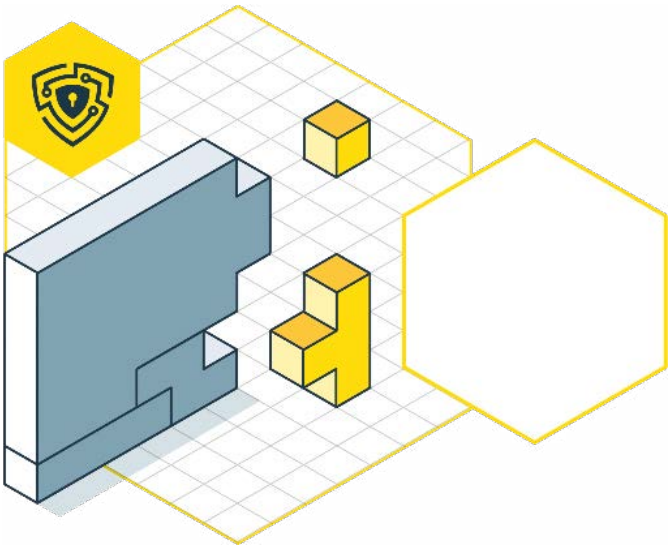
CRASHTEST **SECURITY**

GUIDE FOR HIPAA VULNERABILITIES

WHAT ARE THE STEPS TO KEEP YOUR WEB APP OR API SAFE FROM SUCH VULNERABILITY

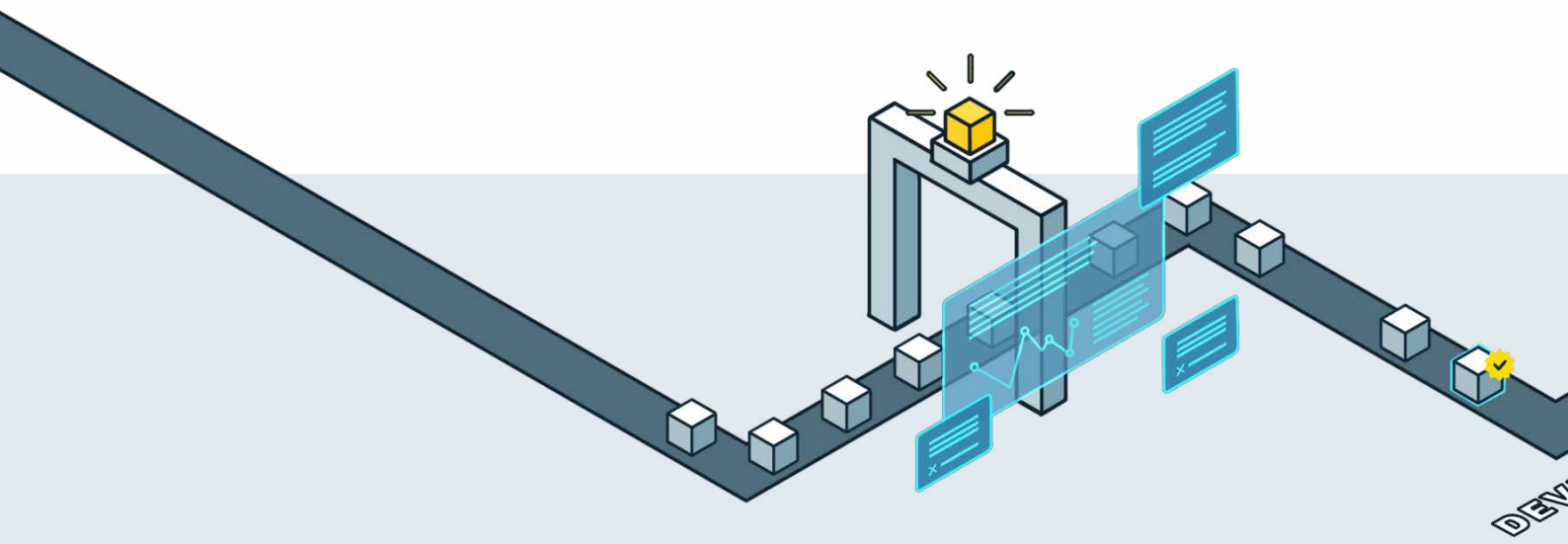
GUIDE FOR THE PREVENTION OF HIPAA ATTACK

Table of Contents



INTRODUCTION TO THIS GUIDE

The Health Insurance Portability and Accountability Act (HIPAA) is a law that stipulates the creation of security standards to safeguard Protected Health Information (PHI). The law focuses on governing the storage and processing of medical records by Health Care Providers and other stakeholders in the healthcare industry.



