HIPAA Compliance and the Cloud

HIPAA Background

Introduction

Trust with customers is essential for any company. An important way for an organization to develop trust is to commit to protecting the data of its customers. With breaches on the rise and an ever-changing compliance landscape, it is vital to regularly review and scrutinize data protection practices.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a set of rules and regulations passed by the U.S. Congress designed to protect the privacy of individuals' personal health information and ensure the security of personal health information (PHI) and electronic personal health information (ePHI).

What are the HIPAA requirements?

HIPAA includes approximately 152 requirements spread across 10 high-level domains:

1. Management
2. Notice
3. Security (Administrative, Technical, and Physical)
4. Transfer (Disclosure to Third Parties)
5. Integrity (Data Quality)
6. Audit and Monitoring
7. Information Management Lifecycle (Use, Storage, Retention and Disposal)
8. Choice (Consent)
9. Access, Correction, Amendment, and Deletions
10. Breach Notification

To whom does HIPAA apply?

HIPAA applies to providers of health care, health plans, and health care clearinghouse services. These providers are required to handle patient personal health information in a way that meets defined security standards. When providers use third-party vendors or services (Business Associates) where personal health information might be stored, those Business Associates need to adhere to the standards as well. This agreement is contractually defined in a Business Associate Agreement (BAA). For additional information, reference the U.S. Department of Health and Human Services HIPAA covered entities website.

What is considered Personal Health Information (PHI) and electronic Personal Health Information (ePHI)? Is name, birthdate, and address important for HIPAA?

PHI stands for Protected Health Information and is any information in a medical record that can be used to identify an individual, which was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

ePHI is Electronic Protected Health Information and is all individually identifiable health information that is created, maintained, or transmitted electronically by mHealth and eHealth products. This includes PHI on desktop, web, mobile, wearable, and other technology such as email, text messages, etc.

Zendesk Q&A

So now that we better understand HIPAA and its requirements, let's cover ways Zendesk can fit into a compliant HIPAA environment.

How does HIPAA work with cloud service providers like Zendesk?

The term "Business Associate" refers to those entities that perform a service related to: claims processing or administration; data analysis processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. For example, a third party administrator that assists a health plan with claims processing would be considered a HIPAA "Business Associate", and its customers would expect the administrator to be HIPAA compliant on their behalf.

Zendesk supports HIPAA covered customers by entering into Business Associate Agreements (BAA). While customers have the ability to use their Zendesk instance in various ways to meet their business needs, HIPAA covered customers must obtain the correct plan level and appropriately configure their Zendesk access controls and usage to help safeguard protected health information (PHI) from misuse and wrongful disclosure.

Although Zendesk, as a Business Associate, supports HIPAA compliance, ultimately customers are responsible for evaluating their own HIPAA compliance. In addition, Zendesk should not be considered the 'Designated Record Set' holder under HIPAA.

Is Zendesk HIPAA compliant?

As a Business Associate, Zendesk is HIPAA compliant. It should be noted that there is no certification recognized by the U.S. Department of Health and Human Services (HHS) for HIPAA compliance. HIPAA compliance, specifically the relationship between a covered entity and a Business Associate, is a shared responsibility.

In order to provide assurance and external verification, Zendesk undergoes several audits on a regular basis. These audits test Zendesk's documentation and approach to security and privacy for datastores, infrastructure, and operations. Zendesk has at least annual audits for the following certifications:

- SOC 2 Type II (Security & Availability): This report can be obtained under NDA by contacting security@zendesk.com
- ISO 27001 (Cloud Security): Can be obtained by contacting security@zendesk.com or requesting via https://www.zendesk.com/product/zendesk-security/
- ISO 27018 (Cloud Privacy): Can be obtained by contacting security@zendesk.com or requesting via https://www.zendesk.com/product/zendesk-security/

Customers may reference these third party audit reports to determine how Zendesk meets and/or supports their HIPAA compliance program.

I need a HIPAA compliant environment. How do I go about configuring my Zendesk account?

First, the ability to provide controls in line with HIPAA's requirements, for the protection of PHI within our production environment, requires the purchase of certain plan

Levels and services. For information regarding plan levels and in-scope products please consult the Advanced Security Infrastructure page.

Second, provided the products you are purchasing are eligible for HIPAA-enablement, you must do the following in order to have a HIPAA-enabled account:

- You must execute Zendesk's BAA;
    - Please contact your Zendesk account executive if you would like to request a copy of Zendesk's BAA
- You must purchase the Advanced Security Add-on; and
    - Please see this article for more information on the Advanced Security Add-on
- You must enable a set of security configurations in accordance with the security configuration requirements for HIPAA Enabled Accounts found here (note that our security configurations may change from time to time due to changes in law and regulation and changes to the Zendesk Service, so it is always advised to 'follow' this article to be apprised of any changes).
    - For further security information, please contact security@zendesk.com.

Conclusion

Zendesk has the ability to help customers fulfill their HIPAA obligations by providing covered entities and Business Associates with a secure place to store PHI and build their customer relationships.