud Services
ZohoOne Engineering	Email & Office	Zoho One is a suite of business apps that helps you manage your whole business in one place. Sign in to access your apps, customize your tabs, and manage your organization with the Admin Panel.	Large	Zoho Cloud Service
Zoho TeamInBox	Email & Office	Create common inboxes for your teams and give them the comfort of working in a transparent workspace.	Small	Zoho Cloud Services
Zoho LandingPage	Marketing	Zoho LandingPage is a landing page software that helps you build high-converting pages with drag-and-drop editor, responsive templates, and in-app integrations. You can also track your page performance, analyze your visitors, and integrate with Google Ads and Zoho CRM.	Medium	Zoho Cloud Services
Service Desk Plus (Cloud)	Enterprise and IT Service Management	ManageEngine ServiceDesk Plus Cloud is a comprehensive help desk and asset management software that provides help desk agents and IT managers an integrated console to monitor	Large	ManageEngine

Product Name	Product Category	Product Description	Product Scale	Division
		and maintain the assets and IT requests generated from the users of the IT resources in an organization.		
Service Desk Plus On-premises	Enterprise and IT service Management	ManageEngine ServiceDesk Plus is a comprehensive help desk and asset management software that provides help desk agents and IT managers an integrated console to monitor and maintain the assets and IT requests generated from the users of the IT resources in an organization.	Large	ManageEngine
ADManager Plus	Active Directory Management	An Active Directory (AD) management and reporting solution that allows IT administrators and technicians to manage AD objects easily and generate instant reports.	Medium	ManageEngine
ManageEngine Endpoint Central /MSP On-premises	Endpoint Management	Endpoint Central is a unified endpoint management (UEM) solution that helps in managing servers, laptops, desktops, smartphones, and tablets from a central location. It's a modern take on desktop management that can be scaled as per organizational needs.	Large	ManageEngine
Qntrl	Workflow Automation	Qntrl is a software that automates your business processes in one go. You can design forms, blueprints, and cards to collect data, design workflows, and request tasks. You can also monitor and manage your progress using reports and notifications.	Large	Qntrl
MedicalMine Division CharmHealth	Healthcare IT	The CharmHealth online system. Electronic Health Records Practice Management Revenue Cycle Management TeleHealth Patient Engagement Portal Medical Billing Platform.	Large	MedicalMine

3.2 The Principal Service Commitments and System Requirements

Zoho makes service commitments to its Clients/User Entities and has established system requirements as part of its service delivery. Some of these commitments are principal to the performance of the service and relate to applicable criteria.

Zoho is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Zoho’s service commitments and system requirements are achieved.

Service commitments to User Entities are documented and communicated in Master Service agreement and Terms of Service or any other agreements as agreed by Zoho and User Entities.

Principal Commitments and Related Controls Requirements

Availability:

Zoho ensures the availability of their product services, Zoho’s policy for scheduling of downtime for maintenance and the remedies available to User Entities/Subscribers in the event of Zoho’s failure to meet the service availability commitment as per the agreed timelines in the Master Service Agreement.

Zoho will execute the Business Continuity and Disaster recovery plan as specified in the relevant individual agreement to periodically test, review and demonstrate the business continuity and disaster recovery plan to, and ensure it is fully operational.

Zoho undertakes to acknowledge and resolve Service Defects reported by the user entities as per the agreed timelines.

CA24: Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis.

CA38: Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.

CA39: Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.

CA78: Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.

CA91: The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.

CA92: Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.

CA93: The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.

Principal Commitments and Related Controls Requirements

CA107: Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

Privacy:

Zoho ensures to maintain security, confidentiality, processing integrity and privacy of Client's/User Entities' data as committed in the Privacy Policy.

CA22: Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.

Zoho ensures to obtain consent from the data subjects, process only those data as required, respond to the requests from the data subject and follow the disclosure requirements specified in the privacy policy.

CA26: On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.

CA27: A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.

CA28: On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

CA104: Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.

CA106: The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:

- 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information
 - 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information
 - 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information
-

Principal Commitments and Related Controls Requirements

4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.

CA107: Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

CA-114: On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in

- 1) Conformity with the purposes identified in the entity's privacy notice.
- 2) Conformity with the consent received from the data subject.
- 3) Compliance with applicable laws and regulations.

CA-116: The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.

CA119: On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.

CA120: The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.

CA125: Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.

CA128: The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.

Principal Commitments and Related Controls Requirements

Security:

Zoho shall provide training to its associates covering the aspects such as the security, confidentiality and availability and Zoho shall perform appropriate background checks for its associates in accordance with its Background Verification policies.

Zoho shall establish a mechanism to prevent unauthorized access to its systems by the means of logical and physical security and also employ appropriate encryption mechanism for the data stored in their servers.

CA04: Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.

CA08: Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.

CA09: Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.

CA10: Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.

CA11: Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.

CA16: Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.

CA15: Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.

CA18: Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.

CA53: For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.

CA54: Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.

Principal Commitments and Related Controls Requirements

CA60: Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.

CA61: Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks.

CA64: On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.

CA65: On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken.

CA76: On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.

Processing Integrity:

Zoho undertakes to acknowledge and resolve Service Defects reported by the Clients as per the agreed timelines.

CA39: Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.

CA44: Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.

CA107: Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

Principal Commitments and Related Controls Requirements

Confidentiality:

Zoho is responsible for maintaining non-disclosure agreement with the parties that would address the confidentiality of Customer's information in connection with the provision of the services by Zoho to its Customers.

CA09: Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.

CA10: Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.

CA105: Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.

3.3 Boundaries of the System

The boundaries of the system for the purposes of this report includes the following details:

- Infrastructure: - Zoho Corporate Office and offshore development centers located in
 - a. Chennai, India
 - b. Tenkasi, India
 - c. Renigunta, India
- Corporate website refers to Zoho's corporate websites - www.zoho.com, www.zoho.au, www.zoho.eu and www.zoho.in which is publicly accessible via the internet.
- International Datacenter (IDC) infrastructure refers to servers, databases and network devices available within the IDCs.
- Production environment refers to servers within the IDC infrastructure used to support the production instances of products.
- IDC Access Network or IAN Network refers to the IDC Access Network that is used for highly restricted logical access from Zoho Development center to the IDC Infrastructure.
- Network Operations Centre or NOC refers to a physically segregated and access controlled work area located in Zoho Development Centers occupied by members from the Server Operations team, NOC Team Members and Sysadmin teams.
- Zoho server rooms refer to servers, databases and network devices available within Zoho's Development Centers used to support non-production environments of products.
- Local Zoho Environment refers to servers and databases supporting development and test instances of products hosted within Zoho server rooms.
- The infrastructure of Zoho includes database and servers pertaining to the in-scope applications. The firewalls and Intrusion Prevention System ('IPS') which are configured in the perimeter firewall and Vulnerability assessment and penetration testing is performed by Zoho. The in-scope applications mentioned in Table 1 in Section 3.1 are primarily supported by operating system Cent OS, Debian OS and database including PostgreSQL and MySQL.

- Software - Zoho has a standard software list for internal use which is approved by the Information Technology Service (ITS) Team. All the Zoho workstations are installed with the standard software; additional software other than those from the approved list are installed based on the approval from the respective managers. The criteria 'processing integrity' pertaining to the in-scope applications is covered through the relevant IT controls that are responsible for the processing of transactions completely, accurately and on a timely basis. Product functionality, including automated controls configured to process clients' business transactions completely and accurately do not form part of the assessment scope of this report.
- People – Zoho has dedicated teams and personnel involved in the operation and use of the system. These are Executive Management, Operations, Technical and Leadership staff, and Support personnel. The Executive Management at Zoho is responsible for establishment of organization policies, overseeing organization activities and achieving business objectives. Operations Management and staff are responsible for client implementation and day-to-day client support. Additionally, they monitor and manage inbound and outbound data flows and related processes. The support personnel include the Admin Team, Legal team, Server Operations Team, Network Operations Centre (NOC) team, physical security, system administration, and HR Team.
- Policies and Procedures – Zoho's Management has developed and communicated policies and procedures across functions including Application Development and Maintenance, Information Security, Data Privacy, Human Resource, Logical Security, Network Security, Infrastructure Change Management, Physical and Environmental Security, Backup and Restoration, and Incident Management to its associates through the intranet. These policies and procedures are reviewed and approved by Zoho's Management on an annual basis and primarily used internally to guide Zoho associates to support the day-to-day operations. The roles and responsibilities of the team members are defined in the policy and procedure document.
- Data – The Backup of Zoho's IDC servers data taken via ZAC tool are stored in Zoho Datacenters for SAAS based products. Basis the request from customer restoration of data is performed by the Zoho Server Operations team.

3.4 Control Environment Elements

3.4.1 Communication and Enforcement of Integrity and Ethical Values

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure.

Zoho has programs and policies defined and documented to promote integrity and ethical values in their environment. Zoho has adopted a code of ethics, referred to as "Employee Code of Conduct". This code of conduct applies to Zoho. Newly joined associates at Zoho are required to sign the Employee Code of Conduct which denotes their acceptance and agreement to abide by the same.

Training

The Training and Development Group plays a key role to facilitate meeting the following objectives of training:

- To enable utilization of manpower resources
- To improve the workforce skills in line with emerging business requirements. The following training programs are mandatory:
 - HR Induction Program

- Information Security Management System (ISMS) Awareness Workshop
- Security and Privacy Awareness Training

Zoho has launched new programs for associates with respect to the changes and developments in the use of technology. Zoho's continuous education programs enhance the relevance and effectiveness of learning. It has enhanced hands-on assessments to facilitate enhanced reach of the enablement program across the organization.

Upon joining Product teams, associates undergo training by designated individuals within the team via product training materials and practical exercises. Product related training materials are made available on Zoho Intranet for their respective teams.

Code of Conduct and Ethics

Zoho has framed a Code of Conduct and Ethics ('the code') which is applicable to the member of the Board, the Executive officers, and associates of the Company and its subsidiaries. Zoho has adopted the Code of Conduct and Ethics which forms the foundation of its ethics and compliance program and is available to all associates on its Intranet portal. It includes global best practices with an interactive resource making it easier for associates to understand while also trying in the elements of the code to Zoho's corporate culture.

Zoho has adopted a Whistle blower policy mechanism for Directors and associates to report concerns about unethical behavior, actual or suspected fraud, or violation of the Company's code of conduct and ethics. Upon initial employment, all associates are issued the Whistle blower policy which is part of the Code of Ethics document and are required to read and accept the policy.

3.4.2 Commitment to Competence

Zoho's Management defines competence as the knowledge and skills necessary to accomplish tasks that define employee's roles and responsibilities. Roles and responsibilities and job descriptions are defined in collaboration by HR and respective Team Managers. Management's commitment to competence includes Management's consideration of the job descriptions, roles and responsibilities for performing specific jobs and ensuring recruitment activities are in line with these requirements. Associates undergo training activities in the form of classroom trainings, training exercises and simulations, and are evaluated on an on-going basis by product teams.

Zoho has adopted ISO 27001, ISO 27701, ISO 27017, ISO 27018 International Standard to establish, document, implement, operate, monitor, review and maintain an Information Security and Privacy Management Systems to demonstrate its ability to provide services in line with the business activities and any applicable statutory, regulatory, legal and other requirements. Its aim is to enhance client satisfaction by continually improving the system. The validity of this existing certification is until August 2025.

3.4.3 Management's Philosophy and Operating Style

Zoho Management's philosophy and operating style encompass a broad range of characteristics including Management's approach to taking and monitoring business risks, and Management's attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zoho has implemented in this area are described below:

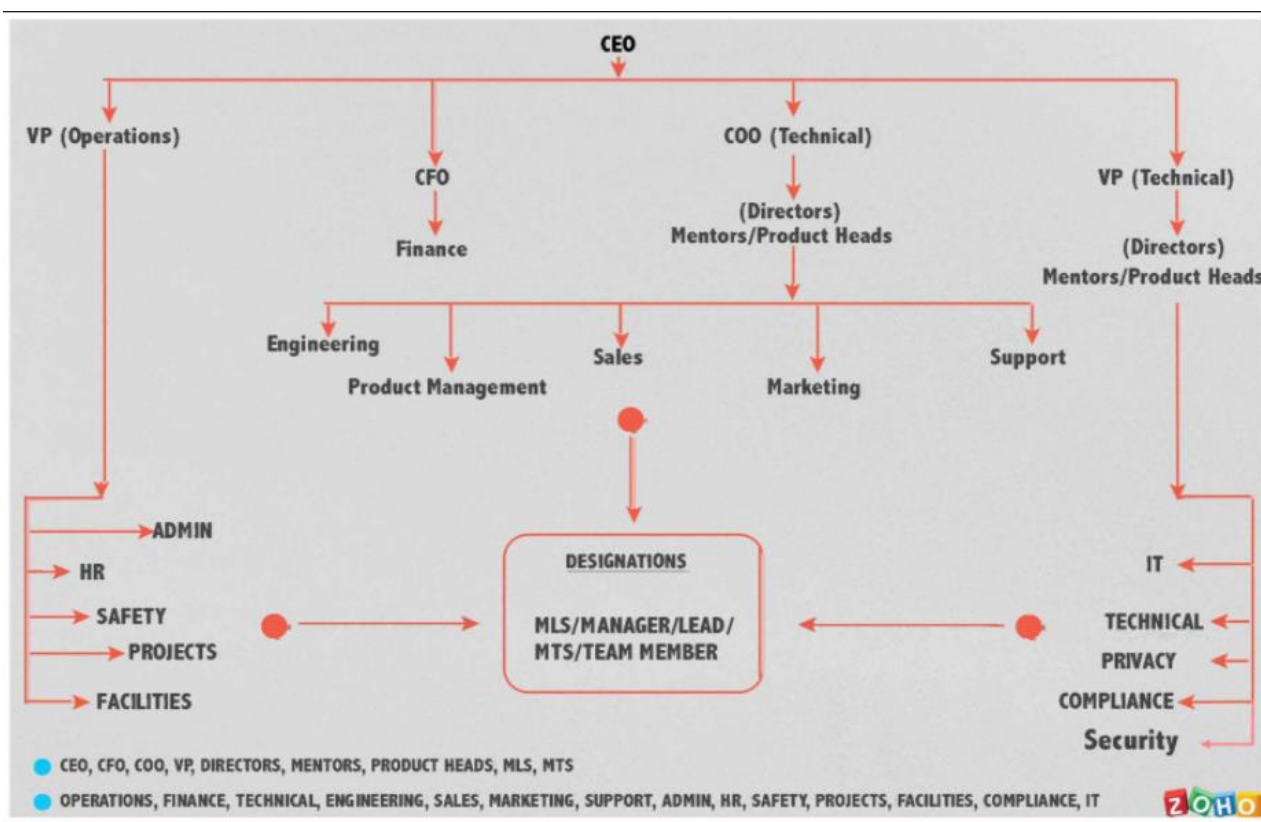
- Management is periodically briefed on regulatory and industry changes affecting the services provided,

- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

3.4.4 Organization Structure

Zoho has defined its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process to meet its commitments and requirements for applicable criteria.

Zoho's organizational structure establishes the key areas of authority and responsibility, appropriate lines of reporting, defined roles, and responsibilities. Roles, responsibilities and authorities associated with the roles that constitute Zoho's organizational structure are defined and documented by Zoho Management. Zoho's Security team is responsible for defining, implementing, and monitoring of policies and procedures related to information security and availability, which are made available to associates through internal portal.



3.4.5 Board of Directors

Zoho operates under the direction of Directors and other stakeholders, as the case may be, who meet and conduct the respective meetings in compliance with the law and for the growth and benefit of the company.

The Board of Directors has established a number of committees for addressing specific areas with well-defined objectives and activities like- Corporate Social Responsibility (CSR) Committee which oversees the implementation of CSR projects and CSR Spending's and Vigil (Whistle Blower) mechanism committee, which provides a channel to the associates and Directors to report to the management the concerns about unethical behavior, actual or suspected fraud or violation of the Codes of conduct or policy.

The Board of Directors meet at least once each quarter and perform the following functions regularly including but not limited to:

- Oversight of the selection, evaluation, development and compensation of senior management.
- Overseas management’s functions and protects the long-term interest of the organization’s stakeholders.
- Reviewing, approving and monitoring fundamentals financial and business strategies and major corporate actions.
- Assessing major risks facing the Company and reviewing options for their mitigation; and
- Ensuring that processes are in place for maintaining the integrity of the Company, the financial statements, compliance with law and ethics, relationship with user entities and suppliers and relationship with other stakeholders.

3.4.6 Assignment of Authority and Responsibility

Following are the roles and responsibilities of personnel within Zoho:

Role	Responsibility and Authority
Chief Executive Officer (CEO)	Responsible for handling Operations, Resource Management, Point of Communication for Directions
Chief Financial Officer (CFO)	Responsible for operations relating to Finance, Tax, Billing, Collections and Treasury.
Chief Operating Officer (COO)	Responsible for end-to-end handling Product Management and Operations
Vice President (VP)	Responsible for General Management, Administration and Product Management
Directors (Mentors / Product Heads)	Responsible for handling specific Zoho Products and Division Specific Management
Member Leadership Staff (MLS) / Member Technical Staff (MTS) / Team Member / Lead	<ul style="list-style-type: none"> - Responsible for handling specific product related roles - Responsible for handling product specific Internal Teams/Divisions/Stream based roles/Product based roles
Information Security Head	<ul style="list-style-type: none"> - Define the Information Security Policy - Ensure the communication and understanding of the Information Security Policy throughout the organization. - Monitor the implementation of security policy established under the Integrated ISPIMS.
Director of Compliance	<ul style="list-style-type: none"> - Accomplishes compliance business objectives by producing value added employee results; offering information and opinion as a member of senior management; integrating objectives with other business units; directing staff. - Develops compliance organizational strategies by contributing information, analysis, and recommendations to strategic thinking and direction, establishing functional objectives in line with organizational objectives. - Establishes compliance operational strategies by evaluating trends; establishing critical measurements; determining production, productivity, quality, and customer-service strategies; designing

Role	Responsibility and Authority
	<p>systems; accumulating resources; resolving problems; implementing change.</p> <ul style="list-style-type: none"> - Monitor the implementation of privacy policy established under the Integrated ISPIIMS. - Protects assets by establishing compliance standards; anticipating emerging compliance trends; designing improvements to internal control structure.
<p>Information Security Compliance Manager</p>	<ul style="list-style-type: none"> - Document and maintain the policies related to security of Organizational Information and information handled as a CSP - Ensure that the Information Security Management System is established, implemented, monitored and maintained. - Co-ordinate improvements to the Information Security Management System. - Perform periodic tests, Implement and act as per the Information Security Continuity Plan. - Facilitate implementation of corrective actions pertaining to Integrated ISPIIMS. - Perform periodic test, Implement and act as per Business Continuity Plan. - Plan and conduct internal audits. - Ensure the planning and execution of external audits. - Measure, track and analyse trends in metrics. - Implement and act per the Integrated ISMS policies that are applicable. - Periodic review of Integrated ISMS documents. - Review policies and documents in consultation with System Administrator before release. - Ensure that selected controls are documented in the Statement of Applicability and are implemented. - Monitor the implementation of Integrated ISMS on a continual basis and report discrepancies to the DOC. - Facilitate risk assessment using cross functional teams. - Identify training needs of Integrated ISMS and coordinate with training department to ensure that the training is completed. - Verify the implemented corrective actions.
<p>Member Technical Staff - Compliance Tools & Support</p>	<ul style="list-style-type: none"> - Establish, designing and implementing the process and tools to make the organization adhere to the compliance. - Analyze the compliance requirements, designing the solutions and implementing the same. - Responding to the compliance related questions raised by the customers. - Attending the conference calls with the customers on compliance. - Conducting meetings with the internal teams and steering.
<p>Product / Department Head / Internal Audit Coordinators</p>	<ul style="list-style-type: none"> - Implement the Integrated Information Security Management System and Cloud security best practices within product / Department. - Product / Department heads act as risk owners & will have the authority take decisions on risk, for their respective departments. - Obtain and communicate customer requirements to the appropriate personnel or functional organizations.

Role	Responsibility and Authority
	<ul style="list-style-type: none"> - Ensure that qualified, skilled, and trained personnel and other resources are available to implement the Integrated Information security Management System. - Ensure integrity, quality, safety, optimal cost, schedule, performance, reliability, accuracy and maintainability of products and services in order to satisfy customer requirements. - Ensure that the personnel comply with applicable standards, regulations, specifications, and documented procedures. - Provide the corrective actions.
Product Data Protection Officer (P-DPO)	<ul style="list-style-type: none"> - Heads & oversees the privacy implementation in their respective products/business units. - Maintains the Data inventory (Information Asset Register) for their respective product/business unit. - Reviews the documents pertaining to the common privacy practices, IAR in their respective teams. - Provides oversight and guidance to the PIMs in privacy related tasks, implementations in their respective products/business unit. - Co-ordinates with the Privacy Steering Committee on various activities related to privacy and compliance within their product/business unit. - Heads, authorizes and reviews the RCA of privacy incidents. - Serves as the first point of contact in case of any privacy incidents or escalations. - Must be or report to the Head of the Business Function/Product
Member- Compliance Audit	<ul style="list-style-type: none"> - Establish and execute compliance monitoring programs around information technology. Participate in internal security assessments, internal audits, customer audits, compliance certifications (external audit), and customer security questionnaire responses. - Assists in creating policies and procedures to help reduce risk, meet regulatory requirements and best business practices. - Performs Information security assessments and prepares findings and remediation reports. - Assists in updating and maintain policies, standards and procedures documents. - Evaluate security controls to ensure effectiveness and compliance, including managing the security control remediation efforts. - Coordinate with various teams in the organization regarding standards, regulations. - Coordinate with teams for Information Security awareness training. - Mapping and analyzing the adherence level with the applicable standards. - Performs other job-related duties as assigned.
Data Protection Officer (DPO)	<ul style="list-style-type: none"> - To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the data privacy regulations. - To monitor compliance with this the applicable data protection laws, and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

Role	Responsibility and Authority
	<ul style="list-style-type: none"> - To provide advice were requested as regards the data protection impact assessment and monitor its performance - To cooperate with the supervisory/data protection regulatory authorities - To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation of certain types of processing of personally identifiable information(as maybe required by the laws) and to consult, where appropriate, with regard to any other matter related to it.
Privacy Implementation Member (PIM)	<ul style="list-style-type: none"> - Implements or assist in implementing the privacy controls and features. - Provides reports of the consistency to the P-DPO on request. - Consults with the Privacy Team and/or Legal team on new activities or processes. - Conducts the Risk Assessment (DPIA) for their team's activities processes and products/features. - Co-operate during Privacy incidents by finding the root cause and works to fix it on priority. - Conduct privacy awareness trainings and exercises during team member on-boarding and periodically. - Ought to report directly to the P-DPO - Provide suggestions to the P-DPO on how to address privacy risks in a better way, proactively.
Lead - Privacy Operations & Management	<ul style="list-style-type: none"> - Establish and maintain the Privacy Program, which addresses the personal data management of both customers and employees. - Aids the ISH in defining the Information Privacy Policy of the organization. - Serve as the internal point of contact for the organisation's information privacy initiatives. - Co-ordinate with the Services and Operations teams to operationalize the program across all the applicable business units. - Facilitate Privacy Risk & Impact assessments as per the scope defined in the DPIA policy. - Initiate, facilitate and promote activities to foster information privacy awareness within the organization. - Perform ongoing monitoring of the compliance with the organisation's policies related to information privacy. - Work with the Legal team on negotiation of contracts with customers, vendors and other third parties. - Review the organisation's policies pertaining to the Information Privacy Program - Work with the Incident Management team during incident analysis and investigations that have effect on the privacy of the applicable parties. - Provide consultation to business personnel on methods to mitigate the risks identified. - Conduct trainings to internal auditors on PIMS - Work with the Compliance team during internal and external audits to assess and review the implementation of the privacy controls and the maturity.

Role	Responsibility and Authority
	<ul style="list-style-type: none"> - Review third party's privacy posture during vendor on-boarding especially when the third party processes personal data on behalf of the organization or its products. - Convert stakeholders' requirements into action plans for the organization, based on the applicable laws and lead the compliance program that follows.
Data Privacy Analyst	<ul style="list-style-type: none"> - Work as part of the Privacy team and assist in the administration, management, of the Zoho's Privacy Program and related projects, such as the EU GDPR compliance program . - Assist the DPO & the Privacy Lead in the handling and coordination of daily firm-wide data privacy exceptions, including but not limited to, response, investigation, logging, reporting and coordination. - Assist in the management and coordination of other on-going compliance, and projects. - Continuously assess Zoho's operations to develop policies, processes, and procedures related to Zoho's privacy practices and programs. - Remain well-informed and support the team members with questions related to Information Privacy Concepts. - Work closely with internal stakeholders, such as legal teams and other corporate functions to analyze and respond to privacy related issues, in co-operation with the Privacy Lead. - Work with internal stakeholders to implement and to maintain privacy best practices, such as conducting Data Protection Impact Assessments. - Assist Information Security team in responding to customer related surveys and questionnaires regarding the Zoho's compliance initiatives. - Evaluate vendor's privacy stature during vendor on-boarding process, especially if the vendor processes personal data on behalf of the organization or its products.
Director of IT (DOIT)	<ul style="list-style-type: none"> - Reviews and approves procedures pertaining to handling some of the privacy and security compliance related processes. - Advises on ways to achieve intended outcomes with respect to addressing risks in processing data. - Enables / spearheads some operations to improve the overall working of the GRC program and serves as an important person in the privacy steering committee.
Central Security Team	<ul style="list-style-type: none"> - Accountable for the overall Information Security and Cloud security Program. - Initiate, facilitate and promote activities related to security awareness in the organization. - Conduct Security Risk & Impact assessments for any new product, technology and architecture component. - Assist and guide the product security engineers on secure coding standards and security assessments guidelines within the product scope. - Responsible for identifying and building security tools and frameworks to assist the development and operations teams.

Role	Responsibility and Authority
	<ul style="list-style-type: none"> - Evaluate evolving new technologies in the context of information security and provide guidance on secure adoption to the product teams. - Closely work with the Incident management team during incident analysis and investigations.

3.4.7 Human Resource Policies and Practices

Zoho has defined policies and procedures on the intranet portal consisting of the HR processes covering the employee life cycle. These policies cover on-boarding, joining formalities, credential and reference checks, payroll processing, travel, leave and attendance management, rewards and recognition, performance review, employee benefits and employee separation. Third party service provider performs background checks for Zoho associates. The checks carried out include verification of educational qualifications and criminal checks as applicable for the associates.

Upon joining Zoho, newly joined associates are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.

The associates are also required to sign a Non- Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media policy on their first day of employment as part of the employee handbook acknowledgement formalities.

3.5 Risk Assessment

Zoho’s risk assessment process identifies and manages risks that could potentially affect Zoho’s ability to provide services to user entities. This ongoing process requires that Management identify significant risks inherent in products or services as they oversee their areas of responsibility. Zoho identifies the underlying sources of risk, measures the impact to organization, measures the likelihood, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks. This process has identified risks resulting from the nature of the services provided by Zoho. Management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel.
- Security risk – Security related vulnerabilities in the Corporate and IDC infrastructure which may impact confidentiality of client data and availability of services.
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance - legal and regulatory changes.

3.6 Information and Communication

Zoho has procedures in place for user entities to report incidents and reach out for support. Roles and responsibilities of Zoho and Client are communicated to all the stake holders. Any upgrades, planned downtimes are communicated to the user entities in advance.

Zoho Intranet channels are an important medium for associate communication to know the policies and procedures. Dedicated portal for GRC (Governance, risk, and compliance) is in place for policies and procedures. The internal communication from the Senior Management or the support groups comes in the form of Blogs, emails, Newsletters, Zoho Connect Portal etc. The communication includes messages related to Security policies and procedures, new initiatives and tools, performance management, rewards, and recognitions etc.

Zoho communicates its commitment to security as a top priority for its customers via Master Service Agreement and Terms of Service. Mock drill for BCP/DR is initiated on an annual basis at Zoho facilities and the results are communicated to the Top management (CEO, CFO & Directors) personnel. Zoho Privacy team communicates changes to confidentiality commitments through Zoho Code of ethics, whenever applicable. Zoho security commitments to users and required security obligations are communicated to users during the induction program.

