VERACODE

Developer's Guide to HIPAA Compliance

Steps to keep your web applications and APIs safe and secure

Table of Contents

The Evolution of HIPAA Compliance

HIPAA compliance has become increasingly complex with the introduction of new technologies and software in the healthcare industry. Regardless of their size, nearly all healthtech companies are responsible for maintaining industry-standard privacy and security for their patients.

So, what exactly is HIPAA? This comprehensive guide will answer all your questions about achieving and maintaining compliance.

HIPAA, which stands for Health Insurance Portability and Accountability Act of 1996, is a federal law in the United States that governs the protection of health information. It establishes various security and privacy requirements for managing protected health information (PHI), which includes personal data such as name, date of birth, biometric identifiers, vehicle identifiers, social security numbers, payment information, contact details, and photos.

Protecting PHI has become more crucial than ever, especially with the increasing adoption of cloud computing and digital infrastructure in the healthcare sector.

Safeguarding Protected Health Information

HIPAA regulations apply to companies that handle Protected Health Information (PHI), whether it's in physical or electronic form. This includes various types of data such as health records, medical histories, lab test results, medical bills, account numbers, and images. If you are a covered entity or business associate (or vendor), you are required to comply with HIPAA regulations.

Achieving compliance with HIPAA involves implementing internal procedures, utilizing appropriate technology, and establishing strategic external relationships. Non-compliance can have significant financial implications for your business. However, there are several best practices that health technology entities can follow to ensure continuous HIPAA compliance. Some well-known examples of HIPAA vulnerabilities include:

Insufficient Transport Layer Security (TLS) Encryption

Although HIPAA does not explicitly mandate the use of encryption protocols, implementing TLS encryption is crucial for safeguarding electronic protected health information (ePHI) during transit. In modern healthcare systems, electronic data transfer is essential for collaboration among business associates, covered entities, and other stakeholders involved in healthcare provision.

Without proper TLS encryption, healthcare systems become vulnerable to man-in-the-middle and eavesdropping attacks. These attacks occur when threat actors intercept communication between two parties or devices, enabling them to gain unauthorized access to personally identifiable health information. Implementing robust TLS encryption is essential to prevent such security breaches.

Lack of Authentication / Authorization

Inadequate authentication processes and authorization requirements in healthcare systems create opportunities for attackers to exploit networks and extract patient data. Without robust authorization mechanisms and data confidentiality, threat actors can gain administrative privileges and control access to critical HIPAA services. This can result in business disruptions and data breaches. It is crucial to implement strong authentication and authorization measures to prevent such incidents.

Remote Code Execution (RCE)

Remote Code Execution (RCE) is a critical vulnerability that enables threat actors to execute arbitrary code on target operating systems. Exploiting this vulnerability grants attackers significant control over the affected machine. They can carry out various malicious activities, including unauthorized access to electronic protected health information (ePHI) data, identity theft of covered entities, and launching ransomware attacks. It is crucial to address RCE vulnerabilities promptly to prevent these severe consequences.

Directory Transversal

Directory Traversal is a vulnerability that enables attackers to access critical files within servers hosting HIPAA services. These files often contain sensitive information such as company passwords, budgets, social security entries, patient health plans, security regulations, application source code, and operating system files. By exploiting this vulnerability, hackers can manipulate the application's response, gain complete control over the server, and compromise the functionality of healthcare services. It is essential to address and mitigate directory traversal vulnerabilities to protect sensitive data and maintain the integrity of healthcare systems.

Human and Non-Human Security Threats

HIPAA attacks are categorized according to the cause of the data breach. This can be broadly classified human security risks and non-human security risks.

1.

Attacks from Human Security Risks

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

- **Human intentional risks**
  These attacks are usually carried out by 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, accidental data deletion and poor account management.

2.

Attacks Targeting Non-human Security Risks

- **Technical risks**
  These risks arise when a healthcare organization ignores the technical requirements or 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 ePHI. Functional risks include coenrollment system deployment, insufficient security policies, and non-existent cybersecurity incident plans.

Assessing the Potential Damage

The potential damage of HIPAA vulnerabilities are often extreme and irreversible. A violation of HIPAA compliance can result in with several probable consequences, such as:

1.

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 cost of recovery.

2.

Reputational damage

Business disruptions due to security breaches often lead to a decline in the trust of the client base. Doubts arise in breached healthcare providers who are unable to control access to sensitive data.

3.

