Zaperon

WHITEPAPER

HIPPA Cybersecurity Compliance Made Easy With Zaperon



Introduction

Healthcare organizations manage highly sensitive Personal Health Information (PHI) and Personal Identifiable Information (PII) data, and the increasing complexity of their IT networks presents threat actors with numerous opportunities for cyberattacks. Healthcare providers are witnessing a rapid rise in data breaches with 133 million healthcare records compromised in 2023, according to the HIPAA Journal.

The IBM Cost of a Data Breach Report 2023 reveals that among all the industries, healthcare industry faces the highest cost of a data breach, averaging $10.10 million per incident. This highlights the critical importance of adopting robust cybersecurity measures for healthcare organizations. Ensuring HIPAA compliance is therefore essential for safeguarding patient data and fortifying defenses against evolving cyber threats, and mitigates legal and financial risks incurred due to such incidents.

$10.10 Million

Cost of a data breach is the highest in healthcare industry

Source: IBM Cost of a Data Breach Report 2023



Understanding HIPAA

Compliance with the Health Insurance Portability and Accountability Act (HIPAA), enacted by U.S. legislation in 1996, is a legal obligation for organizations handling Personal Health Information (PHI). The Office of Civil Rights (OCR) of the US Department of Health and Human Services (HHS) is responsible for enforcing the Privacy and Security Rules.

HIPAA, mandates rigorous standards for safeguarding health information, and its cybersecurity requirements are crucial for maintaining the patient privacy and confidentiality, integrity, and availability of PHI.

It establishes standards for the handling of PHI, which includes any information that can be used to identify a patient and their health status. HIPAA's primary components include

- Privacy Rule, which governs the use and disclosure of PHI.
- Security Rule, which sets standards for safeguarding electronic PHI (ePHI).

Over the years, HIPAA has evolved adapting to technological advancements and increasing data security needs.

THREE PILLARS OF HIPAA SECURITY RULE

HIPAA's safeguards fall into three primary categories and each plays a crucial role in ensuring the confidentiality, integrity, and availability of protected health information (PHI).

ADMINISTRATIVE SAFEGUARDS

Policies for managing PHI, including risk assessments, staff training, and access controls, ensure secure handling of patient information.

PHYSICAL SAFEGUARDS

Controlling access to facilities, securing workstations, and managing device disposal protect the physical spaces where PHI is stored.

TECHNICAL SAFEGUARDS

Using technology such as access controls, audit trails, encryption, and secure data transmission methods protect PHI.

Who Needs to Comply?

- Healthcare Providers
- Healthcare Clearinghouses
- Business Associates
- Research Institutions
- Pharmacies
- Health Insurance Companies



Consequences of Non-Compliance

According to the Department of Health and Human Services (HHS), the Office for Civil Rights (OCR) has issued 138 fines for HIPAA violations, totaling more than $137 million, as of early 2024.

FINANCIAL PENALTIES
Fines up to $1.5 million per year.

CRIMINAL CHARGES
Up to 10 years in prison.

CIVIL PENALTIES
Lawsuits from affected individuals.

LOSS OF TRUST
Damage to reputation.

OPERATIONAL DISRUPTION
Increased audits and scrutiny.

LOSS OF BUSINESS
Potential loss of partnerships and contracts.

Cottage Health was fined **$3 million** for failing to implement adequate security measures, resulting in unauthorized access and disclosure of electronic information of 62,500 patients.

Banner Health in Phoenix experienced a hacking incident exposing the PHI of 2.81 million individuals, leading to a **$1.25 million** fine for failures in risk analysis, system reviews & identity verification.

HIPAA Security Rule Compliance with Zaperon's Identity Protection Platform 2.0

ADMINISTRATIVE SAFEGUARDS

Security Management Process

Organizations must conduct risk analyses, implement measures to reduce risks and vulnerabilities, implement a workforce sanctions policy, and implement procedures to review system activity.

COMPLY WITH ZAPERON

Zaperon enforces least privilege access controls based on user roles, device identity, IP address, geo-location, antivirus status, operating system version, and access time. These measures ensure that users can only access the resources and data necessary for their needs, and only from authorized and secure devices. Activities of the privileged users in Zaperon management console are logged for audit purposes.

Workforce Security

Ensure workforce clearance, limit access to ePHI, and terminate access when roles change or employment ends.