3.7 Monitoring

Zoho has developed an organization-wide Integrated Information Security & Privacy Manual (IISPM) based on the ISO27001 standard. The Information Security ('IS') Policy is structured and is made available to the Zoho associates through a Portal on the Intranet.

The Compliance team is responsible for monitoring compliance with the IISPM policy at Zoho. Internal audits are conducted by the Compliance team at half yearly intervals to monitor compliance with the policy. Any deviation from the laid down policies and procedures is noted as an exception and accordingly reported to Management for corrective action.

3.8 Processes and controls

Human Resource Management:

Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis. Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis. Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates.

Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis. Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates. Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.

Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.

Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the

training is captured in Zoho people. Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.

Physical and Environmental Security:

Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates. For associates joining Zoho, the HR team creates a request for providing physical access card and the same is actioned upon by the Physical Security team. The access cards are distinguished based on the color of the tags described in the HR process document.

In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team deactivates the old access card and issues a new access card. For associates leaving Zoho, the HR team creates a request for revoking physical access card and the same is actioned upon by the Physical Security team on the last working day. Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.

Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals. ' Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days. Environmental safeguards are installed in Zoho facilities comprising of the following:

- Cooling Systems
- UPS with Battery and diesel generator back-up
- Smoke detectors
- Water sprinklers
- Fire resistant floors
- Fire extinguisher

Planned Preventive Maintenance (PPM) is performed on a periodic basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators. Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.

Compliance:

Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis. Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis. Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.

On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action. A contract is defined,

documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses. On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting. Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security as part of ISMS manual, on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal. Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

On an annual and periodic basis (The risk assessment is performed regularly based on the calendar), Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity. Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate. Zoho has defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials. The Security Head oversees and is responsible for the compliance and identification of ePHI data.

Incident Management

Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis. Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.

Incidents reported from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool. A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved. An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.

Support Requests:

Zoho Customer Success team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis. Support related requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.

Products Change Management:

Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master - Project Manager on an annual basis. Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis. Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.

Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team. Secure coding practices are defined and communicated to the respective personnel as part of Zoho's SDLC (Software Development Lifecycle) process. Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.

Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications. The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team. The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution of issues identified from the testing, a sign-off is provided and then the code is deployed in the production environment. Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.

System Administration:

Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager - IT Services on an annual basis. Access to support admin portal of Zoho products are defined through IAM. Zoho support admin access is provisioned by the IAM team after obtaining approval from authorized personnel (IAM Team/Server Operations Team/Network Operations Team/Sysadmin Team). Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, and storage.

For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team. For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team. Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis. Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team (Server operations team or network operations team or sysadmin team) takes corrective action. Authentication of users to Zoho products are governed through IAM through which the password configuration including password complexity and lockout is enforced.

User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner. Zodoor network is used to provide customer support by Zoho team in the customer's production environment. The Zodoor network only provides limited access for Zoho team to customer network to provide support. IDC is network of production servers and supporting network components hosting the cloud products of Zoho.

Security Management:

Zoho Encryption at rest team has defined EAR (Encryption at rest) policy which specifies the procedure for encryption and key management. The document is review by EAR Team Lead and approved by Security - Manager on an annual basis. Zoho uses in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services. Access to KMS server is restricted. The new request is provided by authorized personnel based on approval from Manager in KMS team. Zoho Key Management service team implements encryption of data at rest including usage of Full Disk Encryption (FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.

Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks. Security settings for Domain (AD), IAM (Zoho accounts), IAN (Identity aware network) (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy. Zoho associates are required to use two factor authentication to connect to IDC infrastructure. On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken by the central security team. On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken by the central security team. Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days. Passwords of vendor default account in the production servers are changed on a periodical basis and access is restricted to IDC users.

Zero Trust Operations:

Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request. The access requests are raised in the access approval form in zero trust application by the user selecting the datacenter where access is required. Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.

Network Operations - NOC

Zoho NOC team has defined procedure for logical access and operations of NOC as part of Network operations center policy. The document is reviewed by NOC L3 Engineer/Manager and approved by the NOC Manager on an annual basis. The document is made available on intranet portal for Zoho associates. Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis. Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.

Zoho has implemented measures to monitor the network in order to detect any attacks from the external network. VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team. The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.

On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset. Access to Corporate VPN is authenticated with Zoho users' AD account. Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP. Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers. When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.

Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure. The NOC team uses Network Configuration Manager tool to backup network device configuration on a daily basis (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team. Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.

Server Operations

Zoho Server Operations team has defined data center operations document which specifies procedures relating to day-to-day operations of Server Operations including procedures for degaussing the disks. The document is reviewed by Data Center Manager and approved by Data center member leadership staff on an annual basis. Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis. As part of server hardening the servers are subject to configuration check in ZAC tool. The server can onboarded and added to the IDC network only if the configurations of the servers were proper. Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.

Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner. The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken. Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.

IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR. The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team. Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.

The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage. Log of activities performed by users in IDC servers are captured and stored after each session in the Zoho Logs server and the same is available for review. MI tool is used to ensure time sync for IDC Servers. The MI tool is synchronized to a trusted public time source of the GPS. The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement. Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager. Privileged access to servers is restricted to authorized personnel from the Server Operations team. Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network. Access to external storage devices and internet are disabled on IDC servers to prevent data loss. Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team's daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis. Zoho admin team maintains a register to document the repairs and modifications to the physical components of Zoho facilities that are related to physical access security.

Tools Management:

Password of tools used in Zoho are configured as per the approved password policy. Privilege access to tools used in Zoho is restricted to authorized associates.

Legal:

Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users. The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:

1. Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information.
2. Policies regarding retention, sharing, disclosure, and disposal of their personal information.
3. The mechanism(s) to access, make changes to, or make inquiries regarding their personal information.

4. Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.

Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications. Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.

Privacy:

The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof. Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is:

1. readily accessible and made available to the data subject.
2. Provided in a timely manner to the data subjects.
3. Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity.
4. informs data subjects of a change to a previously communicated privacy notice.
5. Documents the changes to privacy practices that were communicated to data subjects.

Zoho's Privacy Policy includes the below policy around Choice and Consent:

1. Consent is obtained before the personal information is processed or handled.
2. To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences.
3. When authorization is required (explicit consent), the authorization is obtained in writing.
4. Implicit consent has clear actions on how a data subject opts out.
5. Action by a data subject to constitute valid consent.
6. Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the circumstances.

The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions. Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by

1. Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information.
2. Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution.

3. Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.

On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in

1. Conformity with the purposes identified in the entity's privacy notice.
2. Conformity with the consent received from the data subject.
3. Compliance with applicable laws and regulations.

Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:

1. The system processes in place to delete information in accordance with specific retention requirements.
2. Deletion of backup information in accordance with a defined schedule.
3. Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention.
4. Annually reviews information marked for retention.

The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance. Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President. On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges. On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects. The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.

On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel. Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required. The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information. When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC). Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to processing and the rejections are recorded in a repository. On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.

Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis. The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity’s policies for conformity to the requirement. Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary. Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA. An annual review of the organization’s data inventory is performed by the Privacy team to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners. The master activity register lists the PII data used by the product teams along with the roles and security measures.

3.9 HIPAA and Trust Services Criteria

Zoho’s control environment reflects the position taken by management, its Corporate Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure.

The Health Insurance Portability and Accountability Act (HIPAA) statements and trust services criteria are listed below:

Subpart	HIPAA Section	Section Title
C – Security	§164.306	Administrative safeguards

HIPAA §164.306 (a) General requirements. Covered entities and business associates must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

- (i) The size, complexity, and capabilities of the covered entity or business associate.
- (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
- (iii) The costs of security measures.
- (iv) The probability and criticality of potential risks to electronic protected health information.

(c) Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in §§164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information.

(d) Implementation specifications. In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must -

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate -

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate -

(e) Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii).

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Subpart	HIPAA Section	Section Title
C – Security	§164.308	Administrative safeguards

HIPAA §164.308(a)(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

HIPAA §164.308(a)(1)(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

HIPAA §164.308(a)(1)(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.308(a)(1)(ii)(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

HIPAA §164.308(a)(1)(ii)(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

HIPAA §164.308(a)(1)(ii)(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's

HIPAA §164.308(a)(1)(ii)(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

HIPAA §164.308(a)(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

HIPAA §164.308(a)(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

HIPAA §164.308(a)(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(3)(ii)(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(3)(ii)(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

HIPAA §164.308(a)(3)(ii)(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(3)(ii)(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.308(a)(4)(ii)(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

HIPAA §164.308(a)(4)(ii)(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(4)(ii)(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

HIPAA §164.308(a)(5)(ii)(A) Security reminders (Addressable). Periodic security updates.

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

HIPAA §164.308(a)(5)(ii)(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

HIPAA §164.308(a)(5)(ii)(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(5)(ii)(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

HIPAA §164.308(a)(5)(ii)(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

CC6.3 -The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.308(a)(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

HIPAA §164.308(a)(6)(ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

HIPAA §164.308(a)(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

HIPAA §164.308(a)(7)(ii)(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

HIPAA §164.308(a)(7)(ii)(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

HIPAA §164.308(a)(7)(ii)(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

HIPAA §164.308(a)(7)(ii)(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

HIPAA §164.308(a)(7)(ii)(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

HIPAA §164.308(a)(7)(ii)(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

HIPAA §164.308(a)(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

HIPAA §164.308(a)(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

HIPAA §164.308(b)(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.308(b)(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.308(b)(3) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

Subpart	HIPAA Section	Section Title
C – Security	§164.310	Physical safeguards

HIPAA §164.310(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

HIPAA §164.310(a)(2)(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

HIPAA §164.310(a)(2)(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

HIPAA §164.310(a)(2)(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

HIPAA §164.310(a)(2)(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.310(b) Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.310(c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.310(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

HIPAA §164.310(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.310(d)(2)(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

P4.1 - The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

P4.2 - The entity retains personal information consistent with the entity's objectives related to privacy.

P4.3 - The entity securely disposes of personal information to meet the entity's objectives related to privacy.

C1.2 -The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

HIPAA §164.310(d)(2)(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

P4.2 - The entity retains personal information consistent with the entity's objectives related to privacy.

P4.3 - The entity securely disposes of personal information to meet the entity's objectives related to privacy.

C1.2 -The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.310(d)(2)(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

HIPAA §164.310(d)(2)(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

Subpart	HIPAA Section	Section Title
C – Security	§164.312	Technical safeguards

HIPAA §164.312(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.312(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

HIPAA §164.312(a)(2)(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

HIPAA §164.312(a)(2)(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.

HIPAA §164.312(a)(2)(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

HIPAA §164.312(a)(2)(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.312(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

HIPAA §164.312(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

PI1.3 - The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

HIPAA §164.312(c)(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

HIPAA §164.312(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those

HIPAA §164.312(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.312(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

HIPAA §164.312(e)(2)(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

HIPAA §164.312(e)(2)(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Subpart	HIPAA Section	Section Title
C – Security	§164.314	Organizational requirements

HIPAA §164.314(a)(1) Standard: Business associate contracts or other arrangements. The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.314 (a):

(2) Implementation specifications (Required).

(i) Business associate contracts. The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by §164.410.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.314(a)(2)(ii) Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.314(a)(2)(iii) Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.314(b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.314(b)(2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

- §164.314(b)(2)(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;
- §164.314(b)(2)(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;
- §164.314(b)(2)(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
- §164.314(b)(2)(iv) Report to the group health plan any security incident of which it becomes aware

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
C – Security	§164.316	Policies and procedures and documentation requirements

HIPAA §164.316(a) A covered entity or business associate must, in accordance with §164.306:

(a) Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.316(b)(1) Standard: Documentation.

(b)(1)(i) (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(b)(1)(ii) (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.316(b)(2) Implementation specifications:

(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

HIPAA §164.316(b)(2)(ii) Availability (Required). Make documentation available+ to those persons responsible for implementing the procedures to which the documentation pertains.

CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

HIPAA §164.316(b)(2)(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Subpart	HIPAA Section	Section Title
D - Breach	§164.404	Notification to individuals

HIPAA §164.404(a)(1) Standard, General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification

(1) Elements. The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address."

(2) Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language.

(d) Implementation specifications: Methods of individual notification. The notification required by paragraph (a) of this section shall be provided in the following form:

(1) Written notice.

(i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) Additional notice in urgent situations. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
D - Breach	§164.406	Notification to the media

§164.406(1) (a) Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification. The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
D - Breach	§164.408	Notification to the Secretary

HIPAA §164.408(a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.

(b) Implementation specifications: Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.

(c) Implementation specifications: Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
D - Breach	§164.410	Notification by a Business associate

HIPAA §164.410(a) Standard

(a)(1) General rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(a)(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) Implementation specifications: Timeliness of notification. Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification.

(c)(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is

reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(c)(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity’s objectives related to privacy.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.412	Law Enforcement Delay

HIPAA §164.412 If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

- (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
- (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.502	Uses and disclosures of protected health information: General rules

HIPAA §164.502(a) Standard. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Covered entities: Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

- (i) To the individual;
- (ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;

-
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
 - (iv) Except for uses and disclosures prohibited under §164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under §164.508;
 - (v) Pursuant to an agreement under, or as otherwise permitted by, §164.510; and
 - (vi) As permitted by and in compliance with this section, §164.512, §164.514(e), (f), or (g).
- (2) Covered entities: Required disclosures. A covered entity is required to disclose protected health information:
- (i) To an individual, when requested under, and required by §164.524 or §164.528; and
 - (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.
-

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.502(a)

- (3) Business associates: Permitted uses and disclosures. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.
- (4) Business associates: Required uses and disclosures. A business associate is required to disclose protected health information:
- (i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.
 - (ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.
-

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

HIPAA §164.502(a)(5)(i)

Prohibited uses and disclosures.

- (i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:
-

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.502(a)(5)(ii)

(ii) Sale of protected health information:

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(2) Sale of protected health information does not include a disclosure of protected health information:

(i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(iii) For treatment and payment purposes pursuant to § 164.506(a);

(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(vi) To an individual, when requested under § 164.524 or § 164.528;

(vii) Required by law as permitted under § 164.512(a); and

(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a

reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

HIPAA §164.502(b)

Standard: Minimum necessary - Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

- (i) Disclosures to or requests by a health care provider for treatment;
 - (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
 - (iii) Uses or disclosures made pursuant to an authorization under § 164.508;
 - (iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
 - (v) Uses or disclosures that are required by law, as described by § 164.512(a); and
 - (vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.
-

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

HIPAA §164.502(c)

(c) Standard: Uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

HIPAA §164.502(d)

(d) Standard: Uses and disclosures of de-identified protected health information -

(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.502(e)

(1) Standard: Disclosures to business associates.

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in

accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) Implementation specification: Documentation. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

HIPAA §164.502(f)

Standard: Deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

HIPAA §164.502(g)

(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) Implementation specification: Adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)

(i) Implementation specification: Unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

(C) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: Abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

HIPAA §164.502(h)

Standard: Confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

HIPAA §164.502(i)

Standard: Uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

HIPAA §164.502(j)

Standard: Disclosures by whistle blowers and workforce member crime victims -

(1) Disclosures by whistle blowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity’s objectives related to privacy.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity’s objectives related to privacy. The entity assesses those parties’ compliance on a periodic and as-needed basis and takes corrective action, if necessary.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity’s objectives related to privacy.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.504	Uses and disclosures: Organizational requirements

HIPAA §164.504(e)(1) Standard: Business associate contracts.

(i) The contract or other arrangement required by §164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in §164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in §164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) Implementation specifications: Business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by §164.410;

(D) In accordance with §164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract."

(3) Implementation specifications: Other arrangements.

(i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and §164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and §164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and §164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and §164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in §160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and §164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and §164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and §164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with §§164.514(e)(4) and 164.314(a)(1), if applicable.

(4) Implementation specifications: Other requirements for contracts and other arrangements.

(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) Implementation specifications: Business associate contracts with subcontractors. The requirements of §164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by §164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

"(f)(1) Standard: Requirements for group health plans.

(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under §164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by §164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) Implementation specifications: Requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any

employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) Implementation specifications: Uses and disclosures. A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by §164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) Standard: Requirements for a covered entity with multiple covered functions.

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.506	Uses and disclosures to carry out treatment, payment, or health care operations

(a) Standard: Permitted uses and disclosures. Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) through (4) or that are prohibited under §164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) Standard: Consent for uses and disclosures permitted.

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart."

"(c) Implementation specifications: Treatment, payment, or health care operations.

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.508	Uses and disclosures for which an authorization is required

HIPAA §164.508(a) Standard: Authorizations for uses and disclosures

(1) Authorization required: General rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) Authorization required: Psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counselling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i)."

"(3) Authorization required: Marketing.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at §164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved."

"(4) Authorization required: Sale of protected health information.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in §164.501 of this subpart.

(ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) Implementation specifications: General requirements

(1) Valid authorizations.

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the

individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrolment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrolment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrolment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrolment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrolment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrolment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by §164.530(j).

(c) Implementation specifications: Core elements and requirements

(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) Required statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by §164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrolment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrolment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrolment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) Plain language requirement. The authorization must be written in plain language.

(4) Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.510	Uses and disclosures requiring an opportunity for the individual to agree or to object

(a) Standard: Use and disclosure for facility directories

(1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

-
- (B) The individual's location in the covered health care provider's facility;
 - (C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
 - (D) The individual's religious affiliation; and
- (ii) Use or disclose for directory purposes such information:
- (A) To members of the clergy; or
 - (B) Except for religious affiliation, to other persons who ask for the individual by name.
- (2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.
- (3) Emergency circumstances.
- (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:
- (A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and
 - (B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.
- (ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.
- (b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes
- (1) Permitted uses and disclosures.
- (i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.
- (ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.
- (2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:
- (i) Obtains the individual's agreement;
 - (ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
-

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) Limited uses and disclosures when the individual is not present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) Uses and disclosures when the individual is deceased. If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.512	Uses and disclosures for which an authorization or opportunity to agree or object is not required

(a) Standard: Uses and disclosures required by law.

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) Standard: Uses and disclosures for public health activities

(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the

reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labelling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(1) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or

-
- (2) The individual, if the individual is an adult or emancipated minor.
- (2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.
- (c) Standard: Disclosures about victims of abuse, neglect or domestic violence
- (1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:
- (i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
- (ii) If the individual agrees to the disclosure; or
- (iii) To the extent the disclosure is expressly authorized by statute or regulation and:
- (A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
- (B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- (2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:
- (i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- (ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
- (d) Standard: Uses and disclosures for health oversight activities
- (1) Permitted disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
- (i) The health care system;
- (ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
- (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.
- (2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:
-

-
- (i) The receipt of health care;
 - (ii) A claim for public benefits related to health; or
 - (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services."
- (3) Joint activities or investigations. Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.
- (4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.
- (e) Standard: Disclosures for judicial and administrative proceedings
- 1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
- (i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or
 - (ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
 - (A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or
 - (B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.
 - (iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
 - (A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
 - (B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
 - (C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
 - (1) No objections were filed; or
 - (2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
 - (iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
-

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section."

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

"(f) Standard: Disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) Permitted disclosures: Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

(2) Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

-
- (B) Date and place of birth;
 - (C) Social security number;
 - (D) ABO blood type and rh factor;
 - (E) Type of injury;
 - (F) Date and time of treatment;
 - (G) Date and time of death, if applicable; and
 - (H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye colour, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- (ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.
- (3) Permitted disclosure: Victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:
- (i) The individual agrees to the disclosure; or
 - (ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
 - (A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
 - (B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - (C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
- (4) Permitted disclosure: Decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.
- (5) Permitted disclosure: Crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.
- (6) Permitted disclosure: Reporting crime in emergencies.
- (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
 - (A) The commission and nature of a crime;
 - (B) The location of such crime or of the victim(s) of such crime; and
 - (C) The identity, description, and location of the perpetrator of such crime.
 - (ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need
-

of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section."

(g) Standard: Uses and disclosures about decedents

(1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) Standard: Uses and disclosures for research purposes

(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes."

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and
(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(1) An adequate plan to protect the identifiers from improper use and disclosure;

(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review

procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and"

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) Standard: Uses and disclosures to avert a serious threat to health or safety

(1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in §164.501.

(2) Use or disclosure not permitted. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counselling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counselling, or therapy described in paragraph (j)(2)(i) of this section.

(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) Standard: Uses and disclosures for specialized government functions

(1) Military and veterans activities

(i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Défense or Homeland Security may disclose to the Department of Veterans Affairs

(DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.

(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) Medical suitability determinations. A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) Correctional institutions and other law enforcement custodial situations

(i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) Covered entities that are government programs providing public benefits.

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrolment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrolment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(7) National Instant Criminal Background Check System. A covered entity may use or disclose protected health information for purposes of reporting to the National Instant Criminal Background Check System the identity of an individual who is prohibited from possessing a firearm under 18 U.S.C. 922(g)(4), provided the covered entity:

(i) Is a State agency or other entity that is, or contains an entity that is:

(A) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; or

(B) A court, board, commission, or other lawful authority that makes the commitment or adjudication that causes an individual to become subject to 18 U.S.C. 922(g)(4); and

(ii) Discloses the information only to:

(A) The National Instant Criminal Background Check System; or

(B) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; and

(iii)(A) Discloses only the limited demographic and certain other information needed for purposes of reporting to the National Instant Criminal Background Check System; and

(B) Does not disclose diagnostic or clinical information for such purposes.

(l) Standard: Disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.514	Other requirements relating to uses and disclosures of protected health information

(a) Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

(c) Implementation specifications: Re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) Standard: minimum necessary requirements. In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) Implementation specifications: Minimum necessary uses of protected health information.

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) Implementation specification: Minimum necessary disclosures of protected health information.

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of §164.512(i) have been provided by a person requesting the information for research purposes.

(4) Implementation specifications: Minimum necessary requests for protected health information.

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) Implementation specification: Other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(3) Implementation specification: Permitted purposes for uses and disclosures.

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only

to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) Implementation specifications: Data use agreement

(i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) Contents. A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

(iii) Compliance.

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f) Fundraising communications

(1) Standard: Uses and disclosures for fundraising. Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of §164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) Implementation specifications: Fundraising requirements.

(i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) Standard: Uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at §164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: Verification

(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.520	Notice of privacy practices for protected health information

(a) Standard: Notice of privacy practices

(1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans.

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in §164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in §164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section."

(3) Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to correctional institution that is a covered entity.

(b) Implementation specifications: Content of notice. (1) Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

(ii) Uses and disclosures. The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)- (a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; (B)

In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with

respect to a group health plan, may disclose protected health information to the sponsor of the plan;
or

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) Covered entity's duties. The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) Complaints. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) Contact. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) Optional elements.

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) Revisions to the notice. The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) Implementation specifications: Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) Specific requirements for health plans.

(i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) Specific requirements for electronic notice.

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) Implementation specifications: Joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) Implementation specifications: Documentation. A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.522	Rights to request privacy protection for protected health information

(a)(1) Standard: Right of an individual to request restriction of uses and disclosures.

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under §164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §164.502(a)(2)(ii), §164.510(a) or §164.512.

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) Implementation specifications: Terminating a restriction. A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual."

(3) Implementation specification: Documentation. A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

(b)

(1) Standard: Confidential communications requirements.

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) Implementation specifications: Conditions on providing confidential communications.

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.524	Access of individuals to protected health information

(a) Standard: Access to protected health information

(1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

- (i) Psychotherapy notes; and
- (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information."

"(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person."

(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care

professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) Implementation specifications: Requests for access and timely action

(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) Timely action by the covered entity.

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access."

(c) Implementation specifications: Provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested.

(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) Time and manner of access.

(i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

- (1) The designated record sets that are subject to access by individuals; and
- (2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.526	Amendment of protected health information

(a) Standard: Right to amend.

(1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

- (i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
- (ii) Is not part of the designated record set;
- (iii) Would not be available for inspection under §164.524; or
- (iv) Is accurate and complete.

(b) Implementation specifications: Requests for amendment and timely action.

(1) Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements."

(2) Timely action by the covered entity.

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: Denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures.

(i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) Implementation specification: Actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) Implementation specification: Documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.528	Accounting of disclosures of protected health information

(a) Standard: Right to an accounting of disclosures of protected health information.

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in §164.506;

(ii) To individuals of protected health information about them as provided in §164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502;

(iv) Pursuant to an authorization as provided in §164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510;

(vi) For national security or intelligence purposes as provided in §164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in §164.512(k)(5);

(viii) As part of a limited data set in accordance with §164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in §164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under § 164.502(a)(2)(ii) or § 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under § 164.502(a)(2)(ii) or § 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)

(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) Implementation specifications: Provision of the accounting.

(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent

request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

- (1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;
- (2) The written accounting that is provided to the individual under this section; and
- (3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.530	Administrative Requirements

(a)(1) Standard: Personnel designations.

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.

(2) Implementation specification: Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

"(2) Implementation specifications: Training.

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section."

(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

"(2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure."

(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of §164.502(j) or paragraph (g)(2) of this section.

(2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in §160.316 of this subchapter.

(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: Changes to policies and procedures.

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in §164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with §164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by §164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with §164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) Implementation specifications: Changes to privacy practices stated in the notice.

(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by §164.520(b)(3) to state the changed practice and make the revised notice available as required by §164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under §164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) Implementation specification: Changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by §164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) Standard: Documentation. A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

- (iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.
- (iv) Maintain documentation sufficient to meet its burden of proof under §164.414(b).
- (2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
- (k) Standard: Group health plans.
 - (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:
 - (i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
 - (ii) The group health plan does not create or receive protected health information, except for:
 - (A) Summary health information as defined in §164.504(a); or
 - (B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
 - (2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with §164.504(f).

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

Subpart	HIPAA Section	Section Title
E - Privacy	§164.532	Transition provisions

- (a) Standard: Effect of prior authorizations. Notwithstanding §§164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with §164.512(i)(1)(i).
- (b) Implementation specification: Effect of prior authorization for purposes other than research. Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).
- (c) Implementation specification: Effect of prior permission for research. Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) Standard: Effect of prior contracts or other arrangements with business associates. Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) Implementation specification: Deemed compliance -

(1) Qualification. Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of § 164.314(a) or § 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) Limited deemed compliance period. A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) Covered entity responsibilities. Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) Effect of prior data use agreements. If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

Zoho is a Business Associate and not a Covered Entity (Healthcare provider / Health Care Clearing House / Health Plan provider). Hence, therefore the HIPAA statement is not applicable for Zoho.

3.10 Trust Services Criteria and Description of Related Controls

3.10.1 Common criteria related to Control Environment

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Activity Number	Control Activities
CA01	Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.
CA04	Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.
CA05	Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA06	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA07	Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.
CA08	Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.
CA09	Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.
CA10	Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.
CA22	Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA30	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.

Control Activity Number	Control Activities
CA31	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.

CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Number	Activity	Control Activities
CA01		Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA31		Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.

CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Number	Activity	Control Activities
CA01		Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.
CA02		Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA31		Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.
CA104		Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA134		Zoho has defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials. The Security Head oversees and is responsible for the compliance and identification of ePHI data.

CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Number	Activity	Control Activities
CA02		Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.
CA03		Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA04		Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.
CA05		Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA06		Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA08		Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.
CA09		Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.
CA10		Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.
CA42		Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.
CA132		Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.
CA134		Zoho has defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials. The Security Head oversees and is responsible for the compliance and identification of ePHI data.

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Number	Activity	Control Activities
CA01		Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.

Control Number	Activity	Control Activities
CA02		Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.
CA05		Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA06		Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA31		Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.
CA126		On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.

3.10.2 Common criteria related to Communication and Information:

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Number	Activity	Control Activities
CA01		Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.
CA10		Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA42		Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.
CA51		Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.
CA95		MI tool is used to ensure time sync for IDC Servers. The MI tool is synchronized to a trusted public time source of the GPS.

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Number	Activity	Control Activities
CA02		Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.
CA03		Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA07		Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.
CA08		Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.
CA09		Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.
CA10		Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.

Control Number	Activity	Control Activities
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA40		Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master – Project Manager on an annual basis.
CA42		Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.
CA43		Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.
CA70		Zoho NOC team has defined procedure for logical access and operations of NOC as part of Network operations center policy. The document is reviewed by NOC L3 Engineer/Manager and approved by the NOC Manager on an annual basis. The document is made available on intranet portal for Zoho associates.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.
CA132		Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.

CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Number	Activity	Control Activities
CA07		Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR

Control Number	Activity	Control Activities
		Operations and approved by the Deputy Manager – HR Operations on an annual basis.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA39		Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA99		Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network.
CA107		Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA110		Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is: <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice

Control Number	Activity	Control Activities
		5) Documents the changes to privacy practices that were communicated to data subjects.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.
CA135		Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.

3.10.3 Common criteria related to Risk Assessment:

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Number	Activity	Control Activities
CA07		Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets

Control Number	Activity	Control Activities
		that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA43		Secure coding practices are defined and communicated to the respective personnel as part of the Zoho’s SDLC process.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA72		Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA117		Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.

Control Number	Activity	Control Activities
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are

Control Number	Activity	Control Activities
		any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Number	Activity	Control Activities
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.

Control Number	Activity	Control Activities
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA51		Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.
CA135		Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Number	Activity	Control Activities
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.

Control Number	Activity	Control Activities
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA40		Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master – Project Manager on an annual basis.
CA41		Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA51		Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA75		The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.
CA76		On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.
CA80		When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA95		MI tool is used to ensure time sync for IDC Servers. The MI tool is synchronized to a trusted public time source of the GPS.

Control Number	Activity	Control Activities
CA97		Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager.
CA108		Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

3.10.4 Common criteria related to Monitoring Activities:

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.

Control Number	Activity	Control Activities
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA72		Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA104		Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.
CA135		Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Number	Activity	Control Activities
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA31		Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets

Control Number	Activity	Control Activities
		that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA117		Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.

3.10.5 Common criteria relating to Control Activities

CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.

Control Number	Activity	Control Activities
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA41		Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA45		Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA68		Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.
CA69		Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.

Control Number	Activity	Control Activities
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA79		Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA92		Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA103		Privilege access to tools used in Zoho is restricted to authorized associates.
CA104		Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA42		Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.
CA43		Secure coding practices are defined and communicated to the respective personnel as part of the Zoho’s SDLC process.
CA44		Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.

Control Number	Activity	Control Activities
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA52		For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.
CA53		For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA62		Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.
CA63		Zoho associates are required to use two factor authentication to connect to IDC infrastructure.
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA77		Access to Corporate VPN is authenticated with Zoho users' AD account.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA86		Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.
CA87		Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA99		Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.
CA102		Password of tools used in Zoho are configured as per the approved password policy.
CA133		Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.

CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Number	Activity	Control Activities
CA03		Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates
CA11		Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho's information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA30		Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA40		Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master – Project Manager on an annual basis.
CA41		Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and

Control Number	Activity	Control Activities
		implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA70		Zoho NOC team has defined procedure for logical access and operations of NOC as part of Network operations center policy. The document is reviewed by NOC L3 Engineer/Manager and approved by the NOC Manager on an annual basis. The document is made available on intranet portal for Zoho associates.
CA84		Zoho Server Operations team has defined data center operations document which specifies procedures relating to day-to-day operations of Server Operations including procedures for degaussing the disks. The document is reviewed by Data Center Manager and approved by Data center member leadership staff on an annual basis.
CA104		Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.
CA105		Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.
CA110		Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity’s privacy practices). The notice is: <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.

3.10.6 Common criteria related to Logical and Physical Access Controls

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA51		Zoho maintains an asset register for it’s IT assets including servers, software, workstations, network devices, storage.
CA52		For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.

Control Number	Activity	Control Activities
CA53		For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.
CA57		User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner.
CA58		Zoho Encryption at rest team has defined EAR policy which specifies the procedure for encryption and key management. The document is reviewed by EAR Team Lead and approved by Security – Manager on an annual basis.
CA59		Zoho uses in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services. Access to KMS server is restricted. Access to KMS is provided by authorized personnel based on approval from Manager in KMS team.
CA60		Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.
CA61		Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks.
CA62		Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.
CA63		Zoho associates are required to use two factor authentication to connect to IDC infrastructure.
CA68		Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.
CA69		Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.
CA71		Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.
CA76		On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.
CA77		Access to Corporate VPN is authenticated with Zoho users' AD account.
CA79		Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers
CA83		Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.
CA86		Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.
CA87		Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server

Control Number	Activity	Control Activities
		Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.
CA98		Privileged access to servers is restricted to authorized personnel from the Server Operations team.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.
CA101		Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.
CA102		Password of tools used in Zoho are configured as per the approved password policy.
CA103		Privilege access to tools used in Zoho is restricted to authorized associates.
CA133		Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA52		For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.
CA53		For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.
CA57		User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner.
CA58		Zoho Encryption at rest team has defined EAR policy which specifies the procedure for encryption and key management. The document is reviewed by EAR Team Lead and approved by Security – Manager on an annual basis.
CA59		Zoho uses in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services. Access to KMS server is restricted. Access to KMS is provided by authorized personnel based on approval from Manager in KMS team.
CA60		Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.

Control Number	Activity	Control Activities
CA61		Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks.
CA62		Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.
CA63		Zoho associates are required to use two factor authentication to connect to IDC infrastructure.
CA68		Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.
CA69		Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.
CA77		Access to Corporate VPN is authenticated with Zoho users' AD account.
CA79		Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers
CA83		Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.
CA86		Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.
CA87		Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.
CA98		Privileged access to servers is restricted to authorized personnel from the Server Operations team.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.
CA101		Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team's daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.
CA102		Password of tools used in Zoho are configured as per the approved password policy.
CA103		Privilege access to tools used in Zoho is restricted to authorized associates.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.
CA133		Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.

CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement

Control Number	Activity	Control Activities
		and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA57		User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner.
CA62		Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.
CA63		Zoho associates are required to use two factor authentication to connect to IDC infrastructure.
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA68		Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.
CA69		Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.
CA77		Access to Corporate VPN is authenticated with Zoho users' AD account.
CA79		Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers
CA83		Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.
CA86		Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.
CA87		Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.
CA98		Privileged access to servers is restricted to authorized personnel from the Server Operations team.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.
CA101		Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team's daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.
CA102		Password of tools used in Zoho are configured as per the approved password policy.
CA103		Privilege access to tools used in Zoho is restricted to authorized associates.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA11		Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.
CA12		For associates joining Zoho, the HR team creates a request for providing physical access card and the same is actioned upon by the Physical Security team. The access cards are distinguished based on the color of the tags described in the HR process document.
CA13		In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team deactivates the old access card and issues a new access card.
CA14		For associates leaving Zoho, the HR team creates a request for revoking physical access card and the same is actioned upon by the Physical Security team on the last working day.
CA15		Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.
CA16		Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.
CA17		Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities.
CA18		Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.
CA136		Zoho admin team maintains a register to document the repairs and modifications to the physical components of Zoho facilities that are related to physical access security.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA15		Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.
CA17		Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities.
CA18		Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.

Control Number	Activity	Control Activities
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Number	Activity	Control Activities
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA62		Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.
CA63		Zoho associates are required to use two factor authentication to connect to IDC infrastructure.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA77		Access to Corporate VPN is authenticated with Zoho users’ AD account.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA99		Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.
CA102		Password of tools used in Zoho are configured as per the approved password policy.

CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA71		Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA83		Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC’s daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA86		Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.
CA87		Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.
CA88		The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.

Control Number	Activity	Control Activities
CA101		Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA51		Zoho maintains an asset register for it’s IT assets including servers, software, workstations, network devices, storage.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA55		Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA71		Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA75		The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.

Control Number	Activity	Control Activities
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.

3.10.7 Common criteria related to System Operations

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Number	Activity	Control Activities
CA43		Secure coding practices are defined and communicated to the respective personnel as part of the Zoho’s SDLC process.
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA55		Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.

Control Number	Activity	Control Activities
CA71		Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA75		The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA80		When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA97		Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analysed to determine whether they represent security events.

Control Number	Activity	Control Activities
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA49		Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager – IT Services on an annual basis.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA85		Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA92		Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.

Control Number	Activity	Control Activities
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.
CA100		Access to external storage devices and internet are disabled on IDC servers to prevent data loss.

CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Number	Activity	Control Activities
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA54		Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.
CA55		Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.

Control Number	Activity	Control Activities
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.

CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.

Control Number	Activity	Control Activities
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Number	Activity	Control Activities
CA33		Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA35		Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.
CA37		An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.

Control Number	Activity	Control Activities
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.

3.10.8 Common criteria related to Change Management

CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Number	Activity	Control Activities
CA40		Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master – Project Manager on an annual basis.
CA41		Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA45		Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA67		Passwords of vendor default account in the production servers are changed on a periodical basis and access is restricted to IDC users.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA75		The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.

Control Number	Activity	Control Activities
CA76		On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.
CA80		When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.
CA97		Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager.

3.10.9 Common criteria related to Risk Mitigation

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA25		Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

CC9.2 The entity assesses and manages risks associated with vendors and business partners.

Control Number	Activity	Control Activities
CA17		Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA32		On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.
CA135		Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.

3.10.10 Additional controls for Confidentiality:

C1.1: The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.

Control Number	Activity	Control Activities
CA09		Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.
CA10		Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server

Control Number	Activity	Control Activities
		Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA115		<p>Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:</p> <ol style="list-style-type: none"> 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.

C1.2: The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.

Control Number	Activity	Control Activity
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.
CA105		Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.
CA115		<p>Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:</p> <ol style="list-style-type: none"> 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.
CA135		Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.

3.10.11 Additional controls for Availability:

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control Number	Activity	Control Activities
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA29		Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.
CA51		Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.
CA64		On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.
CA65		On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken
CA72		Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.
CA73		Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA81		Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.
CA82		The NOC team uses Network Configuration Manager tool to backup network device configuration on a daily basis (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA92		Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.

Control Number	Activity	Control Activities
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.
CA107		Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

Control Number	Activity	Control Activities
CA11		Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.
CA18		Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.
CA19		Environmental safeguards are installed in Zoho facilities comprising of the following: <ul style="list-style-type: none"> • Cooling Systems • UPS with Battery and diesel generator back-up • Smoke detectors • Water sprinklers • Fire resistant floors • Fire extinguisher
CA20		Planned Preventive Maintenance (PPM) is performed on a periodic basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.
CA21		Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.
CA23		Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA39		Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA66		Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.

Control Number	Activity	Control Activities
CA82		The NOC team uses Network Configuration Manager tool to backup network device configuration on a daily basis (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.
CA88		The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA136		Zoho admin team maintains a register to document the repairs and modifications to the physical components of Zoho facilities that are related to physical access security.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Control Number	Activity	Control Activities
CA24		Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis
CA72		Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.
CA88		The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.

3.10.12 Additional criteria for Processing Integrity:

PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

Control Number	Activity	Control Activities
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA39		Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA44		Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.
CA105		Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.
CA107		Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.

PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

Control Number	Activity	Control Activities
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA44		Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.
CA46		The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.
CA47		The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.
CA48		Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.
CA50		Access to support admin portal of Zoho products are defined through IAM. Zoho support admin access is provisioned by the IAM team after obtaining approval from authorized personnel.
CA56		Authentication of users to Zoho products are governed through IAM through which the password configuration including password complexity and lockout is enforced.

Control Number	Activity	Control Activities
CA67		Passwords of vendor default account in the production servers are changed on a periodical basis and access is restricted to IDC users.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA94		Log of activities performed by users in IDC servers are captured and stored after each session in the Zoho Logs server and the same is available for review.

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA38		Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.
CA39		Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.
CA40		Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master – Project Manager on an annual basis.
CA41		Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.
CA42		Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.
CA43		Secure coding practices are defined and communicated to the respective personnel as part of the Zoho’s SDLC process.
CA45		Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.
CA74		VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.
CA80		When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.

PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA78		Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.
CA91		The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.
CA93		The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.

PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.

Control Number	Activity	Control Activities
CA60		Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.
CA88		The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken
CA89		Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.
CA90		IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.

3.10.13 Additional controls for Privacy:

Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity’s objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity’s privacy practices, including changes in the use of personal information, to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA106		<p>The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:</p> <ol style="list-style-type: none"> 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.
CA107		<p>Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.</p>
CA110		<p>Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is:</p> <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.
CA119		<p>On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.</p>
CA120		<p>The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.</p>

Privacy Criteria Related to Choice and Consent

P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's

basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

Control Number	Activity	Control Activities
CA111		Zoho’s Privacy Policy includes the below policy around Choice and Consent: 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.
CA112		The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA121		On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of “sensitive” personal information is properly delineated and communicated to personnel.
CA122		Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
CA124		When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).
CA128		The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity’s policies for conformity to the requirement.
CA132		Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.

Privacy Criteria Related to Collection

P3.1: Personal information is collected consistent with the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA106		The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:

Control Number	Activity	Control Activities
		<ol style="list-style-type: none"> 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.
CA113		<p>Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by</p> <ol style="list-style-type: none"> 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
CA122		<p>Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.</p>
CA123		<p>The entity’s application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject’s consent before the data subject submits the information.</p>
CA129		<p>Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary</p>
CA130		<p>Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.</p>

P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA110		<p>Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity’s privacy practices). The notice is:</p> <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject.

Control Number	Activity	Control Activities
		2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.
CA111		Zoho’s Privacy Policy includes the below policy around Choice and Consent: 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.
CA112		The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA120		The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.
CA123		The entity’s application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject’s consent before the data subject submits the information.
CA124		When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).

Privacy Criteria Related to Use, Retention, and Disposal

P4.1: The entity limits the use of personal information to the purposes identified in the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA22		Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.

CA28	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA113	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
CA114	On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.
CA120	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.

P4.2: The entity retains personal information consistent with the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA115		Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies: 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.
CA119		On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal

	information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA131	An annual review of the organization’s data inventory is performed by the Privacy team to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.

P4.3: The entity securely disposes of personal information to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activity
CA96		The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.
CA105		Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.
CA109		The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA119		On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA129		Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary

Privacy Criteria Related to Access

P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity’s objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA104		Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.
CA106		The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:

Control Number	Activity	Control Activities
		<ol style="list-style-type: none"> 1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information 2) Policies regarding retention, sharing, disclosure, and disposal of their personal information 3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information 4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.
CA110		<p>Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is:</p> <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects.
CA111		<p>Zoho's Privacy Policy includes the below policy around Choice and Consent:</p> <ol style="list-style-type: none"> 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.
CA116		<p>The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.</p>
CA118		<p>On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.</p>
CA119		<p>On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.</p>

Control Number	Activity	Control Activities
CA120		The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.
CA125		Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.

P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity’s objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA109		The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA112		The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
CA114		On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.
CA118		On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA119		On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA120		The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.

Privacy Criteria Related to Disclosure and Notification

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA36		A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.
CA120		The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.
CA123		The entity’s application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject’s consent before the data subject submits the information.
CA124		When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).
CA125		Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.
CA130		Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA125		Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.

Control Number	Activity	Control Activities
CA126		On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activity
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA36		A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity’s objectives related to privacy. The entity assesses those parties’ compliance on a periodic and as-needed basis and takes corrective action, if necessary.

Control Number	Activity	Control Activity
CA26		On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA126		On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.
CA127		Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA27		A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA36		A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.
CA118		On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA126		On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activity
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA36		A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.

P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects’ personal information, upon the data subjects’ request, to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA34		Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.
CA116		The Director of Compliance (DOC) established a ‘Subject Access Request Policy’ that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.
CA118		On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
CA125		Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.
CA126		On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.

Privacy Criteria Related to Quality

P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity’s objectives related to privacy.

Control Number	Activity	Control Activities
CA28		On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.
CA109		The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.
CA114		On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in <ol style="list-style-type: none"> 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.

Control Number	Activity	Control Activities
CA115		<p>Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:</p> <ol style="list-style-type: none"> 1) The system processes in place to delete information in accordance with specific retention requirements. 2) Deletion of backup information in accordance with a defined schedule. 3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention. 4) Annually reviews information marked for retention.
CA119		<p>On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.</p>

Privacy Criteria Related to Monitoring and Enforcement

P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity’s objectives related to privacy. Corrections and other necessary actions related to identify deficiencies are made or taken in a timely manner.

Control Number	Activity	Control Activities
CA28		<p>On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.</p>
CA107		<p>Based on the request from customers, Zoho enters into a Master Service Agreements (‘MSA’) with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.</p>
CA114		<p>On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in</p> <ol style="list-style-type: none"> 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.
CA116		<p>The Director of Compliance (DOC) established a ‘Subject Access Request Policy’ that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.</p>
CA118		<p>On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been</p>

Control Number	Activity	Control Activities
		denied and reasons for such denials, as well as any communications regarding challenges.
CA119		On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.
CA124		When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).
CA125		Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.
CA129		Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary

3.11 Complementary User Entity Controls ('CUECs')

The controls at Zoho relating to the Application development, Production Support and the related Information Technology General Controls relevant to the applicable criteria, cover only a portion of the overall internal control structure of User entities. The trust services criteria cannot be achieved without taking into consideration operating effectiveness of controls at the Zoho's User entities. Therefore, User entities' internal control structure must be evaluated in conjunction with Zoho's control policies and procedures, and the results of testing summarized in section 4 of this report.

This section highlights those internal control structure responsibilities that Zoho believes should be present at user entities, and which Zoho have considered in developing its control structure policies and the procedures described in this report. In order to rely on the control structure policies and procedures reported herein, user entities and their auditors must evaluate user entities internal control structure to determine if the Complementary User Entities Controls mentioned below or similar procedures are in place and operating effectively.

The CUECs mentioned below are as explained and provided by Zoho's management. These controls address the interface and communication between User entities and Zoho and are not intended to be a complete listing of the controls related to the applicable criteria of User entities. The CUECs mentioned below are as explained and provided by Zoho management:

- 3.11.1 User entities are responsible for providing and managing the access shared with their associates on Zoho products and also for managing the access to the servers and infrastructure in relation to in-premise products (CA62, CA67 and CA98)
- 3.11.2 User entities are responsible for requesting and approving the Master Service Agreement ('MSA') and the approval for implementation of application on Cloud environment (CA107)
- 3.11.3 User entities are responsible for reviewing respective documents made available by Zoho through the corporate website (CA44 and CA105)
- 3.11.4 User entities are responsible for raising any backup restoration request to Zoho. (CA89)

- 3.11.5 User entities are responsible for communicating any support or security or privacy incidents to Zoho on a timely basis. (CA35, CA39 and CA129)
- 3.11.6 User entities are responsible for reviewing the privacy policy and accepting to the privacy notice of Zoho. (CA110, CA120 and CA123)
- 3.11.7 User entities are responsible for testing and implementation of changes / fixes / patches released by Zoho on a timely basis in their on-premise applications. (CA47)
- 3.11.8 User entities are responsible for implementing network and infrastructure security controls supporting the on-premise applications. (CA55, CA64, CA65, CA73 and CA92)
- 3.11.9 User entities are responsible to download and archive the documentation in relation to logs / activities performed by their customers for the period of 6 years as required in the HIPAA statement as per §164.316(b)(2)(i) (CA133)

These CUECs relate to the specific control activities. However, for the ease of reference and enhanced readability, wherever possible, we have provided the cross reference for these CUECs against the control activities in the subsection 4.3.1

3.12 Vendor v/s Subservice Organization (SSO) Analysis

Zoho utilizes subservice organizations to support complete, accurate and timely processing of client transactions which are identified in table 1 below. Zoho management assesses the risks associated with these subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner. These include, but are not limited to, the review of third-party service auditor reports, holding discussions with subservice organization management, participating on the client advisory committees, and performing periodic assessments of subservice organizations’ facilities, processes, and controls. Additionally, Zoho utilizes certain vendors in performing controls related to its services.

Table 1: Subservice Organizations

Zoho’s controls relating to the Application development, Production Support and the related Information Technology General Controls relevant to the applicable criteria process covers only a portion of overall internal control for each user entity of Zoho. It is not feasible for the criteria related to Application development, Production Support and the related Information Technology General Controls to be achieved solely by Zoho. Therefore, each user entity’s internal control must be evaluated in conjunction with Zoho’s controls and the related tests and results described in section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Name of Subservice Organization	Nature of Services Provided
<ul style="list-style-type: none"> - Sabey Data Center Properties LLC - Databank Holdings Limited - Digital Realty Trust Inc. - Equinix Inc. B.V. - CtrlS Datacenters Limited - Equinix Asia Pacific Pte. Ltd 	Datacenter Co-Location Services
<ul style="list-style-type: none"> - Radware - Computerline 	DDoS Monitoring

Subservice organizations are responsible for defining and implementing CSOCs provided in sub-section 3.12.

- 3.12.1 Subservice organizations are responsible for supporting the physical security and environmental safeguard controls for the datacenters (CA12, CA13, CA14, CA15, CA16, CA17, CA18, CA19, CA20, CA21 and CA136)
- 3.12.2 Subservice organizations are responsible to monitor network of Zoho for DDoS attack (CA73)

Table 2: Vendors

Organizations that provide services to a service organization that are not considered subservice organizations are referred to as vendors. As Zoho’s controls alone are sufficient to meet the needs of user entities’ internal control (that is, achievement of the criteria is not dependent on the vendor’s controls), management has concluded that the entity is not a subservice organization. Zoho uses the vendors in the table below to support the specified functions related to the criteria in section 4 of this report. However, the activities performed by these vendors are not required to meet the assertions specified in the criteria, and as a result, no additional procedures are required to be evaluated related to the activities of these vendors.

Name of Vendor	Description of Services Provided
<ul style="list-style-type: none"> - Powerica - HVAC - Ardelisys Technologies Private Limited - SVE Energy Private Limited - Pinnacle System 	Environmental equipment maintenance
<ul style="list-style-type: none"> - G4S Secure Solutions India Private Limited 	Physical Security Agency for Security Personnel
<ul style="list-style-type: none"> - KPMG - Matrix Business Services India Private Limited - Asurint 	Background Verification Services
<ul style="list-style-type: none"> - Amazon CDN 	Content Delivery Network
<ul style="list-style-type: none"> - Easy Post 	Shipping Services
<ul style="list-style-type: none"> - Google Translate 	Translation Service
<ul style="list-style-type: none"> - Litmus 	Email Marketing Service
<ul style="list-style-type: none"> - Kaleyra - Telnyx 	SMS Service
<ul style="list-style-type: none"> - Tata Communications 	Dialing Service

SECTION - 4

MANAGEMENT OF ZOHO'S
DESCRIPTION OF ITS
RELEVANT CRITERIA AND
RELATED CONTROLS, AND
INDEPENDENT SERVICE
AUDITOR'S DESCRIPTION OF
TESTS OF CONTROLS AND
RESULTS

Section 4: MANAGEMENT OF ZOHOO'S DESCRIPTION OF ITS RELEVANT CRITERIA AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

4.1 Description of testing procedures performed

Deloitte Haskins & Sells LLP performed a variety of tests relating to the controls listed in this section throughout the period from December 01, 2022 through November 30, 2023. Our tests of controls were performed on controls as they existed during the period of December 01, 2022 through November 30, 2023 and were applied to those controls specified by Zoho.

In determining the nature, timing, and extent of tests, we considered (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, we ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.

Test	Description
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity, independently reperformed the procedures, and compared any discrepancies identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

4.2 Reliability of information produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information in response to ad hoc requests from the service auditor (e.g., population lists), and (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included procedures to address (a) the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by the Service Organization.

4.3 Reporting on results of testing

The concept of materiality is not applied when reporting the results of control tests because Deloitte Haskins & Sells LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte Haskins & Sells LLP reports all exceptions.

4.3.1 Controls with Trust Services Criteria and HIPAA Mapping

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA01	Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.	CC1.1	§164.308(a)(1)(ii)(C)	§164.308(a)(2)
		CC1.2	§164.308(a)(3)(i)	§164.316(b)(2)(ii)
		CC1.3	§164.412	§164.316(b)(2)(iii)
		CC1.5	§164.308(a)(1)(i)	§164.410(a)
		CC2.1		
CA02	Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.	CC1.3	§164.412	§164.308(a)(5)(i)
		CC1.4	§164.308(a)(2)	§164.308(a)(5)(ii)(A)
		CC1.5	§164.316(b)(2)(ii)	§164.308(a)(6)(i)
		CC2.2	§164.316(b)(2)(iii)	§164.308(a)(6)(ii)
			§164.308(a)(1)(i)	§164.410(a)
CA03	Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates	CC1.4	§164.308(a)(1)(i)	§164.410(a)
		CC2.2	§164.308(a)(5)(i)	§164.310(a)(2)(iv)
		CC5.3	§164.308(a)(5)(ii)(A)	§164.310(d)(1)
			§164.308(a)(6)(i)	§164.310(d)(2)(ii)
			§164.308(a)(6)(ii)	
CA04	Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.	CC1.1	§164.308(a)(1)(ii)(C)	
		CC1.4	§164.308(a)(3)(i)	
CA05	Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis. The	CC1.1	§164.308(a)(1)(ii)(C)	§164.316(b)(2)(ii)
		CC1.4	§164.308(a)(3)(i)	§164.316(b)(2)(iii)
		CC1.5	§164.308(a)(1)(i)	§164.410(a)
			§164.308(a)(2)	