Criminal penalties

An affected entity must report to the Office of Civil Rights, which decides the appropriate penalties for the civil damages and business disruptions that arose from the cybersecurity incident. This also adds to the cost of damage control.

Practical Proactive Measures for Protection

Veracode Dynamic Anlaysis integrates a HIPAA vulnerability scanner that tests your applications against HIPAA compliance standards. This scanner identifies vulnerabilities that could potentially lead to unauthorized access to patient data.

By enabling security professionals and developers to simulate extreme exploit scenarios, the platform helps enhance the security of healthcare systems. It generates automated reports that highlight discovered cybersecurity risks, their severity levels, and recommended mitigation measures to safeguard electronic records.

Best Practices for Continuous Compliance

Enforcing Additional Authentication Controls

Implementing access control is crucial for safeguarding sensitive information from unauthorized users. The best approach involves utilizing multi-factor authentication and secure single-sign-on access control mechanisms. These security controls provide robust protection for electronic data stored in healthcare applications.

By employing multiple validation methods and authentication controls, these security measures verify every request for access to patient data. This ensures that only authorized personnel can obtain electronic protected health information (ePHI) records, further enhancing data security.

Organization-wide Security Awareness Training Program

To mitigate the significant security risks posed by human error or negligence in healthcare organizations, it is vital to educate all members of the organization about the potential risks of HIPAA attacks. This education empowers individuals to make informed decisions and contribute to maintaining secure healthcare operations, thereby preventing data breaches.

Implementing an organization-wide cybersecurity program is key to fostering this understanding and promoting responsible behavior. The program should align with HIPAA's security regulations and raise awareness about social engineering techniques like phishing attacks. By educating employees about these techniques, the program reduces the likelihood of credential hacking and unauthorized access to sensitive information.

Risk Management Policy

Every HIPAA-covered entity should perform a risk analysis to identify potential security vulnerabilities that could lead to a breach of protected health information. The risk management policy should 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
- 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

Ensure Your Application is HIPAA Compliant

Enforce Comprehensive Logging

To protect patient information, healthcare organizations should maintain an audit log of all activities. This log, with proper documentation and regular monitoring, allows security professionals to audit unauthorized access attempts, preventing data breaches. It also helps identify weak areas and strengthen security measures. Key activities to include in the audit log are:

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

Implement Application Security Testing

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

Implement A Cybersecurity Incident Response Plan

As threat actors continuously evolve their tactics to target medical record data and personally identifiable health information, it is crucial for security experts to conduct threat modeling and assess the associated risks of electronic protected health information (ePHI). This helps identify potential vulnerabilities and understand how attackers may exploit them.

While identifying threats and vulnerabilities is essential, it is equally important to implement controls and develop incident response plans to recover patient data and mitigate breaches. Regularly revising the incident response plan is necessary to incorporate technical and administrative safeguards that address emerging technologies and exploit patterns in an ever-changing threat landscape. Additionally, physical safeguards should be included to protect portable media, workstations, and other devices from intentional human security risks.

Veracode Dynamic Analysis: Empowering HIPAA Compliance

Veracode Dynamic Analysis is a comprehensive solution for dynamic application security testing. It effectively identifies vulnerabilities related to HIPAA and other regulations, ensuring the protection of user and patient data.

By regularly testing the security of your web apps and APIs, you can proactively safeguard against PII exposures and meet regulatory requirements. With its automated scanner, Veracode Dynamic Analysis helps you navigate certification hurdles and ensure compliance with cybersecurity standards. It specifically addresses security risks associated with personal health information (ePHI), such as SQL Injections, XSS, Privilege Escalation, and other vulnerabilities.

By integrating this solution with the Veracode's Software Security Platform, you can seamlessly incorporate multiple tools and systems into your software development life cycle. This integration allows for the identification of security risks across your entire tech stack, preventing the introduction of new flaws and reducing risk over time.

Experience the benefits of Veracode Dynamic Analysis for yourself with a free, 14-day trial. Discover how it can help you achieve HIPAA compliance effortlessly and strengthen your software against attacks.

Start Your Free, 14-day Trial

VERACODE

Veracode is intelligent software security. The Veracode Software Security Platform continuously finds flaws and vulnerabilities at every stage of the modern software development lifecycle. Prompted by powerful AI trained by trillions of lines of code, Veracode customers fix flaws faster with high accuracy. Trusted by security teams, developers, and business leaders from thousands of the world's leading organizations, Veracode is the pioneer, continuing to redefine what intelligent software security means.

Learn more at **www.veracode.com**,
on the **Veracode blog** and on **Twitter.**