In traditional healthcare facilities, cybersecurity efforts were initially geared towards protecting legacy systems used to run healthcare operations. With the changing threat landscape, organizations are increasingly adopting security practices, tools, and other administrative safeguards to secure access to healthcare networks and underlying data. To support this, the HIPAA act additionally enlists the legal and technical requirements for protecting critical healthcare assets and keeping medical records safe from the potential risks of a data breach.

Given the sensitivity of Protected Health Information, threat actors target HIPAA vulnerabilities for unauthorized access to critical files and electronic records. This guide discusses various HIPAA vulnerabilities, potential consequences of a HIPAA breach, how such attacks are orchestrated, and standard attack prevention measures.

WHAT IS A HIPAA VULNERABILITY?

Non-conformance with the HIPAA law typically introduces vulnerabilities that lead to attacks on applications with systems running healthcare operations. Personally identifiable health information in such records typically includes social security information, credit files, insurance data, and recent medical history.

HIPAA vulnerabilities are a class of cybersecurity risks that lead to the abuse of confidentiality, availability, and integrity of protected health information in electronic records. Some commonly known HIPAA vulnerabilities include:

Insufficient Transport Layer Security (TLS) encryption

While HIPAA does not explicitly spell out the use of encryption protocols, TLS encryption helps to protect e-PHI data in transit. Modern healthcare systems rely on electronic data transfer to enable collaboration among business associates, covered entities, and other stakeholders involved in the provision of health care. In such instances, the lack of proper TLS encryption causes healthcare systems to be susceptible to man-in-the-middle or other eavesdropping attacks. Such attacks are commonly orchestrated by intercepting communication between two parties/devices, allowing the threat actor to gain unauthorized access to personally identifiable health information.

Lack of authentication/authorization

Healthcare systems with insufficient authentication processes and authorization requirements allow attackers to exploit healthcare networks and subsequently enable them to extract and exfiltrate patient data. Without robust authorization mechanisms and data confidentiality, threat actors can also gain administrative privileges and control access to essential HIPAA services, leading to business disruptions and data breaches.

Remote code execution

RCE is a class of vulnerability that allows cyber actors to execute arbitrary code on target operating systems. Such vulnerabilities enable attackers to orchestrate a wide range of functions on the affected machine, such as **unauthorized access to ePHI data, stealing the identity of the covered entity,** and **exploiting the business from ransomware attacks.**

Directory transversal

This allows the attacker to read critical files within servers hosting HIPAA services. Such files often contain sensitive information, including **company passwords, company budgets, social security entries, patient health plans, organizational security regulations, application source code,** or **crucial operating system files**. Exploits leveraging such sensitive information allow the hacker to alter the application's response, take complete control of the server, and compromise the usability of healthcare services.

TYPES OF HIPAA ATTACKS

HIPAA attacks are categorized according to the cause of the data breach. Types of HIPAA attacks include:

ATTACKS FROM HUMAN SECURITY RISKS

These attacks leverage human knowledge, strengths, and weaknesses to exploit HIPAA vulnerabilities. Human security risks are commonly categorized into:

Human intentional risks

These attacks are usually carried out by terrorists, disgruntled employees, or hackers with malicious intent. Disruptions caused by such attacks typically take time, as the threat actor crafts multiple techniques to beat existing security measures and additional safeguards to steal application data. Examples include phishing attacks to gain unauthorized access, ransomware attacks, and other network-based attacks.

Human unintentional risks

Vulnerabilities that arise from unintended mistakes by an unknown covered entity, business associate, or employees in healthcare organizations, such as inaccurate data entry and accidental data deletion.

ATTACKS TARGETING NON-HUMAN SECURITY

These attacks leverage human knowledge, strengths, and weaknesses to exploit HIPAA vulnerabilities. Human security risks are commonly categorized into:

Technical risks

These risks arise when a healthcare organization ignores the technical requirements for hardening HIPAA services. Non-human technical risks include **exposed secret credentials, unpatched operating systems, running malware,** and **corrupt computer code.**

Functional risks

Potential risks occur when healthcare facilities fail to implement the legal requirements and administrative safeguards to protect e-PHI. Functional risks include **co-enrollment system deployment, insufficient security policies,** and **non-existent cybersecurity incident plans.**

HIPAA VULNERABILITIES - WHAT ARE THE SEVERITY LEVELS?

The potential for damage due to HIPAA vulnerabilities is often extreme and irreversible. A violation of HIPAA compliance comes with several probable consequences, such as:

- **Loss of business revenue** - HIPAA vulnerabilities often lead to ransomware attacks, which subsequently cause monetary loss, including the cost of downtime associated with the breach and the cost of recovery.
- **Damage to reputation** - Business disruptions due to security breaches often lead to reduced trust by the client base. Additionally, the inability to control access to sensitive data also leaves clients doubtful whether to trust such affected health care providers.
- **Criminal penalties** - An affected entity must report to the Office of Civil Rights, which decides the appropriate punishment for the civil damages and business disruptions that arose from the cybersecurity incident. This also adds to the attack's cleaning costs and breach costs.