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	document is made available in the HRMS (Zoho People) to the associates		
CA06	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.	CC1.1 CC1.4 CC1.5	§164.308(a)(1)(ii)(C) §164.308(a)(3)(i) §164.308(a)(1)(i) §164.308(a)(2)
CA07	Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.	CC1.1 CC2.2 CC2.3 CC3.1	§164.308(a)(1)(ii)(C) §164.308(a)(3)(i) §164.410(a) §164.308(a)(1)(i) §164.308(a)(5)(i)
CA08	Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.	CC1.1 CC1.4 CC2.2	§164.308(a)(1)(ii)(C) §164.308(a)(3)(i) §164.308(a)(1)(i) §164.308(a)(5)(i)
CA09	Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.	CC1.1 CC1.4 CC2.2 C1.1	§164.308(a)(1)(ii)(C) §164.308(a)(3)(i) §164.308(a)(1)(i) §164.308(a)(5)(i)
CA10	Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.	CC1.1 CC1.4 CC2.1 CC2.2 C1.1	§164.308(a)(1)(ii)(C) §164.308(a)(3)(i) §164.308(a)(1)(i) §164.308(a)(5)(i)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA11	Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.	CC5.3	§164.310(d)(1)	§164.310(a)(2)(iv)
		CC6.4	§164.310(d)(2)(ii)	§164.310(b)
		A1.2	§164.308(a)(3)(i)	§164.310(c)
			§164.308(a)(3)(ii)(A)	§164.310(d)(2)(iii)
			§164.308(a)(3)(ii)(B)	§164.308(a)(1)(ii)(A)
			§164.308(a)(3)(ii)(C)	§164.308(a)(7)(i)
			§164.308(a)(4)(i)	§164.308(a)(7)(ii)(A)
			§164.308(a)(4)(ii)(B)	§164.308(a)(7)(ii)(B)
			§164.308(a)(4)(ii)(C)	§164.308(a)(7)(ii)(C)
			§164.308(a)(7)(ii)(E)	§164.308(a)(7)(ii)(D)
			§164.310(a)(1)	§164.310(a)(2)(i)
	§164.310(a)(2)(ii)	§164.310(d)(2)(iv)		
	§164.310(a)(2)(iii)			
CA12	For associates joining Zoho, the HR team creates a request for providing physical access card and the same is actioned upon by the Physical Security team. The access cards are distinguished based on the color of the tags described in the HR process document.	CC6.4	§164.308(a)(3)(i)	§164.308(a)(7)(ii)(E)
			§164.308(a)(3)(ii)(A)	§164.310(a)(1)
			§164.308(a)(3)(ii)(B)	§164.310(a)(2)(ii)
			§164.308(a)(3)(ii)(C)	§164.310(a)(2)(iii)
			§164.308(a)(4)(i)	§164.310(a)(2)(iv)
			§164.308(a)(4)(ii)(B)	§164.310(b)
			§164.308(a)(4)(ii)(C)	§164.310(c)
	§164.308(a)(7)(i)	§164.310(d)(2)(iii)		
CA13	In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team deactivates the old access card and issues a new access card.	CC6.4	§164.308(a)(3)(i)	§164.308(a)(7)(ii)(E)
			§164.308(a)(3)(ii)(A)	§164.310(a)(1)
			§164.308(a)(3)(ii)(B)	§164.310(a)(2)(ii)
			§164.308(a)(3)(ii)(C)	§164.310(a)(2)(iii)
			§164.308(a)(4)(i)	§164.310(a)(2)(iv)
			§164.308(a)(4)(ii)(B)	§164.310(b)
			§164.308(a)(4)(ii)(C)	§164.310(c)
	§164.308(a)(7)(i)	§164.310(d)(2)(iii)		
CA14	For associates leaving Zoho, the HR team creates a request for revoking physical access card and the same	CC6.4	§164.308(a)(3)(i)	§164.308(a)(7)(ii)(E)
			§164.308(a)(3)(ii)(A)	§164.310(a)(1)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
	is actioned upon by the Physical Security team on the last working day.		§164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(7)(i)	§164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(a)(2)(iv) §164.310(b) §164.310(c) §164.310(d)(2)(iii)
CA15	Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.	CC6.4 CC6.5	§164.308(a)(7)(i) §164.308(a)(7)(ii)(E) §164.310(a)(2)(iv) §164.310(d)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B)	§164.308(a)(4)(ii)(C) §164.310(a)(1) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(b) §164.310(c) §164.310(d)(2)(ii) §164.312(a)(1) §164.312(d)
CA16	Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.	CC6.4	§164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(7)(i)	§164.308(a)(7)(ii)(E) §164.310(a)(1) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(a)(2)(iv) §164.310(b) §164.310(c) §164.310(d)(2)(iii)
CA17	Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities.	CC6.4 CC6.5 CC9.2	§164.308(a)(7)(i) §164.308(a)(7)(ii)(E) §164.310(a)(2)(iv) §164.310(d)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B)	§164.310(d)(2)(ii) §164.312(a)(1) §164.312(d) §164.308(a)(1)(ii)(A) §164.308(b)(1) §164.308(b)(2) §164.308(b)(3)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
			§164.310(a)(1)
			§164.310(a)(2)(ii)
			§164.310(a)(2)(iii)
			§164.310(b)
			§164.310(c)
CA18	Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.	CC6.4 CC6.5 A1.2	§164.308(a)(7)(ii)(E) §164.310(a)(2)(iv) §164.310(d)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.310(a)(1) §164.310(a)(2)(ii) §164.310(a)(2)(iii)
CA19	Environmental safeguards are installed in Zoho facilities comprising of the following: <ul style="list-style-type: none"> • Cooling Systems • UPS with Battery and diesel generator back-up • Smoke detectors • Water sprinklers • Fire resistant floors 	A1.2	§164.308(a)(1)(ii)(A) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
	<ul style="list-style-type: none"> • Fire extinguisher 			
CA20	Planned Preventive Maintenance (PPM) is performed on a periodic basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.	A1.2	§164.308(a)(1)(ii)(A) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B)	§164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.310(a)(2)(i) §164.310(d)(2)(iv)
CA21	Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.	A1.2	§164.308(a)(1)(ii)(A) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B)	§164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.310(a)(2)(i) §164.310(d)(2)(iv)
CA22	Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.	CC1.1 CC1.2 CC1.3 CC1.5 CC2.1 CC2.2 CC2.3 CC3.1 CC4.1 CC5.1 CC5.2 CC5.3 CC6.1 CC6.2 CC6.3 CC7.4 CC9.1 P4.1	§164.308(a)(2) §164.410(a) §164.308(a)(5)(i) §164.308(a)(5)(ii)(A) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E) §164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(a)(2)(iv) §164.310(d)(1) §164.310(d)(2)(ii) §164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii)	§164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(1) §164.312(c)(1) §164.312(c)(2) §164.312(d) §164.308(a)(1)(i) §164.308(a)(1)(ii)(D) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.308(a)(7)(i) §164.308(a)(8) §164.308(a)(1)(ii)(A) §164.316(a) "§164.316(b)(1) (b)(1)(i)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.310(c)
			(b)(1)(ii)"
			§164.312(a)(2)(i)
			§164.502(a)(5)(ii)
			§164.312(a)(2)(ii)
			§164.310(d)(2)(i)
			§164.312(a)(2)(iii)
			§164.308(a)(1)(ii)(C)
			§164.312(e)(2)(i)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
			§164.412
			§164.308(a)(3)(ii)(B)
CA23	Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.	CC1.2	§164.308(a)(2)
		CC1.5	§164.308(a)(5)(i)
		CC2.2	§164.308(a)(5)(ii)(A)
		CC3.1	§164.308(a)(6)(i)
		CC3.2	§164.308(a)(6)(ii)
		CC3.3	§164.410(a)
		CC4.1	§164.312(b)
		CC5.1	§164.308(a)(8)
		CC5.3	§164.306
		CC6.7	§164.308(a)(1)(i)
		CC9.1	§164.308(a)(1)(ii)(B)
		CC9.2	§164.316(b)(2)(ii)
		A1.1	§164.316(b)(2)(iii)
		A1.2	§164.310(a)(2)(iv)
			§164.310(b)
			§164.310(c)
			§164.310(d)(1)
			§164.310(d)(2)(ii)
			§164.308(a)(7)(ii)(A)
			§164.308(a)(7)(ii)(B)
			§164.308(a)(7)(ii)(C)
			§164.312(a)(1)
			§164.308(a)(7)(ii)(D)
			§164.312(a)(2)(iv)
			§164.310(a)(2)(i)
			§164.312(e)(1)
			§164.310(d)(2)(iv)
			§164.312(e)(2)(i)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA24	Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis	CC3.2	§164.308(a)(1)(ii)(C)	§164.310(d)(2)(iv)
		CC7.2	§164.312(b)	§164.308(a)(7)(i)
		CC7.3	§164.312(c)(1)	§164.308(a)(7)(ii)(A)
		CC7.4	§164.308(a)(1)(i)	§164.308(a)(7)(ii)(B)
		A1.2	§164.308(a)(1)(ii)(D)	§164.308(a)(7)(ii)(C)
		A1.3	§164.308(a)(6)(i)	§164.308(a)(7)(ii)(D)
			§164.308(a)(6)(ii)	§164.308(a)(7)(ii)(E)
			§164.308(a)(8)	§164.310(a)(2)(i)
		§164.308(a)(1)(ii)(A)	§164.312(a)(2)(ii)	
CA25	Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.	CC1.3	§164.412	§164.308(a)(7)(ii)(D)
		CC1.5	§164.308(a)(2)	§164.308(a)(7)(ii)(E)
		CC2.1	§164.308(a)(5)(i)	"§164.316(b)(2)
		CC2.2	§164.308(a)(5)(ii)(A)	(b)(2)(i)"
		CC4.1	§164.308(a)(6)(i)	§164.316(b)(2)(ii)
		CC5.1	§164.308(a)(6)(ii)	§164.316(b)(2)(iii)
		CC9.1	§164.410(a)	§164.308(a)(1)(ii)(A)
			§164.308(a)(8)	§164.316(a)
			§164.306	"§164.316(b)(1) (b)(1)(i)(b)(1)(ii)"
			§164.308(a)(1)(i)	
		§164.308(a)(1)(ii)(B)		
		§164.308(a)(7)(ii)(C)		
CA26	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.	CC1.2	§164.308(a)(2)	§164.308(a)(3)(ii)(B)
		CC1.5	§164.316(b)(2)(ii)	§164.308(a)(3)(ii)(C)
		CC2.1	§164.316(b)(2)(iii)	§164.308(a)(4)(i)
		CC2.2	§164.308(a)(1)(i)	§164.308(a)(4)(ii)(B)
		CC3.1	§164.308(a)(5)(i)	§164.308(a)(4)(ii)(C)
		CC3.2	§164.308(a)(5)(ii)(A)	§164.310(a)(1)
		CC4.1	§164.308(a)(6)(i)	§164.310(a)(2)(ii)
		CC6.5	§164.308(a)(6)(ii)	§164.310(a)(2)(iii)
		P6.4	§164.410(a)	§164.310(b)
			§164.312(b)	§164.310(c)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.310(d)(2)(ii)
			§164.312(a)(1)
			§164.312(d)
			§164.308(a)(1)(ii)(A)
			§164.308(a)(8)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
CA27	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	CC2.3	§164.308(a)(1)(i)
		CC3.3	§164.308(a)(5)(i)
		CC4.1	§164.308(a)(5)(ii)(A)
		CC9.2	§164.308(a)(6)(i)
		C1.1	§164.308(a)(6)(ii)
		P6.1	§164.308(a)(8)
		P6.4	§164.308(a)(1)(ii)(A)
		P6.5	§164.308(b)(1)
			§164.308(b)(2)
			§164.308(b)(3)
			§164.314(a)(1)
			§164.314(a)(2)(iii)
CA28	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.	CC1.2	§164.308(a)(2)
		CC1.3	§164.308(a)(5)(i)
		CC2.1	§164.308(a)(5)(ii)(A)
		CC2.2	§164.308(a)(6)(i)
		CC3.2	§164.308(a)(6)(ii)
		CC3.3	§164.410(a)
		CC4.1	§164.308(a)(8)
		CC4.2	§164.306
		CC5.1	§164.308(a)(1)(i)
		CC5.3	§164.308(a)(1)(ii)(B)
		CC9.1	§164.308(a)(7)(ii)(C)
		P4.1	§164.308(a)(7)(ii)(D)
		P4.2	§164.308(a)(7)(ii)(E)
		P7.1	
		P8.1	
			§164.316(a)
			"§164.316(b)(1)
			(b)(1)(i)
			(b)(1)(ii)"
			"§164.316(b)(2)
			(b)(2)(i)"
			§164.502(a)(5)(ii)
			§164.502(a)(3) and (4)
			§164.502(b)
			§164.502(e)
			§164.502(j)
			"§164.316(b)(2)
			(b)(2)(i)"
			§164.316(b)(2)(ii)
			§164.316(b)(2)(iii)
			§164.308(a)(1)(ii)(A)
			§164.316(a)
			"§164.316(b)(1)
			(b)(1)(i)
			(b)(1)(ii)"
			§164.502(a)(5)(ii)
			§164.310(d)(2)(i)
			§164.310(d)(2)(ii)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA29	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.	CC1.2	§164.308(a)(2)	§164.312(b)
		CC1.3	§164.410(a)	§164.312(c)(1)
		CC1.5	§164.308(a)(5)(i)	§164.308(b)(1)
		CC2.1	§164.308(a)(5)(ii)(A)	§164.308(b)(2)
		CC2.2	§164.306	§164.308(b)(3)
		CC2.3	§164.308(a)(1)(ii)(B)	§164.314(a)(1)
		CC3.1	§164.316(b)(2)(ii)	§164.314(a)(2)(iii)
		CC3.2	§164.316(b)(2)(iii)	§164.316(a)
		CC3.3	§164.310(a)(2)(iv)	"§164.316(b)(1)
		CC3.4	§164.310(d)(1)	(b)(1)(i)
		CC4.1	§164.310(d)(2)(ii)	(b)(1)(ii)"
		CC4.2	§164.308(a)(1)(i)	"§164.316(b)(2)
		CC5.1	§164.308(a)(1)(ii)(C)	(b)(2)(i)"
		CC5.3	§164.308(a)(1)(ii)(D)	§164.308(a)(1)(ii)(A)
		CC7.3	§164.308(a)(6)(i)	§164.308(a)(7)(ii)(C)
CC9.1	§164.308(a)(6)(ii)	§164.308(a)(7)(ii)(D)		
CC9.2	§164.308(a)(7)(i)	§164.308(a)(7)(ii)(E)		
		A1.1	§164.308(a)(8)	§164.312(a)(2)(ii)
CA30	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.	CC1.1	§164.308(a)(1)(ii)(C)	§164.308(a)(1)(ii)(B)
		CC1.2	§164.308(a)(3)(i)	§164.308(a)(7)(ii)(C)
		CC1.3	§164.412	§164.308(a)(7)(ii)(D)
		CC1.5	§164.308(a)(2)	§164.308(a)(7)(ii)(E)
		CC2.1	§164.410(a)	"§164.316(b)(1)
		CC2.2	§164.308(a)(5)(i)	(b)(1)(i)
		CC2.3	§164.308(a)(5)(ii)(A)	(b)(1)(ii)"
		CC3.1	§164.308(a)(6)(i)	"§164.316(b)(2)
		CC3.2	§164.308(a)(6)(ii)	(b)(2)(i)"
		CC3.3	§164.312(b)	§164.316(b)(2)(ii)
		CC3.4	§164.308(a)(8)	§164.316(b)(2)(iii)
		CC4.1	§164.306	§164.310(a)(2)(iv)
		CC5.1	§164.308(a)(1)(i)	§164.310(d)(1)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
		CC5.3	§164.308(a)(1)(ii)(A)	§164.310(d)(2)(ii)
CA31	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.	CC1.1	§164.308(a)(1)(ii)(C)	§164.316(b)(2)(ii)
		CC1.2	§164.308(a)(3)(i)	§164.316(b)(2)(iii)
		CC1.3	§164.412	§164.410(a)
		CC1.5	§164.308(a)(1)(i)	§164.308(a)(1)(ii)(A)
		CC4.2	§164.308(a)(2)	§164.308(a)(8)
CA32	On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.	CC1.2	§164.308(a)(8)	§164.312(b)
		CC2.1	§164.306	§164.308(a)(1)(ii)(A)
		CC3.1	§164.308(a)(1)(i)	§164.308(b)(1)
		CC4.2	§164.308(a)(1)(ii)(B)	§164.308(b)(2)
		CC5.1	§164.316(b)(2)(ii)	§164.308(b)(3)
		CC5.3	§164.316(b)(2)(iii)	§164.314(a)(1)
		CC7.2	§164.310(a)(2)(iv)	§164.314(a)(2)(iii)
		CC9.1	§164.310(d)(1)	§164.316(a)
		CC9.2	§164.310(d)(2)(ii)	"§164.316(b)(1)
			§164.308(a)(1)(ii)(D)	(b)(1)(i)
			§164.308(a)(7)(i)	(b)(1)(ii)"
			§164.308(a)(7)(ii)(C)	"§164.316(b)(2)(b)(2)(i)"
			§164.308(a)(7)(ii)(D)	
			§164.308(a)(7)(ii)(E)	
CA33	Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.	CC2.2	§164.308(a)(5)(i)	§164.308(a)(8)
		CC3.1	§164.308(a)(5)(ii)(A)	§164.312(c)(1)
		CC3.2	§164.410(a)	§164.308(a)(1)(i)
		CC3.3	§164.308(a)(1)(ii)(A)	§164.308(a)(1)(ii)(D)
		CC4.1	§164.310(a)(2)(iv)	§164.308(a)(6)(i)
		CC4.2	§164.310(d)(1)	§164.308(a)(6)(ii)
		CC5.3	§164.310(d)(2)(ii)	§164.308(a)(7)(i)
		CC7.3	§164.308(a)(1)(ii)(C)	§164.312(b)
		CC7.5		

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA34	Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.	CC7.3	§164.308(a)(1)(ii)(C)	§164.312(b)
		CC7.4	§164.312(c)(1)	§164.502(a)(5)(ii)
		CC7.5	§164.308(a)(8)	§164.502(a)(3) and (4)
		P6.1	§164.308(a)(1)(i)	§164.410(a)
		P6.3	§164.308(a)(1)(ii)(D)	§164.502(b)
		P6.4	§164.308(a)(6)(i)	§164.502(e)
		P6.5	§164.308(a)(6)(ii)	§164.502(j)
		P6.6	§164.308(a)(7)(i)	
CA35	Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.	CC2.2	§164.410(a)	§164.308(a)(1)(i)
		CC2.3	§164.308(a)(5)(i)	§164.308(a)(1)(ii)(D)
		CC3.1	§164.308(a)(5)(ii)(A)	§164.308(a)(6)(i)
		CC4.1	§164.308(a)(1)(ii)(A)	§164.308(a)(6)(ii)
		CC7.3	§164.308(a)(1)(ii)(C)	§164.308(a)(7)(i)
		CC7.4	§164.312(c)(1)	§164.312(b)
CA36	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.	CC7.5	§164.308(a)(8)	
		P6.1	§164.502(a)(5)(ii)	§164.502(b)
		P6.3	§164.502(a)(3) and (4)	§164.502(e)
		P6.5	§164.410(a)	§164.502(j)
		P6.6		
CA37	An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.	P6.1	§164.502(a)(5)(ii)	§164.502(b)
		P6.3	§164.502(a)(3) and (4)	§164.502(e)
		P6.5	§164.410(a)	§164.502(j)
		P6.6		
		CC2.2	§164.410(a)	§164.308(a)(1)(i)
		CC2.3	§164.308(a)(5)(i)	§164.308(a)(1)(ii)(D)
		CC3.1	§164.308(a)(5)(ii)(A)	§164.308(a)(6)(i)
		CC4.1	§164.308(a)(1)(ii)(A)	§164.308(a)(6)(ii)
CC4.2	§164.308(a)(1)(ii)(C)	§164.308(a)(7)(i)		
CC7.3	§164.312(c)(1)	§164.312(b)		
CC7.4	§164.308(a)(8)			
CC7.5				

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA38	Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.	CC2.3	§164.308(a)(1)(i)	§164.308(a)(5)(ii)(C)
		CC5.3	§164.308(a)(5)(i)	§164.308(a)(5)(ii)(D)
		CC6.3	§164.308(a)(5)(ii)(A)	§164.312(a)(1)
		PI1.1	§164.308(a)(6)(i)	§164.312(c)(2)
		PI1.2	§164.308(a)(6)(ii)	§164.312(d)
		PI1.3	§164.310(a)(2)(iv)	§164.312(c)(1)
		A1.2	§164.310(d)(1)	§164.308(a)(1)(ii)(A)
			§164.310(d)(2)(ii)	§164.308(a)(7)(i)
			§164.308(a)(3)(i)	§164.308(a)(7)(ii)(A)
			§164.308(a)(3)(ii)(A)	§164.308(a)(7)(ii)(B)
			§164.308(a)(3)(ii)(B)	§164.308(a)(7)(ii)(C)
			§164.308(a)(3)(ii)(C)	§164.308(a)(7)(ii)(D)
			§164.308(a)(4)(i)	§164.310(a)(2)(i)
§164.308(a)(4)(ii)(B)	§164.310(d)(2)(iv)			
§164.308(a)(4)(ii)(C)				
CA 39	Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.	CC2.3	§164.308(a)(1)(i)	§164.308(a)(7)(i)
		PI1.1	§164.308(a)(5)(i)	§164.308(a)(7)(ii)(A)
		PI1.3	§164.308(a)(5)(ii)(A)	§164.308(a)(7)(ii)(B)
		A1.2	§164.308(a)(6)(i)	§164.308(a)(7)(ii)(C)
			§164.308(a)(6)(ii)	§164.308(a)(7)(ii)(D)
			§164.312(c)(1)	§164.310(a)(2)(i)
§164.308(a)(1)(ii)(A)	§164.310(d)(2)(iv)			
CA40	Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master - Project Manager on an annual basis.	CC2.2	§164.308(a)(5)(i)	§164.310(d)(2)(ii)
		CC3.4	§164.308(a)(5)(ii)(A)	§164.308(a)(1)(i)
		CC5.3	§164.308(a)(6)(i)	§164.308(a)(7)(i)
		CC8.1	§164.308(a)(6)(ii)	§164.308(a)(8)
		PI1.3	§164.410(a)	§164.312(a)(1)
			§164.310(a)(2)(iv)	§164.312(c)(1)
			§164.310(d)(1)	

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA41	Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.	CC3.4	§164.306	§164.316(b)(2)(ii)
		CC5.1	§164.308(a)(1)(ii)(A)	§164.316(b)(2)(iii)
		CC5.3	§164.308(a)(1)(ii)(B)	§164.310(a)(2)(iv)
		CC8.1	§164.308(a)(7)(ii)(C)	§164.310(d)(1)
		PI1.3	§164.308(a)(7)(ii)(D)	§164.310(d)(2)(ii)
			§164.308(a)(7)(ii)(E)	§164.308(a)(1)(i)
			"§164.316(b)(1)	§164.308(a)(7)(i)
			(b)(1)(i)	§164.308(a)(8)
			(b)(1)(ii)"	§164.312(a)(1)
			"§164.316(b)(2)	§164.312(c)(1)
CA42	Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.	CC1.4	§164.308(a)(1)(i)	§164.308(a)(5)(ii)(D)
		CC2.1	§164.308(a)(5)(i)	"§164.316(b)(1)
		CC2.2	§164.308(a)(5)(ii)(A)	(b)(1)(i)
		CC5.2	§164.308(a)(6)(i)	(b)(1)(ii)"
		PI1.3	§164.308(a)(6)(ii)	"§164.316(b)(2)
			§164.410(a)	(b)(2)(i)"
			§164.306	§164.316(b)(2)(ii)
			§164.308(a)(1)(ii)(A)	§164.316(b)(2)(iii)
			§164.308(a)(1)(ii)(B)	§164.312(c)(1)
			§164.308(a)(5)(ii)(C)	
CA43	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.	CC2.2	§164.308(a)(1)(i)	§164.308(a)(5)(ii)(D)
		CC3.1	§164.308(a)(5)(i)	"§164.316(b)(1)
		CC5.2	§164.308(a)(5)(ii)(A)	(b)(1)(i)
		CC7.1	§164.308(a)(6)(i)	(b)(1)(ii)"
		PI1.3	§164.308(a)(6)(ii)	"§164.316(b)(2)
			§164.410(a)	(b)(2)(i)"
			§164.306	§164.316(b)(2)(ii)
			§164.308(a)(1)(ii)(A)	§164.316(b)(2)(iii)
			§164.308(a)(1)(ii)(B)	§164.312(b)
			§164.308(a)(5)(ii)(C)	§164.312(c)(1)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA44	Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.	CC5.2	§164.306	(b)(1)(i)
		PI1.1	§164.308(a)(1)(ii)(A)	(b)(1)(ii)"
		PI1.2	§164.308(a)(1)(ii)(B)	"§164.316(b)(2)
			§164.308(a)(5)(ii)(C)	(b)(2)(i)"
			§164.308(a)(5)(ii)(D)	§164.316(b)(2)(ii)
	"§164.316(b)(1)	§164.316(b)(2)(iii)		
CA45	Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.	CC5.1	§164.306	"§164.316(b)(2)
		CC8.1	§164.308(a)(1)(ii)(A)	(b)(2)(i)"
		PI1.3	§164.308(a)(1)(ii)(B)	§164.316(b)(2)(ii)
			§164.308(a)(7)(ii)(C)	§164.316(b)(2)(iii)
			§164.308(a)(7)(ii)(D)	§164.308(a)(1)(i)
			§164.308(a)(7)(ii)(E)	§164.308(a)(7)(i)
			"§164.316(b)(1)	§164.308(a)(8)
			(b)(1)(i)	§164.312(a)(1)
(b)(1)(ii)"	§164.312(c)(1)			
CA46	The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.	CC3.4	§164.308(a)(7)(ii)(C)	(b)(1)(ii)"
		CC5.1	§164.308(a)(7)(ii)(D)	"§164.316(b)(2)
		CC5.2	§164.308(a)(7)(ii)(E)	(b)(2)(i)"
		CC7.1	§164.306	§164.316(b)(2)(ii)
		CC8.1	§164.308(a)(1)(ii)(A)	§164.316(b)(2)(iii)
		PI1.2	§164.308(a)(1)(ii)(B)	§164.312(b)
			§164.308(a)(5)(ii)(C)	§164.308(a)(1)(i)
			§164.308(a)(5)(ii)(D)	§164.308(a)(7)(i)
			"§164.316(b)(1)	§164.308(a)(8)
			(b)(1)(i)	§164.312(a)(1)
CA47	The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On	CC3.4	§164.308(a)(7)(ii)(C)	(b)(1)(ii)"
		CC5.1	§164.308(a)(7)(ii)(D)	"§164.316(b)(2)
		CC5.2	§164.308(a)(7)(ii)(E)	(b)(2)(i)"
		CC7.1	§164.306	§164.316(b)(2)(ii)
		CC8.1	§164.308(a)(1)(ii)(A)	§164.316(b)(2)(iii)
		PI1.2	§164.308(a)(1)(ii)(B)	§164.312(b)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	resolution, a sign-off is provided and then the code is deployed in the production environment.		§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) "§164.316(b)(1) (b)(1)(i)
CA48	Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.	PI1.2	-
CA49	Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager - IT Services on an annual basis.	CC3.1 CC3.4 CC5.1 CC6.6 CC6.7 CC7.1 CC7.2	§164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.308(a)(1)(i) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(d)
CA50	Access to support admin portal of Zoho products are defined through IAM. Zoho support admin access is	PI1.2	-

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	provisioned by the IAM team after obtaining approval from authorized personnel.		
CA51	Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.	CC2.1 CC3.3 CC3.4 CC6.1 CC6.8 A1.1	§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.310(b) §164.312(a)(1) §164.312(a)(2)(i) §164.312(a)(2)(iii) §164.312(a)(2)(iv) §164.312(b) §164.312(c)(1) §164.312(c)(2)
CA52	For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.	CC5.2 CC6.1 CC6.2	§164.306 §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B) "§164.316(b)(1)(b)(1)(i) (b)(1)(ii)" "§164.316(b)(2)(b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A)
CA53	For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then	CC5.2 CC6.1	§164.306 §164.308(a)(1)(ii)(A)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
	creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.	CC6.2	§164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A)	§164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.310(c) §164.312(a)(1) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(c)(1) §164.312(c)(2) §164.312(d) §164.312(e)(2)(i)
CA54	Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.	CC4.1 CC5.1 CC5.2 CC6.6 CC6.8 CC7.1 CC7.2 CC7.3	§164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C)	§164.312(a)(1) §164.312(d) §164.312(e)(1) §164.312(e)(2)(i) §164.308(a)(5)(ii)(B) §164.308(a)(1)(ii)(A) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E) §164.308(a)(1)(i) §164.308(a)(1)(ii)(C) §164.308(a)(1)(ii)(D) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.308(a)(7)(i) §164.308(a)(8)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(b) §164.312(c)(1)
CA55	Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.	CC6.8 CC7.1 CC7.3	§164.308(a)(5)(ii)(B) §164.308(a)(1)(i) §164.308(a)(1)(ii)(C) §164.308(a)(1)(ii)(D) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.308(a)(7)(i) §164.308(a)(8) §164.312(b) §164.312(c)(1)
CA56	Authentication of users to Zoho products are governed through IAM through which the password configuration including password complexity and lockout is enforced.	PI1.2	-
CA57	User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner.	CC6.1 CC6.2 CC6.3	§164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D) §164.310(c) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(e)(2)(i) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(1) §164.312(c)(1) §164.312(c)(2) §164.312(d)
CA58	Zoho Encryption at rest team has defined EAR policy which specifies the procedure for encryption and key management. The document is reviewed by EAR Team Lead and approved by Security – Manager on an annual basis.	CC6.1 CC6.2	§164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.310(c) §164.312(a)(1) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(a)(3)(i) §164.312(a)(3)(ii)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
CA59	Zoho uses in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services. Access to KMS server is restricted. Access to KMS is provided by authorized personnel based on approval from Manager in KMS team.	CC6.1	§164.310(b)
		CC6.2	§164.312(a)(2)(iv)
			§164.312(b)
			§164.312(e)(2)(ii)
			§164.308(a)(1)(ii)(D)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
CA60	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.	CC6.1	§164.310(b)
		CC6.2	§164.312(a)(2)(iv)
		PI1.5	§164.312(b)
			§164.312(e)(2)(ii)
			§164.308(a)(1)(ii)(D)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA61	Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks.	CC6.1	§164.310(b)	§164.308(a)(5)(ii)(C)
		CC6.2	§164.312(a)(2)(iv)	§164.308(a)(5)(ii)(D)
			§164.312(b)	§164.310(c)
			§164.312(e)(2)(ii)	§164.312(a)(1)
			§164.308(a)(1)(ii)(D)	§164.312(a)(2)(i)
			§164.308(a)(3)(i)	§164.312(a)(2)(ii)
			§164.308(a)(3)(ii)(A)	§164.312(a)(2)(iii)
			§164.308(a)(3)(ii)(B)	§164.312(c)(1)
			§164.308(a)(3)(ii)(C)	§164.312(c)(2)
			§164.308(a)(4)(i)	§164.312(d)
			§164.308(a)(4)(ii)(B)	§164.312(e)(2)(i)
			§164.308(a)(4)(ii)(C)	
		CA62	Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.	CC5.2
CC6.1	§164.308(a)(1)(ii)(A)			§164.312(c)(1)
CC6.2	§164.308(a)(1)(ii)(B)			§164.312(c)(2)
CC6.3	"§164.316(b)(1)			§164.308(a)(1)(i)
CC6.6	(b)(1)(i)			§164.308(a)(3)(i)
	(b)(1)(ii)"			§164.308(a)(3)(ii)(A)
	"§164.316(b)(2)			§164.308(a)(3)(ii)(B)
	(b)(2)(i)"			§164.308(a)(3)(ii)(C)
	§164.316(b)(2)(ii)			§164.308(a)(4)(i)
	§164.316(b)(2)(iii)			§164.308(a)(4)(ii)(B)
	§164.310(b)			§164.308(a)(4)(ii)(C)
	§164.312(a)(2)(iv)			§164.308(a)(5)(ii)(C)
	§164.312(b)			§164.308(a)(5)(ii)(D)
	§164.312(e)(2)(ii)			§164.312(a)(1)
	§164.308(a)(1)(ii)(D)			§164.312(d)
	§164.310(c)			§164.312(e)(1)
	§164.312(a)(2)(i)	§164.312(e)(2)(i)		
	§164.312(a)(2)(ii)			