COMPLY WITH ZAPERON

Zaperon only allows authorized personnel to access the applications and enables immediate revocation of access for former employees across devices and applications. If any identity threat is detected, Zaperon swiftly blocks access and issues alerts to IT admins.

Information Access Management

Ensure ePHI access is restricted to covered workforce members in hybrid and affiliated organizations.

COMPLY WITH ZAPERON

Zaperon ensures that users are granted access solely to designated applications through authorized and secure devices. Each device is uniquely identified with a PKI-based certificate, and its posture is continuously monitored to guarantee secure access by remote staff from any location.



THE PHYSICAL SAFEGUARDS

Workstation Security

This standard requires Covered Entities and Business Associates to implement safeguards so that physical access to workstations and devices is limited to only members of the workforce with appropriate authorization.

COMPLY WITH ZAPERON

Zaperon implements zero trust access controls and device binding, ensuring users only access necessary resources and data from authorized and secure devices. Zaperon also safeguards user devices from malware attacks by making sure the antivirus or endpoint protection solution is active and working. Additionally, it ensures the operating system is updated to plug any vulnerabilities.

Device and Media Controls

The implementation specifications attached to this standard include the disposal or re-use of media on which ePHI has been stored and maintaining an inventory of devices and media used by the organization to access ePHI.

COMPLY WITH ZAPERON

Zaperon maintains an inventory of user devices that have access to sensitive information and further safeguards data on endpoints by blocking data transfers via USB, Bluetooth, and AirDrop.

TECHNICAL SAFEGUARDS

Access Controls

Implement user identification, password management, automatic logoff, encryption, and emergency access procedures.

COMPLY WITH ZAPERON

Zaperon employs a zero trust framework to ensure multi-factor authentication, ongoing device trust, and proactive identity threat detection. Users are granted access to designated applications only through authorized and secure devices. Security posture of each device is continuously monitored to maintain secure access from any location. Zaperon eliminates passwords using PKI certificate based authentication technology.

Audit Controls

Implement software to record event logs and examine activity on systems containing ePHI.

COMPLY WITH ZAPERON

Zaperon logs all applications accessed by users and the security posture of their devices, offering clear insights through user-friendly dashboards. It also monitors admin user activities with detailed system logs for audit.

Integrity Controls

Implement controls to ensure ePHI is not improperly altered or destroyed, mitigating threats from malicious insiders and external threats.

COMPLY WITH ZAPERON

To secure all types of applications—whether SaaS, on-premise, or desktop—Zaperon employs least privilege access and a phishing-resistant MFA that verifies over 15 factors related to device certificates, user behavior, device posture, and context. This ensures that only authorized users and devices gain access to the applications.

Person or Entity Authentication

Ensure the verification of workforce member identities to comply with access controls and enforce password management policies.

COMPLY WITH ZAPERON

Zaperon enforces identity and access management controls on both users and their devices i.e. users are granted access only to specific applications and only through authorized devices. Each device is uniquely identified with a PKI-based certificate, and its posture is continuously monitored to ensure secure access from any location.



Zaperon Identity Protection 2.0



PKI-BASED PASSWORDLESS AUTHENTICATION

Utilizes PKI for secure, password-free access, reducing data breach risks from compromised credentials.



PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Enhances security with phishing-resistant MFA, incorporating over 15 authentication factors.



CONTINUOUS ZERO TRUST ACCESS CONTROL

Applies zero trust policies continuously, based on user behavior and device status, for ongoing compliance and security.



PROACTIVE IDENTITY THREAT DETECTION AND RESPONSE

Detects anomalies and addresses identity threats proactively, minimizing potential security risks.



COMPREHENSIVE IDENTITY PROTECTION

Delivers robust identity protection through proactive threat detection and response, securing users, devices, applications, and cloud infrastructure.

Zaperon redefines identity protection with its cutting-edge platform, shielding organizations from identity-based attacks. Combining PKI-based passwordless access with phishing-resistant multi-factor authentication, it continuously enforces zero-trust policies based on user behavior and device status. Proactive threat detection and response guarantee strong security for users, devices, applications, and cloud infrastructure.


+1 202 600 5234


+91 8800 170387

sales@zaperon.com

www.zaperon.com

© 2024 Zaperon, Inc.
All Rights Reserved.