HIPAA background

Introduction

Your customers are covered under any type of entity for a HIPAA obligation. It's your responsibility to provide the people working on your behalf access to PHI and ensure compliance with HIPAA rules and regulations.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) set the rules for protecting medical information. It applies to individuals and organizations, including business associates (BA) that create, receive, maintain, or transmit PHI in any form, whether electronically or otherwise. HIPAA applies to providers of health care, health plans, and health clearinghouses that handle PHI.

What are the HIPAA requirements?

HIPAA includes, approximately, 250 rules and regulations spanning 11 high-level domain:

1. Management
2. Notice
5. Information Management (Security, Retention, Awareness and Training)
6. Access Controls
7. Audit Trail
8. Breach Notification

To whom does HIPAA apply?

HIPAA applies to providers of health care, health plans, and health clearinghouses that handle PHI. This includes any organization, company, or individual that creates, receives, maintains, or transmits PHI, whether electronically or otherwise. HIPAA applies to both covered entities and business associates (BA) that perform services related to PHI transfer or processing.

What is considered Personal Health Information (PHI)?

Personal Health Information (PHI) is any information that is created, maintained, or transmitted electronically by mHealth and eHealth services. It includes any medical or genetic data, which can be used to uniquely identify an individual.

4.

What is HIPAA compliance?

HIPAA compliance is a set of rules and regulations that must be followed by covered entities and business associates to protect the privacy and security of PHI. Covered entities are responsible for ensuring HIPAA compliance. Business associates are required to sign business associate agreements (BAAs) that outline their responsibilities for protecting PHI.

What are the HIPAA requirements?

The HIPAA requirements include:

- Administrative safeguards
- Technical safeguards
- Physical safeguards
- Breach notification
- Security assessments
- Risk analysis
- Access controls

HIPAA compliance is mandatory for all entities that handle PHI, whether it is a covered entity or a business associate. The requirements are designed to ensure the security and confidentiality of PHI.

HIPAA also requires covered entities to implement policies and procedures to protect PHI. This includes the development of a data security program, privacy policies, and procedures for handling PHI.

How does HIPAA work with cloud service providers like Zendesk?

Zendesk supports HIPAA compliance with a robust set of data security features and controls. Zendesk's platform is designed to handle PHI securely, ensuring that data is protected from unauthorized access or disclosure. Zendesk is committed to maintaining the highest level of compliance with HIPAA requirements.

In order to ensure HIPAA compliance, Zendesk offers the following features and services:

- Advanced Security Infrastructure
- HIPAA Compliant Data Storage
- Data Encryption
- Access Control
- Breach Notification
- Risk Analysis
- Security Assessments
- Privacy Policies

These features and services help Zendesk meet the stringent requirements of HIPAA.

What are the HIPAA requirements?

The HIPAA requirements include:

- Administrative safeguards
- Technical safeguards
- Physical safeguards
- Breach notification
- Security assessments
- Risk analysis
- Access controls
- Privacy policies

HIPAA compliance is mandatory for all entities that handle PHI, whether it is a covered entity or a business associate. The requirements are designed to ensure the security and confidentiality of PHI.

HIPAA also requires covered entities to implement policies and procedures to protect PHI. This includes the development of a data security program, privacy policies, and procedures for handling PHI.