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA63	Zoho associates are required to use two factor authentication to connect to IDC infrastructure.	CC5.2	§164.306	§164.312(a)(2)(iii)
		CC6.1	§164.308(a)(1)(ii)(A)	§164.312(c)(1)
		CC6.2	§164.308(a)(1)(ii)(B)	§164.312(c)(2)
		CC6.3	"§164.316(b)(1)	§164.308(a)(1)(i)
		CC6.6	(b)(1)(i)	§164.308(a)(3)(i)
			(b)(1)(ii)"	§164.308(a)(3)(ii)(A)
			"§164.316(b)(2)	§164.308(a)(3)(ii)(B)
			(b)(2)(i)"	§164.308(a)(3)(ii)(C)
			§164.316(b)(2)(ii)	§164.308(a)(4)(i)
			§164.316(b)(2)(iii)	§164.308(a)(4)(ii)(B)
			§164.310(b)	§164.308(a)(4)(ii)(C)
			§164.312(a)(2)(iv)	§164.308(a)(5)(ii)(C)
			§164.312(b)	§164.308(a)(5)(ii)(D)
			§164.312(e)(2)(ii)	§164.312(a)(1)
			§164.308(a)(1)(ii)(D)	§164.312(d)
	§164.310(c)	§164.312(e)(1)		
	§164.312(a)(2)(i)	§164.312(e)(2)(i)		
	§164.312(a)(2)(ii)			
CA64	On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.	CC3.2	§164.306	§164.312(d)
		CC3.3	§164.308(a)(1)(ii)(B)	§164.312(e)(1)
		CC4.2	"§164.316(b)(1)	§164.312(e)(2)(i)
		CC5.1	(b)(1)(i)	§164.308(a)(5)(ii)(B)
		CC6.6	(b)(1)(ii)"	§164.308(a)(1)(ii)(C)
		CC6.8	"§164.316(b)(2)	§164.312(b)
		CC7.1	(b)(2)(i)"	§164.312(c)(1)
		CC7.2	§164.316(b)(2)(ii)	§164.308(a)(1)(i)
		CC7.3	§164.316(b)(2)(iii)	§164.308(a)(1)(ii)(D)
		CC7.4	§164.308(a)(3)(i)	§164.308(a)(6)(i)
		A1.1	§164.308(a)(3)(ii)(A)	§164.308(a)(6)(ii)
			§164.308(a)(3)(ii)(B)	§164.308(a)(7)(i)
			§164.308(a)(3)(ii)(C)	§164.308(a)(8)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
			§164.308(a)(5)(ii)(C)
			§164.308(a)(5)(ii)(D)
			§164.312(a)(2)(ii)
			§164.312(a)(1)
CA65	On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken	CC3.2	§164.306
		CC3.3	§164.308(a)(1)(ii)(B)
		CC4.2	"§164.316(b)(1)
		CC5.1	(b)(1)(i)
		CC6.6	(b)(1)(ii)"
		CC6.8	"§164.316(b)(2)
		CC7.1	(b)(2)(i)"
		CC7.2	§164.316(b)(2)(ii)
		CC7.3	§164.316(b)(2)(iii)
		CC7.4	§164.308(a)(3)(i)
		A1.1	§164.308(a)(3)(ii)(A)
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
			§164.308(a)(5)(ii)(C)
			§164.308(a)(5)(ii)(D)
			§164.312(a)(2)(ii)
			§164.312(a)(1)
CA66	Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.	CC3.3	§164.306
		CC5.2	§164.308(a)(1)(ii)(B)
		CC6.3	"§164.316(b)(1)
		CC6.6	(b)(1)(i)
		CC6.7	(b)(1)(ii)"
		CC6.8	"§164.316(b)(2)
			§164.310(c)
			§164.310(d)(1)
			§164.310(d)(2)(ii)
			§164.310(d)(2)(iii)
			§164.312(a)(1)
			§164.312(a)(2)(iv)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
		CC7.1	(b)(2)(i)" §164.312(e)(1)
		CC7.5	§164.316(b)(2)(ii) §164.312(e)(2)(i)
		A1.2	§164.316(b)(2)(iii) §164.312(e)(2)(ii)
			§164.312(c)(1) §164.308(a)(5)(ii)(B)
			§164.312(c)(2) §164.308(a)(1)(i)
			§164.308(a)(3)(i) §164.308(a)(1)(ii)(D)
			§164.308(a)(3)(ii)(A) §164.308(a)(6)(i)
			§164.308(a)(3)(ii)(B) §164.308(a)(6)(ii)
			§164.308(a)(3)(ii)(C) §164.312(b)
			§164.308(a)(4)(i) §164.308(a)(1)(ii)(A)
			§164.308(a)(4)(ii)(B) §164.308(a)(7)(i)
			§164.308(a)(4)(ii)(C) §164.308(a)(7)(ii)(A)
			§164.308(a)(5)(ii)(C) §164.308(a)(7)(ii)(B)
			§164.308(a)(5)(ii)(D) §164.308(a)(7)(ii)(C)
			§164.312(d) §164.308(a)(7)(ii)(D)
			§164.310(a)(2)(iv) §164.310(a)(2)(i)
			§164.310(b) §164.310(d)(2)(iv)
CA67	Passwords of vendor default account in the production servers are changed on a periodical basis and access is restricted to IDC users.	CC8.1	§164.308(a)(1)(i) §164.308(a)(8)
		PI1.2	§164.308(a)(7)(i) §164.312(a)(1)
CA68	Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.	CC5.1	§164.306 §164.310(c)
		CC6.1	§164.308(a)(1)(i) §164.312(a)(2)(i)
		CC6.2	§164.308(a)(1)(ii)(A) §164.312(a)(2)(ii)
		CC6.3	§164.308(a)(1)(ii)(B) §164.312(a)(2)(iii)
			§164.308(a)(7)(ii)(C) §164.312(e)(2)(i)
			§164.308(a)(7)(ii)(D) §164.308(a)(3)(i)
			§164.308(a)(7)(ii)(E) §164.308(a)(3)(ii)(A)
			"§164.316(b)(1) §164.308(a)(3)(ii)(B)
			(b)(1)(i) §164.308(a)(3)(ii)(C)
			(b)(1)(ii)" §164.308(a)(4)(i)
			"§164.316(b)(2) §164.308(a)(4)(ii)(B)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
		(b)(2)(i)"	§164.308(a)(4)(ii)(C)
		§164.316(b)(2)(ii)	§164.308(a)(5)(ii)(C)
		§164.316(b)(2)(iii)	§164.308(a)(5)(ii)(D)
		§164.310(b)	§164.312(a)(1)
		§164.312(a)(2)(iv)	§164.312(c)(1)
		§164.312(b)	§164.312(c)(2)
		§164.312(e)(2)(ii)	§164.312(d)
		§164.308(a)(1)(ii)(D)	
CA69	Access to Zero Trust server access policy is revoked automatically if the user’s access is revoked in Zoho People.	CC5.1	§164.310(c)
		CC6.1	§164.312(a)(2)(i)
		CC6.2	§164.312(a)(2)(ii)
		CC6.3	§164.312(a)(2)(iii)
		§164.308(a)(7)(ii)(C)	§164.312(e)(2)(i)
		§164.308(a)(7)(ii)(D)	§164.308(a)(3)(i)
		§164.308(a)(7)(ii)(E)	§164.308(a)(3)(ii)(A)
		"§164.316(b)(1)	§164.308(a)(3)(ii)(B)
		(b)(1)(i)	§164.308(a)(3)(ii)(C)
		(b)(1)(ii)"	§164.308(a)(4)(i)
		"§164.316(b)(2)	§164.308(a)(4)(ii)(B)
		(b)(2)(i)"	§164.308(a)(4)(ii)(C)
		§164.316(b)(2)(ii)	§164.308(a)(5)(ii)(C)
		§164.316(b)(2)(iii)	§164.308(a)(5)(ii)(D)
		§164.310(b)	§164.312(a)(1)
		§164.312(a)(2)(iv)	§164.312(c)(1)
		§164.312(b)	§164.312(c)(2)
		§164.312(e)(2)(ii)	§164.312(d)
		§164.308(a)(1)(ii)(D)	
CA70	Zoho NOC team has defined procedure for logical access and operations of NOC as part of Network operations center policy. The document is reviewed by NOC L3 Engineer/Manager and approved by the NOC	CC2.2	§164.410(a)
		CC5.3	§164.310(a)(2)(iv)
		§164.308(a)(5)(ii)(A)	§164.310(d)(1)
		§164.308(a)(6)(i)	§164.310(d)(2)(ii)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	Manager on an annual basis. The document is made available on intranet portal for Zoho associates.		§164.308(a)(6)(ii)
CA71	Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.	CC6.1 CC6.7 CC6.8 CC7.1	§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(c)(1) §164.312(c)(2) §164.312(d) §164.310(a)(2)(iv) §164.310(b) §164.310(c)
			§164.310(d)(1) §164.310(d)(2)(ii) §164.310(d)(2)(iii) §164.310(d)(2)(iv) §164.312(a)(1) §164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(5)(ii)(B) §164.312(b)
CA72	Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.	CC3.1 CC4.1 A1.1 A1.3	§164.312(b) §164.308(a)(8) §164.308(a)(1)(ii)(A) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B)
			§164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E) §164.310(a)(2)(i) §164.312(a)(2)(ii)
CA73	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.	CC3.3 CC5.1 CC5.2 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2 CC7.3 CC7.5 A1.1	§164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A)
			§164.310(d)(2)(ii) §164.310(d)(2)(iii) §164.310(d)(2)(iv) §164.312(a)(1) §164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(5)(ii)(B) §164.308(a)(1)(ii)(C) §164.308(a)(8)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
			§164.308(a)(5)(ii)(C)
			§164.308(a)(5)(ii)(D)
			§164.312(d)
			§164.310(a)(2)(iv)
			§164.310(b)
			§164.310(c)
			§164.310(d)(1)
CA74	VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.	CC3.4 CC6.8 CC7.1 CC8.1 PI1.2 PI1.3	§164.308(a)(5)(ii)(B) §164.312(b) §164.308(a)(1)(i) §164.308(a)(7)(i)
CA75	The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.	CC3.4 CC6.8 CC7.1 CC8.1	§164.308(a)(5)(ii)(B) §164.312(b) §164.308(a)(1)(i) §164.308(a)(7)(i)
CA76	On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the	CC3.4 CC6.1	§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
	NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.	CC8.1	§164.310(b) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(a)(2)(iv) §164.312(b) §164.312(c)(1)	§164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(1)(i) §164.308(a)(7)(i) §164.308(a)(8) §164.312(a)(1)
CA77	Access to Corporate VPN is authenticated with Zoho users' AD account.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.6	§164.306 §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D) §164.310(c) §164.312(a)(2)(i) §164.312(a)(2)(ii)	§164.312(a)(2)(iii) §164.312(c)(1) §164.312(c)(2) §164.308(a)(1)(i) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(1) §164.312(d) §164.312(e)(1) §164.312(e)(2)(i)
CA78	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.	CC3.2 CC3.3 CC4.1 CC5.1 CC6.7 CC6.8	§164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2)	§164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(5)(ii)(B) §164.308(a)(8)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
		CC7.1	(b)(2)(i)" §164.308(a)(1)(i)
		CC7.2	§164.316(b)(2)(ii) §164.308(a)(1)(ii)(D)
		CC7.4	§164.316(b)(2)(iii) §164.308(a)(6)(i)
		CC7.5	§164.310(a)(2)(iv) §164.308(a)(6)(ii)
		A1.1	§164.310(b) §164.308(a)(7)(i)
		PI1.4	§164.310(c) §164.312(b)
			§164.310(d)(1) §164.308(a)(1)(ii)(A)
			§164.310(d)(2)(ii) §164.308(a)(7)(ii)(C)
			§164.310(d)(2)(iii) §164.308(a)(7)(ii)(D)
			§164.310(d)(2)(iv) §164.308(a)(7)(ii)(E)
			§164.312(a)(1) §164.312(a)(2)(ii)
CA79	Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers	CC5.1	§164.310(c) §164.310(c)
		CC6.1	§164.308(a)(1)(i) §164.312(a)(2)(i)
		CC6.2	§164.308(a)(1)(ii)(A) §164.312(a)(2)(ii)
		CC6.3	§164.308(a)(1)(ii)(B) §164.312(a)(2)(iii)
			§164.308(a)(7)(ii)(C) §164.312(e)(2)(i)
			§164.308(a)(7)(ii)(D) §164.308(a)(3)(i)
			§164.308(a)(7)(ii)(E) §164.308(a)(3)(ii)(A)
			"§164.316(b)(1) §164.308(a)(3)(ii)(B)
			(b)(1)(i) §164.308(a)(3)(ii)(C)
			(b)(1)(ii)" §164.308(a)(4)(i)
			"§164.316(b)(2) §164.308(a)(4)(ii)(B)
			(b)(2)(i)" §164.308(a)(4)(ii)(C)
			§164.316(b)(2)(ii) §164.308(a)(5)(ii)(C)
			§164.316(b)(2)(iii) §164.308(a)(5)(ii)(D)
			§164.310(b) §164.312(a)(1)
			§164.312(a)(2)(iv) §164.312(c)(1)
			§164.312(b) §164.312(c)(2)
			§164.312(e)(2)(ii) §164.312(d)
			§164.308(a)(1)(ii)(D)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA80	When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.	CC3.4	§164.312(b)	§164.308(a)(8)
		CC7.1	§164.308(a)(1)(i)	§164.312(a)(1)
		CC8.1	§164.308(a)(7)(i)	§164.312(c)(1)
		PI1.3		
CA81	Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.	CC3.2	§164.306	§164.310(d)(2)(ii)
		CC3.3	§164.308(a)(1)(ii)(B)	§164.310(d)(2)(iii)
		CC4.1	"§164.316(b)(1)	§164.310(d)(2)(iv)
		CC4.2	(b)(1)(i)	§164.312(a)(1)
		CC5.1	(b)(1)(ii)"	§164.312(a)(2)(iv)
		CC5.2	"§164.316(b)(2)	§164.312(e)(1)
		CC6.6	(b)(2)(i)"	§164.312(e)(2)(i)
		CC6.7	§164.316(b)(2)(ii)	§164.312(e)(2)(ii)
		CC6.8	§164.316(b)(2)(iii)	§164.308(a)(5)(ii)(B)
		CC7.1	§164.308(a)(3)(i)	§164.308(a)(1)(ii)(C)
		CC7.2	§164.308(a)(3)(ii)(A)	§164.312(c)(1)
		CC7.3	§164.308(a)(3)(ii)(B)	§164.308(a)(8)
		CC7.4	§164.308(a)(3)(ii)(C)	§164.308(a)(1)(i)
		CC7.5	§164.308(a)(4)(i)	§164.308(a)(1)(ii)(D)
		A1.1	§164.308(a)(4)(ii)(B)	§164.308(a)(6)(i)
			§164.308(a)(4)(ii)(C)	§164.308(a)(6)(ii)
			§164.308(a)(5)(ii)(C)	§164.308(a)(7)(i)
			§164.308(a)(5)(ii)(D)	§164.312(b)
			§164.312(d)	§164.308(a)(1)(ii)(A)
			§164.310(a)(2)(iv)	§164.308(a)(7)(ii)(C)
	§164.310(b)	§164.308(a)(7)(ii)(D)		
	§164.310(c)	§164.308(a)(7)(ii)(E)		
	§164.310(d)(1)	§164.312(a)(2)(ii)		
CA82	The NOC team uses Network Configuration Manager tool to backup network device configuration on a daily basis (full backup). In case of a backup failure, an	A1.1	§164.308(a)(7)(ii)(E)	§164.308(a)(7)(ii)(B)
		A1.2	§164.312(a)(2)(ii)	§164.308(a)(7)(ii)(C)
			§164.308(a)(1)(ii)(A)	§164.308(a)(7)(ii)(D)
			§164.308(a)(7)(i)	§164.310(a)(2)(i)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	automated email is triggered and remediation action is taken by NOC team.		§164.310(d)(2)(iv)
CA83	Access creation, modification and revocation to ManageEngine Event Log Anazlyzer and ManageEngine Network Configuration Manager used for performing NOC’s daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.	CC6.1 CC6.2 CC6.3 CC6.7	§164.312(b) §164.308(a)(1)(ii)(D) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(c)(1)
CA84	Zoho Server Operations team has defined data center operations document which specifies procedures relating to day-to-day operations of Server Operations including procedures for degaussing the disks. The document is reviewed by Data Center Manager and approved by Data center member leadership staff on an annual basis.	CC5.3	§164.310(a)(2)(iv) §164.310(d)(1) §164.310(d)(2)(ii)
CA85	Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.	CC3.1 CC3.4 CC5.1 CC6.6 CC6.7 CC7.1	§164.306 §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
		CC7.2	(b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.308(a)(1)(i) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(d)	§164.310(d)(2)(iv) §164.312(a)(1) §164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(D) §164.308(a)(7)(i) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E) §164.312(b)
CA86	Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.	CC5.2 CC6.1 CC6.2 CC6.3 CC6.7	§164.306 §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.312(b) §164.308(a)(1)(ii)(D) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A)	§164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(c)(1) §164.312(c)(2) §164.312(d) §164.310(a)(2)(iv) §164.310(b) §164.310(c) §164.310(d)(1) §164.310(d)(2)(ii) §164.310(d)(2)(iii) §164.310(d)(2)(iv) §164.312(a)(1) §164.312(a)(2)(iv) §164.312(e)(1)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
CA87	Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.	CC5.2	§164.306
		CC6.1	§164.308(a)(1)(ii)(A)
		CC6.2	§164.308(a)(1)(ii)(B)
		CC6.3	"§164.316(b)(1)
		CC6.7	(b)(1)(i)
			(b)(1)(ii)"
			"§164.316(b)(2)
			(b)(2)(i)"
			§164.316(b)(2)(ii)
			§164.316(b)(2)(iii)
			§164.312(b)
			§164.308(a)(1)(ii)(D)
			§164.312(a)(2)(i)
			§164.312(a)(2)(ii)
			§164.312(a)(2)(iii)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
			§164.308(a)(3)(ii)(B)
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
CA88	The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken.	CC6.7	§164.310(a)(2)(iv)
		A1.2	§164.310(b)
		A1.3	§164.310(c)
		PI1.5	§164.310(d)(1)
			§164.310(d)(2)(ii)
			§164.310(d)(2)(iii)
			§164.312(a)(1)
			§164.312(a)(2)(iv)
			§164.308(a)(1)(ii)(A)
			§164.310(d)(2)(iv)
			§164.308(a)(7)(i)
			§164.308(a)(7)(ii)(A)
			§164.308(a)(7)(ii)(B)
			§164.308(a)(7)(ii)(C)
			§164.308(a)(7)(ii)(D)
			§164.308(a)(7)(ii)(E)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.312(e)(1)
			§164.312(e)(2)(i)
			§164.312(e)(2)(ii)
CA89	Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.	CC6.1 CC6.7 C1.1 A1.2 A1.3 PI1.5	§164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(A) §164.310(d)(2)(iv) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.310(d)(1) §164.310(d)(2)(ii) §164.310(d)(2)(iii) §164.312(a)(1)
CA90	IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.	CC6.7 CC7.2 A1.1 A1.2 A1.3 PI1.5	§164.310(a)(2)(iv) §164.310(b) §164.310(c) §164.310(d)(1) §164.310(d)(2)(ii) §164.310(d)(2)(iii) §164.312(a)(1) §164.312(a)(2)(iv) §164.312(e)(1) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA91	The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.	CC4.2	§164.306	§164.308(a)(1)(ii)(D)
		CC5.1	§164.308(a)(1)(ii)(B)	§164.308(a)(6)(i)
		CC6.8	"§164.316(b)(1)	§164.308(a)(6)(ii)
		CC7.1	(b)(1)(i)	§164.312(b)
		CC7.2	(b)(1)(ii)"	§164.308(a)(7)(ii)(E)
		CC7.3	"§164.316(b)(2)	§164.312(a)(2)(ii)
		CC7.4	(b)(2)(i)"	§164.308(a)(1)(ii)(A)
		CC7.5	§164.316(b)(2)(ii)	§164.308(a)(7)(i)
		A1.1	§164.316(b)(2)(iii)	§164.308(a)(7)(ii)(A)
		A1.2	§164.308(a)(5)(ii)(B)	§164.308(a)(7)(ii)(B)
		PI1.4	§164.308(a)(1)(ii)(C)	§164.308(a)(7)(ii)(C)
				§164.312(c)(1)
		§164.308(a)(8)	§164.310(a)(2)(i)	
		§164.308(a)(1)(i)	§164.310(d)(2)(iv)	
CA92	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.	CC5.1	§164.306	§164.316(b)(2)(iii)
		CC7.2	§164.308(a)(1)(i)	§164.308(a)(1)(ii)(D)
		A1.1	§164.308(a)(1)(ii)(B)	§164.308(a)(7)(i)
			"§164.316(b)(1)	§164.312(b)
			(b)(1)(i)	§164.308(a)(1)(ii)(A)
			(b)(1)(ii)"	§164.308(a)(7)(ii)(C)
			"§164.316(b)(2)	§164.308(a)(7)(ii)(D)
			(b)(2)(i)"	§164.308(a)(7)(ii)(E)
		§164.316(b)(2)(ii)	§164.312(a)(2)(ii)	
CA93	The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.	CC4.2	§164.306	§164.312(b)
		CC5.1	§164.308(a)(1)(ii)(B)	§164.308(a)(1)(i)
		CC5.2	§164.308(a)(5)(ii)(C)	§164.308(a)(1)(ii)(D)
		CC6.8	§164.308(a)(5)(ii)(D)	§164.308(a)(6)(i)
		CC7.1	"§164.316(b)(1)	§164.308(a)(6)(ii)
		CC7.2	(b)(1)(i)	§164.308(a)(7)(i)
		CC7.3	(b)(1)(ii)"	§164.308(a)(8)
		CC7.4	"§164.316(b)(2)	§164.308(a)(1)(ii)(A)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
		A1.1	(b)(2)(i)"	§164.308(a)(7)(ii)(C)
		PI1.3	§164.316(b)(2)(ii)	§164.308(a)(7)(ii)(D)
		PI1.4	§164.316(b)(2)(iii)	§164.308(a)(7)(ii)(E)
			§164.308(a)(5)(ii)(B)	§164.312(a)(2)(ii)
			§164.308(a)(1)(ii)(C)	§164.312(c)(1)
CA94	Log of activities performed by users in IDC servers are captured and stored after each session in the Zoho Logs server and the same is available for review.	PI1.2		-
CA95	MI tool is used to ensure time sync for IDC Servers. The MI tool is synchronized to a trusted public time source of the GPS.	CC2.1 CC3.4		-
CA96	The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.	CC6.1 CC6.5 CC7.2 CC7.3 C1.2 PI1.5 P4.3	§164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(a)(2)(iv) §164.312(c)(1) §164.312(c)(2) §164.312(e)(2)(i) §164.312(e)(2)(ii) §164.308(a)(3)(i) §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C)	§164.310(a)(1) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(b) §164.310(c) §164.312(a)(1) §164.312(d) §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(D) §164.308(a)(7)(i) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E) §164.312(b) §164.310(d)(2)(i) §164.310(d)(2)(ii)
CA97	Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are	CC3.4 CC7.1	§164.312(b) §164.308(a)(1)(i)	§164.308(a)(8) §164.312(a)(1)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager.	CC8.1	§164.308(a)(7)(i)
CA98	Privileged access to servers is restricted to authorized personnel from the Server Operations team.	CC6.1	§164.310(b)
		CC6.2	§164.312(a)(2)(iv)
		CC6.3	§164.312(b)
			§164.312(e)(2)(ii)
			§164.308(a)(1)(ii)(D)
			§164.310(c)
			§164.312(a)(2)(i)
			§164.312(a)(2)(ii)
			§164.312(a)(2)(iii)
			§164.312(e)(2)(i)
			§164.308(a)(3)(i)
			§164.308(a)(3)(ii)(A)
CA99	Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network.	CC2.3	§164.308(a)(5)(i)
		CC5.2	§164.308(a)(5)(ii)(A)
		CC6.6	§164.308(a)(6)(i)
			§164.308(a)(6)(ii)
			§164.306
			§164.308(a)(1)(ii)(A)
			§164.308(a)(1)(ii)(B)
			"§164.316(b)(1)
			(b)(1)(i)
			(b)(1)(ii)"
			"§164.316(b)(2)
			(b)(2)(i)"
			§164.316(b)(2)(ii)
			§164.316(b)(2)(iii)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
CA100	Access to external storage devices and internet are disabled on IDC servers to prevent data loss.	CC5.2	§164.306	§164.308(a)(5)(ii)(D)
		CC6.1	§164.308(a)(1)(ii)(B)	§164.312(d)
		CC6.2	"§164.316(b)(1)	§164.310(a)(2)(iv)
		CC6.3	(b)(1)(i)	§164.310(b)
		CC6.6	(b)(1)(ii)"	§164.310(c)
		CC6.7	"§164.316(b)(2)	§164.310(d)(1)
		CC6.8	(b)(2)(i)"	§164.310(d)(2)(ii)
		CC7.1	§164.316(b)(2)(ii)	§164.310(d)(2)(iii)
		CC7.2	§164.316(b)(2)(iii)	§164.310(d)(2)(iv)
			§164.312(a)(2)(i)	§164.312(a)(1)
			§164.312(a)(2)(ii)	§164.312(a)(2)(iv)
			§164.312(a)(2)(iii)	§164.312(e)(1)
			§164.312(c)(1)	§164.312(e)(2)(i)
			§164.312(c)(2)	§164.312(e)(2)(ii)
			§164.308(a)(1)(i)	§164.308(a)(5)(ii)(B)
			§164.308(a)(3)(i)	§164.308(a)(1)(ii)(A)
			§164.308(a)(3)(ii)(A)	§164.308(a)(1)(ii)(D)
			§164.308(a)(3)(ii)(B)	§164.308(a)(7)(i)
			§164.308(a)(3)(ii)(C)	§164.308(a)(7)(ii)(C)
			§164.308(a)(4)(i)	§164.308(a)(7)(ii)(D)
	§164.308(a)(4)(ii)(B)	§164.308(a)(7)(ii)(E)		
	§164.308(a)(4)(ii)(C)	§164.312(b)		
	§164.308(a)(5)(ii)(C)			
CA101	Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.	CC6.1	§164.312(b)	§164.312(c)(2)
		CC6.2	§164.308(a)(1)(ii)(D)	§164.312(d)
		CC6.3	§164.312(a)(2)(i)	§164.310(a)(2)(iv)
		CC6.7	§164.312(a)(2)(ii)	§164.310(b)
			§164.312(a)(2)(iii)	§164.310(c)
			§164.308(a)(3)(i)	§164.310(d)(1)
			§164.308(a)(3)(ii)(A)	§164.310(d)(2)(ii)
	§164.308(a)(3)(ii)(B)	§164.310(d)(2)(iii)		