HOW TO IDENTIFY HIPAA VULNERABILITIES WITH CRASHTEST SECURITY?

The Crashtest Security Suite includes an integrated HIPAA vulnerability scanner to test your APIs or web applications benchmarked against HIPAA compliance standards. The scanner probes the application for any security gaps that allow for unauthorized access to patient data.

Crashtest Security also offers a penetration testing tool that helps security researchers improve the security of health care systems by enabling them to model extreme exploit situations. The platform also provides automated reports with discovered cybersecurity risks, severity levels, and suggested mitigation measures to protect electronic records.

HIPAA VULNERABILITIES PREVENTION TECHNIQUES

Security measures to prevent HIPAA vulnerabilities include:

ENFORCING ADDITIONAL AUTHENTICATION CONTROLS

Implementing access control is considered the best approach to protect sensitive information from unauthorized users. Multi-factor authentication and secure single-sign-on help administer access control mechanisms that ensure robust security for electronic data stored in healthcare apps. These security controls use multiple validation methods and authentication controls to verify any request for access to patient data, further ensuring only authorized personnel can obtain e-PHI records.

ORGANIZATION-WIDE SECURITY AWARENESS TRAINING PROGRAM

As human error or negligence is one of the most significant security risks for healthcare organizations, it is crucial to educate everyone within an organization on the potential risks of a HIPAA attack and help them make careful decisions. An organization-wide cybersecurity program helps each individual to understand their responsibility in maintaining secure healthcare operations and preventing the organization from data breach attacks. The program should adopt HIPAA's security regulations and entail awareness of social engineering techniques such as phishing attacks to reduce the possibility of credential hacking and unauthorized access.

RISK MANAGEMENT POLICY

To secure a healthcare organization's networks from HIPAA vulnerabilities, every HIPAA-covered entity should perform a risk analysis to identify potential security vulnerabilities that can affect protected health information. The risk management policy should essentially factor in imminent threats while assessing the existing security posture of critical healthcare assets.

A comprehensive risk management program should entail:

- Thorough documentation of where protected health information is stored, received, transmitted, processed, and maintained.
- A list of potential risks and vulnerabilities
- An assessment of the effectiveness of security measures and procedures for protecting electronic records
- Possibility of threat actors exploiting a vulnerability
- Potential damage of a cybersecurity incident
- Severity levels for each identified risk
- Mitigations performed to correct security violations/future events

BEST PRACTICES IN PREVENTING HIPAA ATTACKS

Some security practices to prevent HIPAA attacks include:

ENFORCE COMPREHENSIVE LOGGING

A healthcare organization is recommended to keep an audit log of all activities to protect the confidentiality, integrity, and availability of patient information. With an adequately documented log entry and regular monitoring, security professionals can audit unauthorized access attempts to patient data, thereby helping to prevent data breaches. Logs also prove valuable for organizations to identify their weak areas and strengthen security measures. Some of the key activities to include in the audit log include:

A comprehensive risk management program should entail:

- Authentication attempts
- Medical record changes
- Changes to user data and permissions
- Access privileges and critical files accessed
- Any attempts to break access controls

IMPLEMENT A CYBERSECURITY INCIDENT RESPONSE PLAN

As threat actors consistently devise new approaches to targeting medical record data and other personally identifiable health information, security experts must undertake threat modeling and assess the associated risks of ePHI and determine how attackers can leverage them for an attack. While identifying threats and open vulnerabilities are paramount, adopting controls and incident response plans for recovering patient data and mitigating an ongoing breach is equally critical.

The incident response plan should be revised regularly to incorporate technical and administrative safeguards around emerging technologies and exploit patterns with an extending threat landscape. It is also important to include physical safeguards in the incident response plans that protect portable media, workstations, and other devices from intentional human security risks.

IMPLEMENT AUTOMATED VULNERABILITY SCANNING

Attackers leverage vulnerabilities in access control, input validation, deserialization, and TLS encryption to gain unauthorized access to PHI records. An automated vulnerability scanning solution continuously probes applications and information systems for potential risks cyber actors can exploit. Additionally, automated scanning reduces the manual tasks involved in monitoring critical healthcare assets, allowing developers and security professionals to focus on building additional safeguards for threat mitigation.

START AUTOMATED TESTING AND SCANNING TODAY

Crashtest Security offers a suite of vulnerability scanners to help identify HIPAA and other related vulnerabilities. The scanners include an automated HIPAA penetration testing system to help assess the severity of security risks for healthcare organizations and the magnitude of exploitation such risks may cause.

To know more about how Crashtest Security can help your organization secure patients' personally identifiable health information, try a 14-day, free demo today.

Start 2-Week Trial for Free

CRASHTEST **SECURITY**

WWW.CRASHTEST-SECURITY.COM