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(3)(ii)(C)
			§164.308(a)(4)(i)
			§164.308(a)(4)(ii)(B)
			§164.308(a)(4)(ii)(C)
			§164.308(a)(5)(ii)(C)
			§164.308(a)(5)(ii)(D)
			§164.312(c)(1)
CA102	Password of tools used in Zoho are configured as per the approved password policy.	CC5.2	§164.306
		CC6.1	§164.308(a)(1)(ii)(A)
		CC6.2	§164.308(a)(1)(ii)(B)
		CC6.3	"§164.316(b)(1)
		CC6.6	(b)(1)(i)
			(b)(1)(ii)"
			"§164.316(b)(2)
			(b)(2)(i)"
			§164.316(b)(2)(ii)
			§164.316(b)(2)(iii)
			§164.310(b)
			§164.312(a)(2)(iv)
			§164.312(b)
			§164.312(e)(2)(ii)
			§164.308(a)(1)(ii)(D)
			§164.310(c)
			§164.312(a)(2)(i)
			§164.312(a)(2)(ii)
CA103	Privilege access to tools used in Zoho is restricted to authorized associates.	CC5.1	§164.306
		CC6.1	§164.308(a)(1)(i)
		CC6.2	§164.308(a)(1)(ii)(A)
		CC6.3	§164.308(a)(1)(ii)(B)
			§164.308(a)(7)(ii)(C)
			§164.308(a)(7)(ii)(D)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement	
			§164.308(a)(7)(ii)(E) "§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(b) §164.312(a)(2)(iv) §164.312(b) §164.312(e)(2)(ii) §164.308(a)(1)(ii)(D)	§164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D) §164.312(a)(1) §164.312(c)(1) §164.312(c)(2) §164.312(d)
CA104	Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.	CC1.3 CC4.1 CC5.1 CC5.3 P5.1	§164.308(a)(2) §164.412 §164.308(a)(8) §164.306 §164.308(a)(1)(i) §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.308(a)(7)(ii)(E)	"§164.316(b)(1) (b)(1)(i) (b)(1)(ii)" "§164.316(b)(2) (b)(2)(i)" §164.316(b)(2)(ii) §164.316(b)(2)(iii) §164.310(a)(2)(iv) §164.310(d)(1) §164.310(d)(2)(ii)
CA105	Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.	CC5.3 C1.2 PI1.1 P4.3	§164.310(a)(2)(iv) §164.310(d)(1)	§164.310(d)(2)(i) §164.310(d)(2)(ii)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
CA106	<p>The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:</p> <p>1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information</p> <p>2) Policies regarding retention, sharing, disclosure, and disposal of their personal information</p> <p>3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information</p> <p>4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.</p>	<p>P1.1</p> <p>P3.1</p> <p>P5.1</p>	-
CA107	<p>Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.</p>	<p>CC2.3</p> <p>A1.1</p> <p>PI1.1</p> <p>P1.1</p> <p>P8.1</p>	<p>§164.308(a)(1)(ii)(A)</p> <p>§164.308(a)(7)(ii)(C)</p> <p>§164.308(a)(7)(ii)(D)</p> <p>§164.308(a)(7)(ii)(E)</p> <p>§164.312(a)(2)(ii)</p>
CA108	<p>Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.</p>	<p>CC1.2</p> <p>CC1.3</p> <p>CC2.2</p> <p>CC2.3</p> <p>CC3.1</p> <p>CC3.3</p> <p>CC3.4</p>	<p>§164.308(a)(2)</p> <p>§164.410(a)</p> <p>§164.308(a)(1)(i)</p> <p>§164.308(a)(5)(i)</p> <p>§164.308(a)(6)(ii)</p> <p>§164.312(b)</p>

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
CA109	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.	P4.3 P5.2 P7.1	§164.310(d)(2)(i) §164.310(d)(2)(ii)
CA110	Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity’s privacy practices). The notice is: <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects. 	CC2.3 CC5.3 P1.1 P3.2 P5.1	§164.308(a)(1)(i) §164.308(a)(5)(i) §164.308(a)(5)(ii)(A) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.310(a)(2)(iv) §164.310(d)(1) §164.310(d)(2)(ii)
CA111	Zoho’s Privacy Policy includes the below policy around Choice and Consent:	P2.1 P3.2 P5.1	-

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	<p>1) Consent is obtained before the personal information is processed or handled.</p> <p>2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences.</p> <p>3) When authorization is required (explicit consent), the authorization is obtained in writing.</p> <p>4) Implicit consent has clear actions on how a data subject opts out.</p> <p>5) Action by a data subject to constitute valid consent.</p> <p>6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.</p>		
CA112	<p>The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.</p>	<p>P2.1 P3.2 P5.2</p>	-
CA113	<p>Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by</p>	<p>P3.1 P4.1</p>	<p>§164.502(a)(5)(ii) §164.310(d)(2)(i)</p>

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	<ol style="list-style-type: none"> 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations. 		
CA114	<p>On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in</p> <ol style="list-style-type: none"> 1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations. 	<p>P4.1 P5.2 P7.1 P8.1</p>	<p>§164.502(a)(5)(ii) §164.310(d)(2)(i)</p>
CA115	<p>Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:</p> <ol style="list-style-type: none"> 1) The system processes in place to delete information in accordance with specific retention requirements. 	<p>C1.1 C1.2 P4.2 P7.1</p>	<p>§164.310(d)(2)(i) §164.310(d)(2)(ii)</p>

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	<p>2) Deletion of backup information in accordance with a defined schedule.</p> <p>3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention.</p> <p>4) Annually reviews information marked for retention.</p>		
CA116	The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.	P5.1 P6.7 P8.1	-
CA117	Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.	CC3.1 CC4.2	§164.312(b) §164.308(a)(1)(ii)(A) §164.308(a)(8)
CA118	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.	P5.1 P5.2 P6.5 P6.7 P8.1	§164.502(b) §164.502(e) §164.502(j)
CA119	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing,	P1.1 P4.2 P4.3 P5.1 P5.2	§164.310(d)(2)(i) §164.310(d)(2)(ii)

CA #	Control Activities	Trust Services Criteria		HIPAA Statement
	disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.	P7.1 P8.1		
CA120	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.	P1.1 P3.2 P4.1 P5.1 P5.2 P6.1	§164.310(d)(2)(i) §164.502(a)(5)(ii) §164.502(b)	§164.502(e) §164.502(j) §164.502(a)(3) and (4)
CA121	On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of “sensitive” personal information is properly delineated and communicated to personnel.	P2.1		-
CA122	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.	P2.1 P3.1		-
CA123	The entity’s application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject’s consent before the data subject submits the information.	P3.1 P3.2 P6.1	§164.502(a)(5)(ii) §164.502(b) §164.502(e)	§164.502(j) §164.502(a)(3) and (4)
CA124	When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).	P2.1 P3.2 P6.1 P8.1	§164.502(a)(5)(ii) §164.502(b) §164.502(e)	§164.502(j) §164.502(a)(3) and (4)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
CA125	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.	P5.1 P6.1 P6.2 P6.7 P8.1	§164.502(a)(5)(ii) §164.502(a)(3) and (4) §164.502(b) §164.502(e) §164.502(j)
CA126	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.	CC1.5 P6.2 P6.4 P6.5 P6.7	§164.308(a)(1)(i) §164.502(a)(3) and (4) §164.502(b) §164.502(e) §164.502(j) §164.410(a)
CA127	Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.	CC2.2 CC2.3 CC3.1 CC3.2 CC3.3 CC3.4 CC6.2 CC6.3 CC6.5 CC9.1 CC9.2 P6.4	§164.410(a) §164.308(a)(4)(ii)(C) §164.310(a)(1) §164.308(a)(1)(i) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.308(a)(5)(i) §164.310(a)(2)(iii) §164.308(a)(5)(ii)(A) §164.310(b) §164.310(c) §164.312(b) §164.310(d)(2)(ii) §164.308(a)(1)(ii)(D) §164.312(a)(1) §164.312(d) §164.312(a)(2)(i) §164.308(a)(1)(ii)(A) §164.312(a)(2)(ii) §164.308(b)(1) §164.312(a)(2)(iii) §164.308(b)(2) §164.312(e)(2)(i) §164.308(b)(3) §164.308(a)(5)(ii)(C) §164.314(a)(1) §164.312(c)(1) §164.314(a)(2)(iii) §164.312(c)(2) §164.316(a) §164.308(a)(3)(i) "§164.316(b)(1) §164.308(a)(3)(ii)(A) (b)(1)(i) §164.308(a)(3)(ii)(B) (b)(1)(ii)" §164.308(a)(3)(ii)(C) "§164.316(b)(2)(b)(2)(i)"

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
			§164.308(a)(4)(i) §164.308(a)(4)(ii)(B)
CA128	The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.	P2.1	-
CA129	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary	P3.1 P4.3 P8.1	§164.310(d)(2)(i) §164.310(d)(2)(ii)
CA130	Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.	P3.1 P6.1	§164.502(a)(5)(ii) §164.502(b) §164.502(e) §164.502(j) §164.502(a)(3) and (4)
CA131	An annual review of the organization's data inventory is performed by the Privacy team to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.	P4.2	§164.310(d)(2)(i) §164.310(d)(2)(ii)
CA132	Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.	CC1.4 CC2.2 P2.1	§164.308(a)(1)(i) §164.308(a)(5)(i) §164.308(a)(5)(ii)(A) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.410(a)
CA133	Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.	CC5.2 CC6.1 CC6.2	§164.306 §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B) "§164.316(b)(1) (b)(1)(i) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
		(b)(1)(ii)"	§164.308(a)(5)(ii)(C)
		"§164.316(b)(2)	§164.308(a)(5)(ii)(D)
		(b)(2)(i)"	§164.310(c)
		§164.316(b)(2)(ii)	§164.312(a)(1)
		§164.316(b)(2)(iii)	§164.312(a)(2)(i)
		§164.310(b)	§164.312(a)(2)(ii)
		§164.312(a)(2)(iv)	§164.312(a)(2)(iii)
		§164.312(b)	§164.312(c)(1)
		§164.312(e)(2)(ii)	§164.312(c)(2)
		§164.308(a)(1)(ii)(D)	§164.312(d)
		§164.308(a)(3)(i)	§164.312(e)(2)(i)
		§164.308(a)(3)(ii)(A)	
CA134	Zoho has defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials. The Security Head oversees and is responsible for the compliance and identification of ePHI data.	CC1.3 CC1.4	§164.308(a)(2) §164.412
CA135	Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.	CC2.3 CC3.3 CC4.1 CC9.2 C1.2	§164.308(a)(1)(i) §164.308(a)(5)(i) §164.308(a)(5)(ii)(A) §164.308(a)(6)(i) §164.308(a)(6)(ii) §164.308(a)(8) §164.308(a)(1)(ii)(A) §164.308(b)(1) §164.308(b)(2) §164.308(b)(3) §164.314(a)(1)
CA136	Zoho admin team maintains a register to document the repairs and modifications to the physical	CC6.4 A1.2	§164.308(a)(3)(i) §164.310(b) §164.310(c)

CA #	Control Activities	Trust Services Criteria	HIPAA Statement
	components of Zoho facilities that are related to physical access security.	§164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) §164.308(a)(4)(i) §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) §164.308(a)(7)(ii)(E) §164.310(a)(1) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(a)(2)(iv)	§164.310(d)(2)(iii) §164.308(a)(1)(ii)(A) §164.308(a)(7)(i) §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D) §164.310(a)(2)(i) §164.310(d)(2)(iv)

4.3.2 Test Procedures Performed by Service Auditors

In addition to the tests listed below for each control specified by Zoho, ascertained through corroborative inquiry with Compliance Lead, Technical Staff – Compliance Tools & Support, and Control Owner that each control activity listed below operated as described throughout the period.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA01	Zoho has a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.	Inspected organization chart and email communication relating to approval of organization chart for aspects such as 'Content of Org chart', 'Approved by' and 'Approved on' to ascertain whether Zoho had a defined organizational structure establishing the key areas of authority and responsibility, appropriate lines of reporting and defined roles which was reviewed and approved by Senior Manager-HR on an annual basis.	None	None	No Exception Noted.
CA02	Zoho HR Team has defined job descriptions specifying the responsibilities for key job positions. The document is reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.	Inspected the job description policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho HR Team had defined job descriptions specifying the responsibilities for key job positions and whether the document was reviewed and approved by Associate Director - TA & Global HR Operations on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA03	Zoho HR team has defined a Human Resource Security Policy. The document is reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates.	<p>Inspected the Human Resource Security policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho HR team had defined a Human Resource Security Policy and whether the document was reviewed by Assistant Manager - HR Operations and approved by the Deputy Manager - HR Operations on an annual basis.</p> <p>Further inspected for sample associates, the HRMS portal for aspects such as 'Host name', 'Availability of policy document on the intranet portal' to ascertain whether the document was made available in the HRMS (Zoho People) to the associates.</p>	None	None	No Exception Noted.
CA04	Procedures for background verification of Zoho associates is defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.	Inspected the Human Resource Security Policy for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved date' to ascertain whether the procedures for background verification of Zoho associates was defined as part of Human Resource Security Policy by the Assistant Manager-HR Operations and approved by the Senior Manager-HR on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA05	Zoho HR team has defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis. The document is made available in the HRMS (Zoho People) to the associates	<p>Inspected the code of ethics document for aspects such as ‘Content of document’, ‘Version number’, ‘Reviewed by’, ‘Approved by’ and ‘Approved on’ to ascertain whether Zoho HR team had defined a Code of Ethics Document which specifies the expectations towards legal compliance, policy compliance, responsible personal conduct, responsible behavior, and data privacy and protection and whether the document was reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.</p> <p>Further inspected for sample associates, the Zoho People application for aspects such as ‘Host name’, ‘Availability of policy document on the intranet portal’ to ascertain whether the document was made available in the HRMS (Zoho People) to the associates.</p>	None	None	No Exception Noted.
CA06	Zoho has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.	Inspected the performance appraisal policy document for the aspects such as ‘Content of document’, ‘Version number’, ‘Reviewed by’, ‘Approved by’ and ‘Approved on’ to ascertain whether Zoho had defined procedures for periodic performance appraisals including the review and assessment of professional development activities.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA07	Zoho Human Resource team has defined whistle blower mechanism as part of code of ethics document which specifies guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specifies the action to be taken in case of any violation. The document is reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.	Inspected the whistle blower policy document for the aspects such as ‘Content of document’, ‘Version number’, ‘Reviewed by’, ‘Approved by’ and ‘Approved on’ to ascertain whether Zoho Human Resource team had defined whistle blower mechanism as part of code of ethics document which specified guidance on raising possible non-compliance instances such as code violation, criminal offence, security breach, leak of confidential information, legal non-compliance etc. It also specified the action to be taken in case of any violation and whether the document was reviewed by Assistant Manager – HR Operations and approved by the Deputy Manager – HR Operations on an annual basis.	None	None	No Exception Noted.
CA08	Upon new associates joining, a Background Check (BGC) is performed by the third party service providers. A BGC report is provided to Zoho on completion of the background check and in case of a negative result, the employee is terminated.	<p>Inspected for sample new joiners, the Background check report for aspects such as 'Associate name', 'Date of BGC' and 'Status of BGC' to ascertain whether upon new associates joining, a Background Check (BGC) was performed by the third party service providers. A BGC report was provided to Zoho on completion of the background check.</p> <p>Further inspected for sample negative BGC results, the Zoho People Report for aspects such as 'Date of joining', 'Date of BGC' and 'Termination date' to ascertain whether in case of a negative result, the employee was terminated.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA09	Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people.	Inspected for sample newly joined associates, the training attendance register in Zoho People for aspects such as 'employee name', 'date of attendance', 'date of joining'; Further inspected induction deck for aspects such as 'name of deck' and 'contents' to ascertain whether upon a new associate joining, an induction training was conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho and whether the attendance for the training was captured in Zoho people.	None	None	Exception Noted Refer Exception #1
CA10	Upon joining Zoho, the associates are required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.	Inspected for sample new joiners, the document signed by the associates for aspects such as 'Employee name', 'Date of joining', 'Documents signed' and 'Date of signing the documents' to ascertain whether upon joining Zoho, the associates were required to sign a Non Disclosure Agreement (NDA), Acceptable Use Policy, Anti Harassment Policy and Social Media Policy during the pre-onboarding process.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA11	Zoho physical security team has defined a Physical Security Policy which specifies the physical access restrictions to the NOC / Server Operations processing area. The document is reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis. The document is made available on intranet portal for Zoho associates.	<p>Inspected the physical security policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho physical security team had defined a physical security policy which specified the physical access restrictions to the NOC / Server Operations processing area and whether the document was reviewed by Manager Safety and Security and approved by the Head of Safety and Security on an annual basis.</p> <p>Further inspected for sample associates, the intranet portal for aspects such as 'Host name', 'Availability of policy document on the intranet portal' to ascertain whether the document was made available on intranet portal for Zoho associates.</p>	None	None	No Exception Noted.
CA12	For associates joining Zoho, the HR team creates a request for providing physical access card and the same is actioned upon by the Physical Security team. The access cards are distinguished based on the color of the tags described in the HR process document.	<p>Inspected for sample new joiners, the physical access management tool and email communication relating to account creation for aspects such as 'Username', 'Employee ID', 'Joining date', 'Physical access account created on', 'Email sent by', 'Email sent to' and 'Email sent on' to ascertain whether for associates joining Zoho, the HR team created a request for providing physical access card and the same was actioned upon by the Physical Security team.</p> <p>Further Inspected the physical access cards for sample associates and HR policy for aspects such as 'Color of Access Card Tag' and 'Tag assigned to' to ascertain whether the access cards were distinguished based on the color of the tags described in the HR process document.</p>	None	3.12.1	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA13	In case an access card is lost, the associate raises a request in Zoho people. Based on the request, the Physical Security team deactivates the old access card and issues a new access card.	Inspected for sample access card lost cases, the physical access management tool and email communication relating to account deactivation for aspects such as 'Username', 'Employee ID', 'Email sent by', 'Email sent to', 'Email sent on' 'Access Card lost reported on', 'Access card deactivated on' and 'New access card created on' to ascertain whether in case an access card was lost, the associate raised a request in Zoho people and whether based on the request, the Physical Security team deactivated the old access card and issued a new access card.	None	3.12.1	No Exception Noted.
CA14	For associates leaving Zoho, the HR team creates a request for revoking physical access card and the same is actioned upon by the Physical Security team on the last working day.	Inspected for sample leavers, the physical access management tool and email communication relating to account deactivation for aspects such as 'Username', 'Employee ID', 'Last working date', 'Physical access account disabled on', 'Email sent by', 'Email sent to' and 'Email sent on' to ascertain whether for associates leaving Zoho, the HR team created a request for revoking physical access card and the same was actioned upon by the Physical Security team on the last working day.	None	3.12.1	Exception Noted Refer Exception #2

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA15	Proximity card-based access control system is installed at the entry / exit points within the facilities. In addition, access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room is restricted to authorized personnel using proximity card-based access control system.	<p>Observed Zoho facilities for aspects such as ‘installation of proximity card-based access control system’ and ‘location of installation’ to ascertain whether proximity card-based access control system was installed at the entry / exit points within the facilities.</p> <p>Further inspected the user access list to server room, NOC room, Switch room, Server Operations Workspace and asset storage room for aspects such as ‘User access’ and ‘Department’ to ascertain whether access to the Zoho Server room, NOC room, Switch room, Server Operations Workspace and asset storage room was restricted to authorized personnel using proximity card-based access control system.</p>	None	3.12.1	No Exception Noted.
CA16	Entry/exit points are manned 24x7 by the Security personnel restricting access to authorized individuals.	Observed the entry and exit points of Zoho facilities; Further inspected for sample dates, the security guard register for aspects such as ‘date’, ‘shift details’, ‘time-in and time-out details’, and ‘signature details’ to ascertain whether entry/exit points were manned 24x7 by the Security personnel restricting access to authorized individuals.	None	3.12.1	No Exception Noted.
CA17	Entry and Exit details of the vendors / visitors to Zoho facilities are recorded through Visitor Management System (VMS) / visitor register. Laptops of the vendors/visitors are declared at the entrance of the Zoho facilities.	Inspected for sample dates, the visitor-vendor register for aspects such as ‘date’, ‘visitor/vendor name’, ‘time-in and time-out details’ and ‘electronic device declaration details’ to ascertain whether entry and exit details of the vendors / visitors to Zoho facilities were recorded through Visitor Management System (VMS) / visitor register and whether laptops of the vendors/visitors were declared at the entrance of the Zoho facilities.	None	3.12.1	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA18	Zoho facilities and server rooms are monitored through Closed-Circuit Television (CCTV) cameras. CCTV recordings are retained for 60 days.	<p>Observed the Zoho facilities and server rooms for aspects such as 'Installation of CCTV cameras' and 'installation points'. Further observed the security guard monitoring of CCTV camera recordings to ascertain whether Zoho facilities and server rooms were monitored through Closed-Circuit Television (CCTV) cameras.</p> <p>Further inspected the CCTV footage for sample dates for aspects such as 'Location' and 'recordings' to ascertain whether CCTV recordings were retained for 60 days.</p>	None	3.12.1	No Exception Noted.
CA19	<p>Environmental safeguards are installed in Zoho facilities comprising of the following:</p> <ul style="list-style-type: none"> • Cooling Systems • UPS with Battery and diesel generator back-up • Smoke detectors • Water sprinklers • Fire resistant floors • Fire extinguisher 	<p>Observed the Zoho facilities for aspects such as 'locations', 'cooling facilities', 'UPS with battery and diesel generator', 'smoke detectors', 'water sprinklers', 'fire extinguisher' and 'fire-resistant floors' to ascertain whether environmental safeguards were installed in Zoho facilities comprising the following:</p> <ul style="list-style-type: none"> • Cooling Systems • UPS with Battery and diesel generator back-up • Smoke detectors • Water sprinklers • Fire resistant floors • Fire extinguisher 	None	3.12.1	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA20	Planned Preventive Maintenance (PPM) is performed on a periodic basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.	Inspected sample preventive maintenance reports for aspects such as 'name of equipment', 'date of maintenance report' and 'performed by' to ascertain whether Planned Preventive Maintenance (PPM) was performed on a periodic basis by the third parties to the UPS, fire extinguishers, smoke detectors, water sprinkler, cooling systems, and generators.	None	3.12.1	No Exception Noted.
CA21	Mock Fire drills are conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.	Inspected for inscope locations the mock fire drill report for aspects such as 'Conducted on', 'location' and 'Observations of mock fire drill' to ascertain whether Mock Fire drills were conducted by Safety Security team of Zoho on an annual basis to assess the readiness of the workforce for evacuation during a disaster.	None	3.12.1	No Exception Noted.
CA22	Zoho compliance team has defined an organization wide Integrated Management System Manual which specifies the information security and privacy requirement and also defines the related roles and responsibilities. The document is reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.	Inspected the Integrated Management System Manual policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho compliance team had defined an organization wide Integrated Management System Manual which specified the information security and privacy requirement and also defined the related roles and responsibilities and whether The document was reviewed by Information Security Compliance Manager and approved by the Security Head on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA23	Zoho Compliance team has defined risk management policy which specifies the operational, strategic and IT risks related to the infrastructure and services provided by Zoho. The document is reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.	Inspected the Risk management policy document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Compliance team had defined risk management policy which specified the operational, strategic and IT risks related to the infrastructure and services provided by Zoho and whether the document was reviewed by compliance team member and approved by the Information Compliance Manager on an annual basis.	None	None	No Exception Noted.
CA24	Zoho Compliance Team has defined a Business Continuity Plan and Disaster Recovery Procedure. The document is reviewed and approved by the Compliance Leadership team on an annual basis.	Inspected the business continuity plan and disaster recovery procedure document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Compliance Team had defined a Business Continuity Plan and Disaster Recovery Procedure. The document was reviewed and approved by the Compliance Leadership team on an annual basis	None	None	No Exception
CA25	Zoho Compliance Team has defined Internal Audit Process Manual. The document is reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.	Inspected the Internal audit process manual for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Compliance Team had defined Internal Audit Process Manual and whether the document was reviewed by Compliance Team Member and approved by Information Security Compliance Manager on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA26	On an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports are obtained for co-location data centers and are reviewed by the Zoho NOC team. In case there are any non-compliances noted in the report, the compliance team follows up with the co-location service provider for further action.	Inspected the email communication relating to data center co-location provider certification/report review for aspects such as 'vendor name', 'attestation report details', 'observations noted', 'Action taken', 'Report evaluated by' and 'Report evaluated on' to ascertain whether on an annual basis, SOC 1/SOC 2 or ISO 27001 certification reports were obtained for co-location data centers and were reviewed by the Zoho NOC team and whether in case there were any non-compliances noted in the report, the compliance team followed up with the co-location service provider for further action.	None	None	No Exception Noted.
CA27	A contract is defined, documented and approved between Zoho and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by Zoho and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	Inspected for sample third parties, the agreement document signed between Zoho and third party vendor for aspects such as 'scope', 'confidentiality clause', 'validity', 'type of service', 'agreement signed by' and 'agreement signed on' to ascertain whether a contract was defined, documented and approved between Zoho and third parties for services in relation to hosting of servers and whether any changes to the contracts were agreed by Zoho and the third parties and whether the contract included the scope of services to be provided, confidentiality and other related commitments / clauses.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA28	On a half-yearly basis, the Zoho compliance team conducts internal audit of Zoho’s information security and privacy controls. Findings from the internal audit are presented to the management and remediation action is taken on a timely basis.	<p>Inspected for a sample half-year the Internal Audit Report for aspects such as ‘audit period’, ‘agenda’, ‘scope’, ‘audit risk count’ and ‘department / teams’ to ascertain whether on a half-yearly basis, the Zoho compliance team conducted the internal audit of Zoho’s information security and privacy controls.</p> <p>Further inspected the MOM for aspects such as ‘Points discussed’, ‘Date of meeting’, ‘Remediation Performed’, ‘Remediation timeline’ and ‘Meeting Participants’ to ascertain whether findings from the internal audit were presented to the management and remediation action was taken on a timely basis.</p>	None	None	No Exception Noted.
CA29	Management Review Meeting is held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status is discussed as part of the meeting.	Inspected ISMS Management review meeting for aspects such as ‘meeting/report date’, ‘auditors’, ‘remediation action’, ‘remediation action date’, ‘MoM prepared by’ and ‘approved by’ for sample half-year. Further Inspected ISMS Management review meeting deck and Minutes of meeting for aspects such as ‘Audit period’, ‘Date of review meeting’, ‘Meeting participants’, ‘Agenda’ and ‘Action points’ to ascertain whether management Review Meeting was held on a half-yearly basis to discuss the key findings noted in the internal audit, incorporate management functions and also to review the risk assessment. Summary of non-conformances along with implementation status was discussed as part of the meeting.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA30	Zoho's management committee is responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis. Policies and procedures related to information security are made available to associates through the intranet portal.	Inspected the Integrated Management System Manual in Zoho portal for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on', and 'Availability in intranet portal' to ascertain whether Zoho's management committee was responsible for defining, implementing, and monitoring policies and procedures related to Information security and reviewed on an annual basis and whether policies and procedures related to information security were made available to associates through the intranet portal.	None	None	No Exception Noted.
CA31	Management establishes an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls are discussed.	Inspected the minutes of the sample meetings held for aspects such as 'Date of meeting', 'Participants of meeting', 'Agenda / minutes of meeting' to ascertain whether management established an oversight through periodical meetings held with the senior management and Internal Audit function including the Finance team as part of which Business, security and internal controls were discussed.	None	None	No Exception Noted.
CA32	On an annual and periodic basis, Zoho performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701). The ISO standards identifies the processes, and related information assets that are critical for Zoho to ensure information security and privacy standards are adhered across the entity.	Inspected sample Information Technology (IT) Risk Assessment reports for aspects such as 'Risk Assessment performed on', 'Risk Assessment performed by', 'Criteria', 'Domains' and 'Validity' to ascertain whether on an annual and periodic basis, Zoho performed organization wide Information Technology Risk Assessment as part of the ISO standards (27001, 27017, 27018 and 27701) and whether the ISO standards identified the processes, and related information assets that were critical for Zoho to ensure information security and privacy standards were adhered across the entity.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA33	Zoho Incident management team has defined an incident management system policy. The document is reviewed and approved by the Information security manager on an annual basis.	Inspected the incident management system policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Incident management team had defined an incident management system policy and whether the document was reviewed and approved by the Information security manager on an annual basis.	None	None	No Exceptions Noted.
CA34	Zoho Privacy team has defined privacy incident identification and breach response procedure which specifies examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The document is reviewed and approved by the Director of compliance on an annual basis. The incident management procedures are communicated to personnel who handle personal information.	<p>Inspected the privacy incident identification and breach response procedure document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Privacy team had defined privacy incident identification and breach response procedure which specified examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach and whether the document was reviewed and approved by the Director of compliance on an annual basis.</p> <p>Further inspected the announcement details in Zoho Connect portal for aspects such as 'announcement name', 'contents of announcement' and 'uploaded by' to ascertain whether the incident management procedures were communicated to personnel who handle personal information.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA35	Incidents from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho incident management team for resolution. The relevant product team performs root cause analysis (RCA) and updates the incident in the Zoho creator tool.	Inspected for sample incidents, the ticket from creator tool for aspects such as 'Incident ID', 'Incident Title', 'Description of the incident', 'RCA available', 'Raised By' 'Incident Cause', 'Incident Category' and 'Incident start time' and 'Status' to ascertain whether incidents from customer were raised as ticket in Zoho Desk Portal which was assigned to the Zoho incident management team for resolution and whether the relevant product team performed root cause analysis (RCA) and updates the incident in the Zoho creator tool.	3.11.5	None	No Exception Noted.
CA36	A message is sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA is prepared by product team and it is reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues are resolved.	Inspected for sample privacy incidents the creator tickets for aspects such as 'Incident ID', 'Incident Title', 'Description of the incident', 'RCA available', 'Raised By' 'Incident Cause', 'Incident Category' and 'Incident start time' and 'Status' to ascertain whether A message was sent to the privacy staff informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. RCA was prepared by product team and it was reviewed by the Incident management/Privacy team upon which incidents flagged as privacy issues were resolved.	None	None	No Exception Noted.
CA37	An Incident report is reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal. The report includes the categories of incidents, downtime details (in case of availability incident) and the incident description.	Inspected the incident report for aspects such as 'Reviewed by', 'Reviewed on', 'Name of report', 'Report uploaded by', 'Date of report' and 'Content of report' to ascertain whether An Incident report was reviewed by the Information Security Manager and published on a yearly basis by the Zoho Incident Coordinator in the Zoho Connect Portal and whether the report included the categories of incidents, downtime details (in case of availability incident) and the incident description.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA38	Zoho Customer Support team has defined support process document. The document is reviewed and approved by the Global Head of customer service on an annual basis.	Inspected the support process document policy document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Customer Support team had defined support process document and whether the document was reviewed and approved by the Global Head of customer service on an annual basis.	None	None	No Exception Noted.
CA 39	Support requests raised from customer are raised as ticket in Zoho Desk Portal which is assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.	Inspected for sample support ticket raised the desk tickets in Zoho Desk Portal for aspects such as 'Ticket ID', 'Query raised via', 'Ticket raised by', 'Ticket raised on', 'Ticket closed by', 'Ticket closed on', 'Status' and 'SLA details' to ascertain whether support requests raised from customer were raised as ticket in Zoho Desk Portal which was assigned to the Zoho Product Support Engineer / Zoho Technical Support Engineer for resolution within the SLA agreed with the customers.	3.11.5	None	No Exception Noted.
CA40	Zoho Compliance team has defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation. The document is reviewed by Information Security Compliance Manager and approved by the Web Master - Project Manager on an annual basis.	Inspected the change management policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Compliance team had defined change management policy which specifies procedures pertaining to infrastructure and product changes, which define the process of initiation, approval, review and implementation and whether the document was reviewed by Information Security Compliance Manager and approved by the Web Master - Project Manager on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA41	Zoho has defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.	Inspected for sample products, the SDLC document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho had defined Software Development Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation and whether the documents were reviewed and approved by the respective Product Teams on an annual basis.	None	None	No Exception Noted.
CA42	Support documents including the system flow diagrams and other design documents for the products are maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.	Inspected for sample products, the support process document for aspects such as 'Product name', 'Availability in work drive' and 'Edit access list' to ascertain whether support documents including the system flow diagrams and other design documents for the products were maintained and made available to Zoho associates with edit access restricted to the respective product team and compliance team.	None	None	No Exception Noted.
CA43	Secure coding practices are defined and communicated to the respective personnel as part of the Zoho's SDLC process.	Inspected for entity wide SDLC document and for sample products, the SDLC documents for aspects such as 'Product details', 'Category' and 'availability in work drive' to ascertain whether secure coding practices were defined and communicated to the respective personnel as part of the Zoho's SDLC process.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA44	Product descriptions, help documents and terms of usage / service are defined and are made available to the customers via corporate website.	Inspected the corporate website for sample products for aspects such as 'Product name', 'website – URL where the document was hosted' and 'contents' to ascertain whether product descriptions, help documents and terms of usage / service were defined and were made available to the customers via corporate website.	3.11.3	None	No Exception Noted.
CA45	Zoho maintains a dedicated Development and test environment, which is separate from the Production environment for its applications.	Inspected for sample products the segregation of environment for aspects such as 'Development environment paths/URL's', 'test environment paths/URL's' and 'Production environment paths/URL's' to ascertain whether Zoho maintained a dedicated Development and test environment, which was separate from the Production environment for its applications.	None	None	No Exception Noted.
CA46	The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.	Inspected for sample builds, the Code repository details in Configuration Management tool for aspects such as 'Build URL' and 'Availability of repository' to ascertain whether the code created by the development team was maintained in a centralized repository by the Configuration Management (CM) team and whether the code developed by the Developers was pushed into the CM tool, which was an in-house tool used by the CM team.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA47	The developed code is tested using the in-house CM tool prior to check-in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off is provided and then the code is deployed in the production environment.	Inspected for sample builds, the build workflow details and corresponding records for aspects such as 'Product name', 'Build URL', 'Build Compile date', 'Number of blocking issue', 'Approval for blocking issue', 'Availability of testcase document', 'Tested by', 'Tested on', 'QA signoff provided by', 'QA signoff provided on', 'Prod push date', 'Build push applied DC' to ascertain whether the developed code was tested using the in-house CM tool prior to check-in and whether once the code was checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment. On resolution, a sign-off was provided and then the code was deployed in the production environment.	3.11.7	None	No Exception Noted.
CA48	Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.	Inspected for sample products the Zoho logs for aspects such as 'Log forwarding configuration', 'Type of log monitored', 'Retention period' and 'Access restriction' to ascertain whether Zoho cloud products provided the log of activities performed by the users. The logs were stored in Zoho logs and access was restricted to the authorized personnel only.	None	None	No Exception Noted.
CA49	Zoho Sysadmin team has defined OS Hardening guidelines for workstation. The document is reviewed by the respective member of IT Service and approved by the Manager - IT Services on an annual basis.	Inspected OS Hardening guidelines of workstation for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Sysadmin team had defined OS Hardening guidelines for workstation and whether the document was reviewed by the respective member of IT Service and approved by the Manager - IT Services on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA50	Access to support admin portal of Zoho products are defined through IAM. Zoho support admin access is provisioned by the IAM team after obtaining approval from authorized personnel.	Inspected for sample support admins access provisioned during the examination period the Zoho Request ticket for aspects such as 'associate name', 'requested by', 'requested on', 'Authorized by' and 'Date of provisioning' to ascertain whether access to support admin portal of Zoho products were defined through IAM. Zoho support admin access was provisioned by the IAM team after obtaining approval from authorized personnel.	None	None	No Exception Noted.
CA51	Zoho maintains an asset register for it's IT assets including servers, software, workstations, network devices, storage.	Inspected the asset registry for aspects such as 'Device Type', 'Tool used' and 'Responsibility' to ascertain whether Zoho maintained an asset register for it's IT assets including servers, software, workstations, network devices, storage.	None	None	No Exception Noted.
CA52	For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.	Inspected for sample new joiners, the IAM account creation log, AD account creation log and email communication relating to account creation for aspects such as 'Username', 'Employee ID', 'Request ID', 'Joining date', 'IAM account created on', 'AD account created on', 'Email sent by', 'Email sent to' and 'Email sent on' to ascertain whether For associates joining Zoho, the HR team created IAM account in Zoho People application and whether the HR team then created a request for creating AD account and the same was actioned upon by the Sysadmin team.	None	None	Exception Noted. Refer Exception #3

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA53	For associates leaving Zoho, the HR team disables IAM account in Zoho People application. The HR team then creates a request for revoking AD account and the same is actioned upon by the Sysadmin team.	Inspected for sample leavers, the IAM account deletion log, AD account deletion log and email communication relating to account deletion for aspects such as 'Username', 'Employee ID', 'Request ID', 'Last working date', 'IAM account revoked on', 'AD account revoked on', 'Delay in access revocation', 'Email sent by', 'Email sent to' and 'Email sent on' to ascertain whether for associates leaving Zoho, the HR team disabled IAM account in Zoho People application and whether the HR team then created a request for revoking AD account and the same was actioned upon by the Sysadmin team.	None	None	No Exception Noted.
CA54	Antivirus software is installed in the user work stations and corporate servers. The latest updates and definitions are pushed automatically to the workstations on a periodical basis.	<p>Inspected for sample workstations, the AV software for aspects such as 'Hostname' and 'Availability of Antivirus' to ascertain whether antivirus software was installed in the user work stations.</p> <p>Inspected for sample servers, the AV software for aspects such as 'Hostname' and 'Availability of Antivirus' to ascertain whether antivirus software was installed in the corporate servers.</p> <p>Further inspected the antivirus configuration for aspects such as 'Synchronization interval' and 'AV version' to ascertain whether the latest updates and definitions were pushed automatically to the workstations on a periodical basis.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA55	Monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.	Inspected Antivirus console for aspects such as 'Tool name', 'Real-time monitoring status', 'AV Dashboard' and 'SDP integration'. Further inspected for sample alerts, the tickets for aspects such as 'Ticket number', 'Opened on', 'Closed on' and 'Closure action' to ascertain whether monitoring of Anti Virus console is performed on a real time basis by the IT Team. Alerts generated are created as ticket in service desk plus tool for which respective team takes corrective action.	3.11.8	None	No Exception Noted.
CA56	Authentication of users to Zoho products are governed through IAM through which the password configuration including password complexity and lockout is enforced.	Inspected the configuration in IAM for aspects such as 'Password Configuration and Complexity enabled' and 'authentication to Zoho products' to ascertain whether authentication of users to Zoho products were governed through IAM through which the password configuration including password complexity and lockout was enforced.	None	None	No Exception Noted.
CA57	User Access Review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network are reviewed by the manager / Department Head / Admin on an annual basis. Corrective actions, if any, are taken on a timely manner.	Inspected the creator tool for IAM role user access review for aspects such as 'Date of review', 'Count of IAM roles', 'Number of request raised', 'Reviewed by', 'closure date' and 'Closure actions performed' Further inspected the timeline of review from IAM manual to ascertain whether user access review of users with access to IAM Roles that grant access to the products and users with access to Zodoor and IDC network were reviewed by the manager / Department Head / Admin on an annual basis and whether Corrective actions, if any, were taken on a timely manner.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA58	Zoho Encryption at rest team has defined EAR policy which specifies the procedure for encryption and key management. The document is reviewed by EAR Team Lead and approved by Security – Manager on an annual basis.	Inspected the EAR policy document for the aspects such as ‘Content of document’, ‘Version number’, ‘Reviewed by’, ‘Approved by’ and ‘Approved on’ to ascertain whether Zoho Encryption at rest team had defined EAR policy which specified the procedure for encryption and key management. The document was reviewed by EAR Team Lead and approved by Security – Manager on an annual basis.	None	None	No Exception Noted.
CA59	Zoho uses in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services. Access to KMS server is restricted. Access to KMS is provided by authorized personnel based on approval from Manager in KMS team.	<p>Inspected the Key Management Service tool for aspects such as ‘Product name’, ‘Use of encryption key’, ‘Role as per HR’ and ‘User listing’ to ascertain whether Zoho used in-house Key Management Service (KMS) to create, store and manages keys across all Zoho services and whether access to KMS server was restricted.</p> <p>Inspected the sample access requests for aspects such as ‘Requestor Name’, ‘Access Requested’, ‘Request date’, ‘Access provided’ to ascertain whether access to KMS was provided by authorized personnel based on approval from Manager in KMS team.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA60	Zoho Key Management service team implements encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products. Zoho also uses encryption for its emails.	<p>Inspected for sample products the encryption agent for aspects such as ‘Product name’, ‘encryption status’ to ascertain whether Zoho Key Management service team implemented encryption of data at rest (including usage of FDE) to protect customer data based on the business requirement for Zoho Products.</p> <p>Further inspected the encryption configuration for Zoho email for aspects such as ‘Status of encryption’ and ‘Type of encryption to ascertain whether Zoho also used encryption for its emails.</p>	None	None	No Exception Noted.
CA61	Zoho Cloud products use TLS 1.2/1.3 encryption for data that are transferred through public networks.	Inspected the website network configuration for aspects such as ‘Domain’ and ‘TLS version’ to ascertain whether Zoho Cloud products used TLS 1.2/1.3 encryption for data that were transferred through public networks.	None	None	No Exceptions Noted.
CA62	Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy.	Inspected the Zoho Password policy and password configuration of Domain Controller, IAM, IAN and Zero Trust for aspects such as ‘Content of password policy’, ‘Password configuration’ and ‘Account lockout configuration’ to ascertain whether security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust were configured as per Zoho Password Policy	3.11.1	None	<p>Exception Noted.</p> <p>Refer Exception #4</p>
CA63	Zoho associates are required to use two factor authentication to connect to IDC infrastructure.	Inspected the IAN and Zero Trust authentication configuration for aspects such as ‘TFA Configuration’ to ascertain whether Zoho associates were required to use two factor authentication to connect to IDC Infrastructure	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA64	On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken.	Inspected for sample products the vulnerability assessment report for aspects such as 'Request ID', 'Datacenter', 'Date of vulnerability scan', 'Scan performed by', 'Count of deviations' and 'Resolution' to ascertain whether on a weekly basis, the central security team performed vulnerability scanning to ensure application security for its products and whether in case of any deviations identified, corrective action was taken.	3.11.8	None	No Exception Noted.
CA65	On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken	Inspected for sample products the penetration testing reports for aspects such as 'Scope', 'Testcases handled', 'Date of vulnerability scan', 'Count of deviations' and 'Resolution' to ascertain whether on a yearly basis, the product security team performed penetration testing to ensure application security for its products. In case of any deviations identified, corrective was taken	3.11.8	None	No Exception Noted.
CA66	Any files uploaded to Zoho cloud products are scanned for malicious content by the Malware Analysis tool. The logs relating to malware detection are stored in Zoho logs for 60 days.	Inspected the malware analysis tool, malware scan configuration and retention configuration for aspects such as 'Name of DC', 'Retention period', 'Hacksaw rule status' and 'File check configuration' and further inspected the oldest log available to ascertain whether any files uploaded to Zoho cloud products were scanned for malicious content by the Malware Analysis tool and whether the logs relating to malware detection were stored in Zoho logs for 60 days.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA67	Passwords of vendor default account in the production servers are changed on a periodical basis and access is restricted to IDC users.	Inspected for sample production servers (OS and DB), user listing for aspects such as 'Server name' 'Product mapped to Server', 'IDC', 'Application Server/ Database details' 'Vendor default account password changed' to ascertain whether Passwords of vendor default account in the production servers were changed on a periodical basis and access was restricted to IDC users.	3.11.1	None	No Exception Noted.
CA68	Access to Zero Trust server access policy is provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.	Inspected for sample requests the access approval form from zero trust application for aspects such as 'Policy name', 'Status', 'Approver', 'Requester', 'Mapped user', 'Verified by', 'Verified on', 'Agent version installed', 'Approved by', 'Hardening status' and 'Approved on' to ascertain whether access to Zero Trust server access policy was provided by SPM (Security poster management) team based on the request raised by Server Operations team member and the hardening check performed by Zero trust agent installed in the workstation of the member who raised the request.	None	None	No Exception Noted.
CA69	Access to Zero Trust server access policy is revoked automatically if the user's access is revoked in Zoho People.	Inspected the batch job of Zoho People for aspects such as 'Integration details' and 'Function details' to ascertain whether access to Zero Trust server access policy was revoked automatically if the user's access was revoked in Zoho People.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA70	Zoho NOC team has defined procedure for logical access and operations of NOC as part of Network operations center policy. The document is reviewed by NOC L3 Engineer/Manager and approved by the NOC Manager on an annual basis. The document is made available on intranet portal for Zoho associates.	<p>Inspected the NOC operations center policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho NOC team had defined procedure for logical access and operations of NOC as part of Network operations center policy and whether the document was reviewed by NOC L3 Engineer/Manager and approved by the NOC Manager on an annual basis.</p> <p>Further inspected for sample associates for aspects such as 'Host name', 'Availability of policy document on the intranet portal' to ascertain whether the document was made available on intranet portal for Zoho associates.</p>	None	None	No Exception Noted
CA71	Network diagram detailing the network devices such as firewalls, Routers and switches is maintained by the NOC Team. The Network Diagram is Reviewed and Approved by the NOC Manager/L3 Engineer on an Annual Basis.	Inspected the network diagram and email communication relating to review of network diagram for aspects such as 'Scope', 'Network devices', 'Prepared by', 'Approved by' and 'Approved on' to ascertain whether network diagram detailing the network devices such as firewalls, Routers and switches was maintained by the NOC Team and whether the network diagram was reviewed and approved by the NOC Manager/L3 Engineer on an Annual Basis.	None	None	No Exception Noted.
CA72	Network level Business Impact Assessment (BIA) is performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.	Inspected the business impact assessment report for aspects such as 'Date of business impact assessment', 'Preparer', 'Reviewer', 'Approver', 'Type of system' and 'Name of service' to ascertain whether network level Business Impact Assessment (BIA) was performed by the NOC team and reviewed by NOC L3 Engineers/Manager and Approved by NOC Managers on an annual basis.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA73	Zoho has implemented measures to monitor the network in order to detect any attacks from the external network.	Inspected DDoS configuration for aspects such as 'Datacenter', 'DdoS Monitored by' and 'Availability of summary report' to ascertain whether Zoho had implemented measures to monitor the network in order to detect any attacks from the external network.	3.11.8	3.12.2	No Exception Noted.
CA74	VLAN Segregation is established for NOC Room. Request for creation/changes of VLAN is requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs. Upon approval, the request is processed by the NOC Team.	<p>Inspected the VLAN interface configuration for aspects such as 'VLAN description' and 'IP Address' to ascertain whether VLAN Segregation was established for NOC Room.</p> <p>Further inspected for sample VLAN creation/changes, the ticket from Creator application for aspects such as 'Request ID', 'Requested by', 'Approved by', 'Approved on' and 'Processing status' to ascertain whether request for creation/changes of VLAN was requested by Sysadmin Team (in the case of Corporate offices) or by the Server Operations team (in the case of IDCs). Managers / L3 of the Sysadmin team or Server Operations team approve / deny the requests based on the provided inputs and whether upon approval, the request was processed by the NOC Team.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA75	The NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool. For the changes to the firewall, the approval is obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.	Inspected for sample firewall rule changes, the firewall rule change ticket from Creator application for aspects such as 'Request ID', 'Datacenter', 'Requested by', 'Approved by – First level', 'Approved on – First level', 'Approved by – Second level', 'Approved on – Second level' and 'Processing status' to ascertain whether the NOC team adds / removes / modifies firewall rules based on the requests raised by Zoho Product Teams/Sysadmin Team/ Server Operations Team through the Firewall Access Form in the Zoho Creator tool and whether for the changes to the firewall, the approval was obtained from the respective Product Manager and also from the Sysadmin or Server Operations team as a second level approval.	None	None	No Exception Noted.
CA76	On a half-yearly basis, the NOC Engineers review the existing firewall rules and the same is approved by the NOC Manager/ L3 Engineer. In the case of any deviations noted during the firewall review, the NOC Engineer makes the necessary changes in the firewall ruleset.	Inspected for sample half year the firewall rule review reports of inscope locations for aspects such as 'Datacenter', 'Request ID', 'Reviewed on', 'Reviewed by', 'Approval details' and 'Deviation and Closure details' to ascertain whether on a half-yearly basis, the NOC Engineers reviewed the existing firewall rules and the same was approved by the NOC Manager/ L3 Engineer and whether in the case of any deviations noted during the firewall review, the NOC Engineer made the necessary changes in the firewall ruleset.	None	None	No Exception Noted.
CA77	Access to Corporate VPN is authenticated with Zoho users' AD account.	Inspected the VPN authentication configuration for aspects such as 'LDAP integration' and 'TFA configuration' to ascertain whether access to Corporate VPN was authenticated with Zoho users' AD account.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA78	Zoho ensures availability of data centers through redundant networks in the data centers. Redundancy of internet connectivity is also ensured via utilization of separate ISP.	Inspected the NOCMON network dashboard for aspects such as 'Name of DC', 'ISP of DC' and 'ISP of Peer DC' to ascertain whether Zoho ensures availability of data centers through redundant networks in the data centers and whether Redundancy of internet connectivity was also ensured via utilization of separate ISP.	None	None	No Exception Noted.
CA79	Admin Access to Firewall, Event log analyzer and Network Configuration Manager is restricted to NOC Engineers and Senior NOC Engineers	Inspected the user listing from Firewall, Event log analyzer and Network Configuration Manager for aspects such as 'User listing' and 'Type of access' to ascertain whether admin access to Firewall, Event log analyzer and Network Configuration Manager was restricted to NOC Engineers and Senior NOC Engineers.	None	None	No Exception Noted.
CA80	When the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raises a request via the Change Control Form in the Zoho Creator tool which is approved by the NOC Manager/ L3 Engineer.	Inspected for sample configuration/ device changes, the ticket from Zoho creator tool for aspects such as 'Request ID', 'Datacenter', 'Requested by', 'Approved by', 'Approved on' and 'Processing status' to ascertain whether when the NOC team undertakes configuration/ device changes, the Senior NOC Engineer raised a request via the Change Control Form in the Zoho Creator tool which was approved by the NOC Manager/ L3 Engineer.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA81	Network devices are monitored using NOCMON and Event Log Analyzer Tool. Alerts are auto-generated in SDP portal for which the NOC teams tracks to closure.	Inspected the SDP Portal and alert configuration from NOCMON and Event log analyzer tool for aspects such as 'Type of integration' and 'Alert generated to'; Further inspected for sample alerts the 'Alert triggered from', 'Request ID', 'Ticket opened on', 'Ticket closed on' and 'Ticket closed by' to ascertain whether network devices were monitored using NOCMON and Event Log Analyzer Tool and whether alerts were auto-generated in SDP portal for which the NOC teams tracked to closure.	None	None	No Exception Noted.
CA82	The NOC team uses Network Configuration Manager tool to backup network device configuration on a daily basis (full backup). In case of a backup failure, an automated email is triggered and remediation action is taken by NOC team.	Inspected backup configuration from Network Configuration Manager tool for aspects such as 'Datacenter', 'Devices backed up', 'Frequency of backup' and 'Backup alert sent to'; Further inspected for sample dates the backup logs for aspects such as 'Device ID', 'Backup generated on', 'Status' and 'Follow up action' to ascertain whether the NOC team used Network Configuration Manager tool to backup network device configuration on a daily basis (full backup) and whether in case of a backup failure, an automated email was triggered and remediation action was taken by NOC team.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA83	Access creation, modification and revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations is performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.	<p>Inspected for sample access creation and access modification, the tickets from Zoho creator tool for aspects such as 'Request ID', 'Raised on', 'Raised for', 'Access required to tool', 'Approver by', 'Approved on' and 'Access granted on' to ascertain whether access creation and modification to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations was performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.</p> <p>Further inspected for sample access revocation, the tickets from Zoho creator tool for aspects such as 'Request ID', 'Raised on', 'Raised for', 'Access required to tool', 'Access revoked on' and 'Date of access revocation' to ascertain whether access revocation to ManageEngine Event Log Analyzer and ManageEngine Network Configuration Manager used for performing NOC's daily operations was performed by Senior NOC member based on approval by NOC L3 Engineer/ NOC Manager on a timely basis.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA84	Zoho Server Operations team has defined data center operations document which specifies procedures relating to day-to-day operations of Server Operations including procedures for degaussing the disks. The document is reviewed by Data Center Manager and approved by Data center member leadership staff on an annual basis.	Inspected the Data center operations document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Server Operations team had defined data center operations document which specified procedures relating to day-to-day operations of Server Operations including procedures for degaussing the disks and whether the document was reviewed by Data Center Manager and approved by Data center member leadership staff on an annual basis.	None	None	No Exceptions Noted.
CA85	Zoho Server Operations team has defined OS Hardening guidelines for servers as part of Server Operations procedure. The document is reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.	Inspected OS Hardening guidelines of server for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Server Operations team had defined OS Hardening guidelines for servers as part of Server Operations procedure and whether the document was reviewed by Manager – Server Operations and approved by the Senior Manager – Server Operations on an annual basis.	None	None	No Exceptions Noted.
CA86	Access to IDC Landing Access Machine and IDC server is provided by Server Operations team member based on the approval from the Server Operations Manager.	Inspected for sample access creation to IDC landing machines, the tickets for aspects such as 'Request ID', 'Approved by', 'Approved on', 'Access granted by' and 'Access granted on' to ascertain whether access to IDC Landing Access Machine and IDC server was provided by Server Operations team member based on the approval from the Server Operations Manager.	None	None	No Exceptions Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA87	Access to IDC Landing Access Machine and IDC server is revoked by Server Operations team member based on the HR notification on a timely manner.	Inspected for sample access revocation to IDC landing machines, the tickets for aspects such as 'Request ID', 'Notification sent by', 'Notification sent on', 'Last working date as per HR', 'Access revoked by' and 'Access revoked on' to ascertain whether access to IDC Landing Access Machine and IDC server was revoked by Server Operations team member based on the HR notification on a timely manner.	None	None	No Exceptions Noted.
CA88	The Server Operations team has configured the ZAC tool for daily incremental and weekly full backups of the database servers. The backups are retained for a period of 3 months. In case of a backup failure, an automated email is sent to the Server Operations team and corrective action is taken.	Inspected for sample servers, the backup configuration from ZAC tool for aspects such as 'Type of server', 'Server IP', 'Backup frequency' and 'Backup retention'; Further inspected for sample dates/weeks the backup logs for aspects such as 'Date of backup', 'Backup status' and 'Follow up action taken' to ascertain whether the Server Operations team had configured the ZAC tool for daily incremental and weekly full backups of the database servers and whether the backups were retained for a period of 3 months and whether in case of a backup failure, an automated email was sent to the Server Operations team and corrective action was taken.	None	None	No Exception Noted.
CA89	Backup restoration requests are received from the customers to the respective Product Support Team. The Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handles the backup restoration in relation to the cloud-based services within the agreed SLA.	Inspected for sample backup restoration requests, the ticket for aspects such as 'Request ID', 'Service type', 'Backup path', 'Restoration path', 'Status', 'Requested on', 'Closed on', 'SLA details' and 'Handled by' to ascertain whether backup restoration requests were received from the customers to the respective Product Support Team and whether the Product Support Team routes the request to Server Operations team through Zoho Creator tool, who handled the backup restoration in relation to the cloud-based services within the agreed SLA.	3.11.4	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA90	IDCs are set up with redundant database clusters to ensure mirroring of customer data. Customer data is mirrored in a separate geographic location to ensure BCP/DR.	Inspected the ZAC tool for aspects such as 'Datacenter', 'Master- Slave configuration', 'Sync Interval' and 'Type of sync' to ascertain whether IDCs were set up with redundant database clusters to ensure mirroring of customer data and whether customer data was mirrored in a separate geographic location to ensure BCP/DR.	None	None	No Exception Noted.
CA91	The Server Operations team monitors the availability of Zoho service from different geographical locations across globe using the Site24x7 tool. In case an error is detected in the Site24x7 tool, automated emails alerts are sent to respective application team and Server Operations Teams. Corrective action is taken by the Server Operations Engineers and RCA is documented by the incident management team.	<p>Inspected the alert configuration from Site24x7 application for aspects such as 'Locations monitored', 'Display name' and 'Parameters' to ascertain whether the Server Operations team monitored the availability of Zoho service from different geographical locations across globe using the Site24x7 tool.</p> <p>Further inspected for sample alerts, the ticket from creator tool for aspects such as 'Incident ID', 'Customer affected', 'Service impacted', 'Closed by' and 'Availability of RCA' to ascertain whether in case an error was detected in the Site24x7 tool, automated emails alerts were sent to respective application team and Server Operations Teams and whether corrective action was taken by the Server Operations Engineers and RCA was documented by the incident management team.</p>	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA92	Zoho has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodical basis, the Server Operations team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.	<p>Inspected business continuity plan document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho had a Disaster Recovery Data Center (DR DC) to ensure the business continuity.</p> <p>Inspected the annual DR Testing report for aspects such as 'Datacenter', 'disaster recovery testing details', 'test results' and 'approval details' to ascertain whether on a periodical basis, the Server Operations team switched the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan (BCP) / Disaster Recovery (DR) readiness.</p>	3.11.8	None	No Exception Noted.
CA93	The Server Operations team monitors the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.	Inspected the MI tool for aspects such as 'Datacenter', 'Dashboard URL' and 'Service Monitored'. Further inspected the tickets for sample alerts generated to ascertain whether the Server Operations team monitored the performance of the servers using the MI tool for monitoring of hard-drive failures, storage and memory usage.	None	None	No Exception Noted.
CA94	Log of activities performed by users in IDC servers are captured and stored after each session in the Zoho Logs server and the same is available for review.	Inspected for IDC logs for aspects such as 'Name of DC', 'Fields monitored', 'Reviewed by', 'Reviewed on' and 'Retention period' to ascertain whether log of activities performed by users in IDC servers were captured and stored after each session in the Zoho Logs server and the same was available for review.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA95	MI tool is used to ensure time sync for IDC Servers. The MI tool is synchronized to a trusted public time source of the GPS.	Inspected the MI tool for sample servers the time sync configuration for aspects such as 'Product name', 'Server hostname', 'Status of time sync' and 'Time sync source' to ascertain whether MI tool was used to ensure time sync for IDC Servers and whether the MI tool was synchronized to a trusted public time source of the GPS.	None	None	No Exception Noted.
CA96	The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.	Inspected for sample failed hard disk drives, the email communication relating to disposal approval for aspects such as 'Datacenter', 'Degaussed on', 'Disposed/replaced on', 'Approved by' and 'Approved on' to ascertain whether the failed hard disk drives were degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/ replacement.	None	None	Exception Noted. Refer Exception #5
CA97	Patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs are initially tested in a local environment/ test lab, then moved to a DR DC following which these changes are implemented in the IDC after obtaining approval from the Server Operations Manager.	Inspected for sample patches and upgrades, the ticket relating to patches for aspects such as 'Patch ID', 'Applicable DC', 'Patch tested by', 'Patch tested on', 'Deployed DC', 'Deployed on' and 'Approval details' to ascertain whether patches and upgrades in relation to the infrastructure (Operating System and Databases) within the IDCs were initially tested in a local environment/ test lab, then moved to a DR DC following which these changes were implemented in the IDC after obtaining approval from the Server Operations Manager.	None	None	No Exception Noted.
CA98	Privileged access to servers is restricted to authorized personnel from the Server Operations team.	Inspected the privileged access user listing for the sample servers for aspects such as 'Product name', 'Server name', 'Type of access', 'Role as per HR' and 'User list' to ascertain whether privileged access to servers was restricted to authorized personnel from the Server Operations team.	3.11.1	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA99	Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restrict unauthorized access into Zoho network.	Inspected for sample web servers the internet connection status for aspects such as 'Product name', 'Server hostname', 'Internet connection status', 'load balancer ID' and 'DMZ Firewall rules' to ascertain whether Zoho hosts the web servers in a demilitarized zone with load balancers and firewall that restricted unauthorized access into Zoho network.	None	None	No Exception Noted
CA100	Access to external storage devices and internet are disabled on IDC servers to prevent data loss.	Inspected for sample servers, the external storage block configuration and network configuration for aspects such as 'Host name', 'Status of external storage block' and 'Status of internet block' to ascertain whether access to external storage devices and internet were disabled on IDC servers to prevent data loss.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA101	Access creation, modification and revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations is performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.	<p>Inspected for sample access creation and access modification, the tickets from Zoho creator tool for aspects such as ‘Request ID’, ‘Raised on’, ‘Raised for’, ‘Access required to tool’, ‘Approver by’, ‘Approved on’ and ‘Access granted on’ to ascertain whether access creation and modification to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations was performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.</p> <p>Further inspected the AD/IAM integration for aspects such as ‘Tool name’ and ‘AD/IAM integration’ to ascertain whether access revocation to Site24x7, ZAC, SDP, Password Manager Pro used for performing Server Operation team’s daily operations was performed by Senior Server Operation member based on approval by Server Operation manager on a timely basis.</p>	None	None	No Exception Noted
CA102	Password of tools used in Zoho are configured as per the approved password policy.	Inspected password configuration for the tools and password policy for aspects such as ‘type of authentication’, ‘password configured’ and ‘compared with password policy’ to ascertain whether password of tools used in Zoho were configured as per the approved password policy.	None	None	No Exception Noted
CA103	Privilege access to tools used in Zoho is restricted to authorized associates.	Inspected user access listing for the tools for aspects such as ‘username’, ‘Role Assigned’ and ‘HR Job role’ to ascertain whether privilege access to tools used in Zoho was restricted to authorized associates.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA104	Zoho Legal Team has defined Privacy Policy which specifies limitation of collection, processing of information, notice, uses and disclosure of information. The document is reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.	Inspected the privacy policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Legal Team had defined Privacy Policy which specified limitation of collection, processing of information, notice, uses and disclosure of information and the document was reviewed by Senior Corporate Counsel and approved by General Counsel on an annual basis.	None	None	No Exception Noted
CA105	Zoho Privacy team has defined a Data Retention and Disposal Procedure as part of Privacy Policy Document which specifies the expectations towards disposal of client information upon discontinuation of Zoho services. The document is reviewed by member of legal team and approved by the General Counsel on an annual basis. The document is made available on corporate website for end users.	<p>Inspected the data retention and disposal procedure document for the aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Privacy team had defined a data retention and disposal procedure as part of Privacy Policy Document which specified the expectations towards disposal of client information upon discontinuation of Zoho services and whether the document was reviewed by member of legal team and approved by the General Counsel on an annual basis.</p> <p>Further inspected for sample associates for aspects such as 'Host name', 'Availability of policy document on the intranet portal' to ascertain whether the document was made available on corporate website for end users.</p>	3.11.3	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA106	<p>The member of legal team reviews the privacy notice and documents his / her approval that the notice includes the following disclosures:</p> <p>1) Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information</p> <p>2) Policies regarding retention, sharing, disclosure, and disposal of their personal information</p> <p>3) The mechanism(s) to access, make changes to, or make inquiries regarding their personal information</p> <p>4) Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection.</p>	<p>Inspected the Privacy Policy and Review details for aspects such as 'policy name', 'contents of policy', 'version no.', 'prepared by', 'reviewed by', 'approved by', 'date of approval' to ascertain whether the member of legal team reviewed the privacy notice and documents his / her approval that the notice satisfied the criteria specified in the control activity</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA107	Based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.	Inspected for sample request raised from the customers the MSA agreement for aspects such as 'Name of customer', 'Type of service', 'Agreement signed by', 'Agreement signed on' and 'Content of agreement' to ascertain whether based on the request from customers, Zoho enters into a Master Service Agreements ('MSA') with them for Zoho applications and whether the agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the Zoho Applications.	3.11.2	None	No Exception Noted
CA108	Zoho Legal team is responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.	Inspected the Responsibility Matrix and Privacy Policy for aspects such as 'Responsibility' , 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether Zoho Legal team was responsible to oversee the contractual and regulatory requirements within Zoho environment including data privacy and protection.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA109	The Privacy Team has defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity. The Director of Compliance (DOC) annually reviews cases that involve disagreements over the accuracy of personal data and also denial of data requests from subjects to validate the appropriate justifications provided thereof.	<p>Inspected the privacy policy document for aspects such as 'Content of document', 'Version number', 'Reviewed by', 'Approved by' and 'Approved on' to ascertain whether the Privacy Team had defined policies and procedures to notify data subjects of how to update or correct personal information held by the entity.</p> <p>Inspected the service desk portal and we noted that there were no instances of disagreements involved over the accuracy and completeness of personal information during the examination period.</p> <p>Further, obtained email confirmation from Privacy Head, stating that, that there were no instances of disagreements involved over the accuracy and completeness of personal information during the examination period.</p> <p>Therefore, DHS LLP could not test the operating effectiveness of disagreements involved over the accuracy and completeness of personal information during the examination period</p>	None	None	<p>No Exception Noted</p> <p>The operating effectiveness of disagreements involved over the accuracy and completeness of personal information could not be tested since there were no related activity during the examination period.</p>

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA110	<p>Zoho provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity’s privacy practices). The notice is:</p> <ol style="list-style-type: none"> 1) readily accessible and made available to the data subject. 2) Provided in a timely manner to the data subjects 3) Clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. 4) informs data subjects of a change to a previously communicated privacy notice 5) Documents the changes to privacy practices that were communicated to data subjects. 	<p>Inspected for sample data collection points the evidence of providing privacy notice for aspects such as ‘privacy policy-check box’, ‘privacy policy – agreement option’, ‘account signup page details’ and ‘website URL’ and inspected Privacy Policy hosted in Zoho corporate website for aspects such as ‘contents of the policy- notification of changes’ and ‘date last updated’ to ascertain whether Zoho provided notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes were made to the entity’s privacy practices) and also whether the notice satisfied the criteria specified in the control activity</p>	3.11.6	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA111	<p>Zoho’s Privacy Policy includes the below policy around Choice and Consent:</p> <ol style="list-style-type: none"> 1) Consent is obtained before the personal information is processed or handled. 2) To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. 3) When authorization is required (explicit consent), the authorization is obtained in writing. 4) Implicit consent has clear actions on how a data subject opts out. 5) Action by a data subject to constitute valid consent. 6) Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances. 	<p>Inspected Privacy Policy document for aspects such as ‘name of the policy’, ‘contents of policy’, version no.’, ‘preparer’, ‘reviewer’, ‘approver’ and ‘date of approval’ to ascertain whether Zoho’s Privacy Policy contained information about choice and consent options included the aspects mentioned in the control activity.</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA112	The privacy team has established procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent. The privacy team has also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.	<p>Inspected the Master Activity register for aspects such as ‘reviewed by’, ‘version details’, ‘approved by’ and ‘date of approval’ to ascertain whether the privacy team had established procedures to assess the nature of the information collected to determine whether personal information received required an explicit consent.</p> <p>Inspected for sample activities/products from Master activity register for aspects such as ‘type of activity’, ‘mode of receiving the consent’ and ‘consent seeking process’ to ascertain whether the privacy team had also established procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA113	<p>Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfil the business purpose by</p> <ol style="list-style-type: none"> 1) Reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. 2) Reviewing the privacy policies and personal information collection methods of third parties prior to contract execution. 3) Reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations. 	<p>Inspected Privacy Policy document and Master Activity register for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'preparer', 'reviewer', 'approver', 'date of approval', and 'nature of information collected' to ascertain whether members of the privacy staff determine whether personal information was collected only for the purposes identified in the privacy notice and only the minimum necessary personal information was collected to fulfil the business purpose of the criteria specified in the control activity.</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA114	<p>On an annual basis the privacy team reviews privacy policies and procedures to ensure that personal information is used in</p> <p>1) Conformity with the purposes identified in the entity’s privacy notice. 2) Conformity with the consent received from the data subject. 3) Compliance with applicable laws and regulations.</p>	<p>Inspected Privacy Policy document and Privacy review meeting for aspects such as ‘name of the policy’, ‘contents of policy’, version no.’, ‘reviewed by’ and ‘privacy review meeting content’ to ascertain whether on an annual basis the privacy team reviewed privacy policies to ensure that personal information was required to be used in the criteria specified in the control activity.</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA115	<p>Zoho has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. The policy specifies:</p> <p>1) The system processes in place to delete information in accordance with specific retention requirements.</p> <p>2) Deletion of backup information in accordance with a defined schedule.</p> <p>3) Requires approval by the Director of Compliance (DOC) for information to be retained beyond its retention period and specifically marks such information for retention.</p> <p>4) Annually reviews information marked for retention.</p>	<p>Inspected Privacy Policy and Data Retention document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'preparer', 'reviewer', 'approver' and 'date of approval' to ascertain whether Zoho had documented its personal information retention policies and procedures, which were reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations and also whether the policy contained the contents specified in the control activity.</p>	None	None	No Exception Noted
CA116	<p>The Director of Compliance (DOC) established a 'Subject Access Request Policy' that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data subjects to access their information. The policy is reviewed and approved on an annual basis by the Director of Compliance.</p>	<p>Inspected Subject Access Request Policy for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether the Director of Compliance (DOC) established a 'Subject Access Request Policy' that defined authentication of data subjects into system and how the entity personnel were to respond to requests by data subjects to access their information and also to ascertain whether the policy was reviewed and approved on an annual basis by the Director of Compliance .</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA117	Zoho has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at Zoho. Privacy team report to the Director of Compliance who in-turn reports to the Vice President.	<p>Inspected the RACI Matrix for aspects such as 'Version Number', 'Reviewed by', 'Reviewed on', 'Approved by' and 'Approved on' to ascertain whether Zoho had constituted a Privacy Team which was responsible for implementing and maintaining the data privacy program at Zoho.</p> <p>Further inspected the Employee Tree Structure within Zoho People application for aspects such as 'organization structure', 'employee name', 'role name' and 'reporting details' to ascertain whether privacy team report to the Director of Compliance who in-turn reports to the Vice President.</p>	None	None	No Exception Noted
CA118	On an annual basis, the Director of Compliance (DOC) reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.	<p>Inspected the creator tool and we noted that there were no instances of data subject access request denied during the examination period.</p> <p>Further, obtained email confirmation from Privacy Head, stating that, that there were no instances of data subject access request denied during the examination period.</p> <p>Therefore, DHS LLP could not test the operating effectiveness of this control activity during the examination period</p>	None	None	The operating effectiveness of this control activity could not be tested as there was no related activity during the examination period

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA119	On an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.	Inspected the MOM of the privacy review meeting and privacy notice for aspects such as 'contents of MOM', 'Date of review meeting', 'prepared by', 'approved by', 'date of approval', 'privacy notice' and 'Details of sharing the MOM' to ascertain whether on an annual basis, the Director of Compliance and privacy staff meet to discuss the new types of personal information that was collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that was collected, systems and processes were updated to provide notice to the data subjects.	None	None	No Exception Noted
CA120	The entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.	Inspected the Zoho connect portal/ website and email communication for aspects such as 'sent by', 'sent to', 'sent on', 'subject', and 'contents of email communication-announcement of Privacy Policy', to ascertain whether the entity communicated to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to optout, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of privacy information.	3.11.6	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA121	On an annual basis, the Director of Compliance (DOC) reviews its policies to ensure the definition of “sensitive” personal information is properly delineated and communicated to personnel.	Inspected the Information Classification Policy for Personal and Special Category of Data document for aspects such as, ‘Prepared by’, ‘Contents of the document’, ‘version details’, ‘date of review’ and ‘Reviewed by’; Further inspected the Intranet portal for aspects such as ‘Availability of Information Classification Policy’ to ascertain whether on an annual basis, the Director of Compliance (DOC) reviewed its policies to ensure the definition of “sensitive” personal information was properly delineated and communicated to personnel.	None	None	No Exception Noted
CA122	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.	<p>Inspected Privacy Policy document, Privacy Notice and Privacy Review Meeting for aspects such as ‘policy name’, ‘contents of policy’, ‘version no.’, ‘privacy notice to data subjects’ ‘Privacy regulations review’ and ‘contents of the meeting’ to ascertain whether members of the privacy staff verified that the entity has legal ground to collect data from the data subjects and that such legal grounds were documented prior to Collection.</p> <p>Inspected the sample review performed for activities/products from Master activity register for aspects such as ‘type of activity’, ‘mode of receiving the consent’ and ‘consenting seeking process’ to ascertain whether members of the privacy staff verify, on a test basis, that the entity had requested and received explicit written consent from the data subjects, when such consent was required.</p>	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA123	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.	Inspected the Zoho's customer account creation sign-up webpages and other sample customer facing portals for aspects such as 'sign-up webpage' 'URL name', 'consent details', 'Location specific details' and 'privacy policy link' to ascertain whether the entity's application(s) provided for user interface (UI) screens that had a click button that captured and recorded a data subject's consent before the data subject submitted the information.	3.11.6	None	No Exception Noted
CA124	When consent is required, business unit personnel documented a process for obtaining consent. Updates to the consent process are reviewed and approved by the Director of Compliance (DOC).	Inspected the Consent Guidelines & Consent seeking process document for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether when consent was required, business unit personnel documented a process for obtaining consent and updates to the consent process were reviewed and approved by the Director of Compliance (DOC).	None	None	No Exception Noted
CA125	Requests for disclosure are recorded by business unit personnel (including the date received and specific details regarding the request). When required, consent of the data subject is obtained prior to granting access to data and the rejections are recorded in a repository.	Inspected for the sample disclosure requests recorded and maintained by the Zoho Legal team, Process Document for Legal Disclosures and the minutes of meeting for aspects such as 'Ticker number', 'Status', 'Date of request', 'Type of request', 'Type of data requested', 'Notification to customer', 'Date of request closure', 'Worked and closed by' to ascertain whether requests for disclosure were recorded by business unit personnel (including the date received and specific details regarding the request) and whether when required, consent of the data subject was obtained prior to granting access to data and the rejections were recorded in a repository.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA126	On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information.	Inspected the vendor list for service specific sub processors for aspects such as 'Date of review', 'entity name', 'purpose', 'location of processing' and 'applicable services' to ascertain whether on an annual basis, the privacy staff obtained a list of paid vendors or other third parties and identified those that process personal information.	None	None	No Exception Noted
CA127	Risk assessment is performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.	Inspected for sample third parties, the Risk Assessment performed for aspects such as 'Date of review', 'name of sub processor', 'service description', 'applicable services', 'Risk assessment details' and 'Risk treatment plan' to ascertain whether risk assessment was performed annually by Zoho Privacy Team to assess the risk of third party service providers identified by them and identify suitable risk treatment plan on an annual basis.	None	None	No Exception Noted
CA128	The privacy staff reviews relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. They also review and update the entity's policies for conformity to the requirement.	Inspected Privacy Review Checklist document for aspects such as 'contents', 'version details', 'review details', 'reviewed by', 'approved by' and 'date of approval' to ascertain whether the privacy staff reviewed relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possessed other legal ground to process the data and whether they also reviewed and updated the entity's policies for conformity to the requirement.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA129	Privacy related complaints are investigated to identify whether there were incidents of unfair or unlawful practices and performs follow-up if necessary	Inspected the Privacy incident tickets for sample incidents for aspects such as 'incident title', 'incident type', 'incident start date', 'notification details', 'mitigation details', 'PIA was conducted', 'incident end date' and 'Follow-up' to ascertain whether privacy related complaints were investigated to identify whether performed follow-up if necessary	3.11.5	None	No Exception Noted
CA130	Privacy Impact Assessment (PIA) is conducted for system changes to assess for privacy implications. Personnel who are authorized to make system changes are trained to perform PIA.	<p>Inspected the Privacy Impact Assessment Report document for sample changes in the manual tracker for aspects such as 'description of request', 'change request – document name', 'approved by', 'date of approval', 'residual risk and mitigation measures' to ascertain whether Privacy Impact Assessment (PIA) was conducted for system changes to assess for privacy implications.</p> <p>Inspected the Privacy Awareness Training deck for aspects such as 'training name', 'contents of deck', 'associate name', 'associate ID', 'Team name' and 'completion date and time' to ascertain whether personnel who were authorized to make system changes were trained to perform PIA.</p>	None	None	No Exception Noted
CA131	An annual review of the organization's data inventory is performed by the Privacy team to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.	Inspected the Master activity register for aspects such as 'field name', 'source of data', 'reason for collection', 'access and storage details', 'retention details', 'reviewed by', 'version details', 'approved by' and 'date of approval' to ascertain whether an annual review of the organization's data inventory was performed by the Privacy team to verify that the documentation was kept current and included the location of the data, a description of the data, and identified data owners.	None	None	No Exception Noted

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA132	Zoho provides updated privacy training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.	Inspected Privacy Awareness Training session viewers report for aspects such as ‘associate name’, ‘viewed date and time’ and also inspected the Privacy Awareness Training deck for aspects such as ‘name of the deck’, ‘presented by’ and ‘contents of deck’ to ascertain whether Zoho provided updated privacy training and awareness to personnel that included defining what constitutes personal information and what personal information was considered sensitive.	None	None	No Exception Noted
CA133	Zoho cloud products provides the log of activities performed by the users. The logs are stored in Zoho logs and access is restricted to the authorized personnel only.	Inspected the log configurations and access list for aspects such as ‘configuration of logs is enabled’, ‘retention period’, ‘product name’, ‘sample log/event’, ‘list of users with access to logs’, ‘designation of users’ to ascertain whether Zoho cloud products provided the log of activities performed by the users and whether the logs were stored in Zoho logs and access was restricted to the authorized personnel only.	3.11.9	None	No Exception Noted
CA134	Zoho has defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials. The Security Head oversees and is responsible for the compliance and identification of ePHI data.	Inspected the HIPAA compliance policy for aspects such as ‘version’, ‘approved by’, ‘reviewed by’ and ‘contents of the policy’ to ascertain whether Zoho had defined an organization wide policy to address and monitor the compliance with HIPAA including the requirements from law enforcement officials and whether the Security Head oversees and was responsible for the compliance and identification of ePHI data.	None	None	No Exception Noted.

#	Control Activity	Tests Performed	CUECs	CSOCs	Results of Tests
CA135	Zoho maintains signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA apply to subcontractors in the same manner as requirements apply to contracts or other arrangements between a covered entity and business associate.	Inspected the sample contracts signed for aspects such as 'subcontractor/business associates', 'date of signature', 'contents of agreement' and 'signed by' to ascertain whether Zoho maintained signed agreements with subcontractors / business associates to acknowledge that requirements of HIPAA applied to subcontractors in the same manner as requirements applied to contracts or other arrangements between a covered entity and business associate.	None	None	No Exception Noted.
CA136	Zoho admin team maintains a register to document the repairs and modifications to the physical components of Zoho facilities that are related to physical access security.	Inspected the register for sample repairs for aspects such as 'date', 'location', 'physical component', 'type of repair', 'date of completion' to ascertain whether Zoho admin team maintained a register to document the repairs and modifications to the physical components of Zoho facilities that were related to physical access security.	None	3.12.1	No Exception Noted.

4.4 Management Responses to Exceptions

The Audit exceptions presented in the Section 4.4 of this report were reviewed and discussed on February 28, 2024, during a dedicated Closing Meeting attended by the Zoho Compliance Team.

The Management Responses to the exceptions noted is as under:

Exception Number	Description of Exception	Trust Services Criteria and Control Activity Impacted by Exception	Management Response to Exception
Exception #1	We noted that for 2 out of 25 sample new joiners, the evidence for completion of induction training was not available.	CA09: Upon a new associate joining, an induction training is conducted by the HR Team to make the associate aware of the information security and Privacy practices and various policies of Zoho. The attendance for the training is captured in Zoho people. Trust Services Criteria : CC1.1, CC1.4, CC2.2 and C1.1	We agree with the exception noted. The same has been actioned upon with appropriate escalation to our senior management after the completion of assessment period. Also, we did not note any security violations for these 2 associates. In addition to this, management periodically communicates the information security and privacy requirements to the associates through email.

Exception Number	Description of Exception	Trust Services Criteria and Control Activity Impacted by Exception	Management Response to Exception
Exception #2	We noted that for 2 out of 25 sample off boarded associates, the physical access was revoked with a delay ranging from 7 to 14 days	<p>CA-14: For associates leaving Zoho, the HR team creates a request for revoking physical access card and the same is actioned upon by the Physical Security team on the last working day.</p> <p>Trust Services Criteria : CC6.4</p>	<p>We agree with the exception noted.</p> <p>However, inspected the access logs for the 2 associates and noted that they did not enter the Zoho facility and Zoho datacenter after their last working day.</p> <p>Going forward, will ensure the physical access will be revoked on their last working day.</p>

Exception Number	Description of Exception	Trust Services Criteria and Control Activity Impacted by Exception	Management Response to Exception
Exception #3	<p>We noted that for 5 out of 25 sample new joiners, IAM accounts were created before joining date ranging from 1 to 8 days.</p> <p>Further, we noted that for 4 out of 25 sample new joiners, domain accounts were created before joining date ranging from 1 to 7 days.</p>	<p>CA52: For associates joining Zoho, the HR team creates IAM account in Zoho People application. The HR team then creates a request for creating AD account and the same is actioned upon by the Sysadmin team.</p> <p>Trust Services Criteria : CC5.2, CC6.1 and CC6.2</p>	<p>We agree with the exception noted.</p> <p>The access was created because of bulk ID creation. However only default IAM and AD access was created and access to application and infrastructure was not provided. Hence no admin activities could be performed with these IDs.</p> <p>The credentials for IAM and AD accounts were shared with the associates only on the date of joining. As per the IAM logs, identified associates did not access the in-scope applications prior to their Date of Joining, also these associates did not have access to in-scope servers and database instances during the assessment period.</p> <p>Going forward, will ensure to activate IDs on the date of joining.</p>

Exception Number	Description of Exception	Trust Services Criteria and Control Activity Impacted by Exception	Management Response to Exception
Exception #4	We noted that password expiry parameter for Zoho Domain (AD) and account lockout and dictionary check parameter for Zero Trust were not in line with Zoho's password policy.	CA62: Security settings for Domain (AD), IAM (Zoho accounts), IAN (Zodoor and IDC) and Zero trust are configured as per Zoho Password Policy. Trust Services Criteria : CC5.2, CC6.1, CC6.2, CC6.3 and CC6.6	<p>We agree with the exception noted.</p> <p>The password expiry for domain accounts and Account lockout and dictionary check for zero trust accounts were not configured in line with the policy. We have initiated the rectification activity for the same.</p> <p>IAM account were used to login into Zoho applications while IAN accounts along with MFA were used to connect to Zoho VPN through which Zoho network components like server, database and network devices were accessed. Both IAM and IAN accounts adhered to Zoho's password policy during the assessment period.</p>

Exception Number	Description of Exception	Trust Services Criteria and Control Activity Impacted by Exception	Management Response to Exception
Exception #5	We noted that for 5 out of 25 sample failed hard disk drives, there is no evidence of approval for degaussing of disks.	<p>CA96: The failed hard disk drives are degaussed by Server Operations team based on the approval provided by Server Operations Managers prior to disposal/replacement.</p> <p>Trust Services Criteria : CC6.1, CC6.5, CC7.2, CC7.3, C1.2, PI1.5 and P4.3</p>	<p>We agree with the exception noted.</p> <p>The asset degaussing was managed by the Server Operations Managers for the 5 instances of disk disposal/replacement. However, evidences for degaussing prior to disposal were available but a formal approval were not recorded.</p> <p>Further, going forward the approvals will be documented as part of the asset disposal process.</p>

Deloitte Haskins & Sells LLP

This material has been prepared by Deloitte Haskins & Sells LLP (“DHSLLP”), on a specific request from you and contains proprietary and confidential information. This material may contain information sourced from publicly available information or other third-party sources. DHSLLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. The information contained in this material is intended solely for you. Any disclosure copy or further distribution of this material or the contents thereof is strictly prohibited.

Nothing in this material creates any contractual relationship between DHSLLP and you. Any mutually binding legal obligations or rights may only be created between you and DHSLLP upon execution of a legally binding contract. By using this material and any information contained in it, the user accepts this entire notice and terms of use.

©2024 Deloitte Haskins & Sells LLP.

Document Reference No RA-TPA-31067111-2024-25-R12