FORTRA™

SOLUTION BRIEF (TRIPWIRE)

THE TRIPWIRE HIPAA SOLUTION

Meeting the Security Standards Set Forth in Section 164

The United States Health Insurance Portability and Accountability Act of 1996, or HIPAA, was enacted to safeguard Protected Health Information (PHI) by mandating procedures and controls to assure the public that critical and private information is controlled from loss of confidentiality, integrity or availability. With few exceptions, an organization is subject to HIPAA if it exchanges data related to the health care profession.

Both HIPAA and the regulatory environment have evolved since 1996. In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) was signed into law as part of American Recovery and Reinvestment Act (ARRA). This law includes new rules that affect the health care industry and those entities that might handle, process or maintain personal health information.

The new rules revolve around two primary areas:

- The mandated adoption of new electronic health record systems (and standards, controls and protections around that adoption)
- The expansion of breach notification rules concerning personal health records

In 2013, the HIPAA Omnibus rule, in a health information technology (HIT) context, was enacted to modify the HIPAA Privacy, Security and Enforcement Rules to implement statutory amendments under the HITECH Act. The HIPAA Omnibus rule has extensive changes to strengthen the security and privacy of PHI, such as extending liability to business associates and increasing penalties with a maximum penalty of $1.5 million per violation. HIPAA and HITECH are separate and unrelated laws, though they do strengthen each other in certain ways. For example, HITECH stipulates that technologies and technology standards created under HITECH do not compromise HIPAA privacy and security laws.

Organizations subject to HIPAA, known as Covered Entities (CE), include:

- Health care providers — doctors, hospitals, etc.,
- Health care insurance and health plan clearing houses,
- Businesses that self-insure; and
- Businesses that sponsor a group health plan and provide assistance to their employees on medical coverage (such as flexible spending accounts).

HIPAA Impact

US Department of Human and Health Services (HHS) is becoming more aggressive with the violations and fines. In the first half 2016 alone, HHS recorded close to $15 million in settlement payments.[1] Healthcare cyber attacks are also on the rise and appear to be shifting their tactics. Healthcare care records are still being stolen and resold on the black market, but the price is dropping, pivoting some of the monetization to ransomware attacks.[2] The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. HIPAA is intended to mandate security processes to evade these cyber attacks. Keep in mind, experiencing a cyber attack is not just a compliance concern — it's a healthcare business concern of loss of service and business.

Your HIPAA Compliance

Meeting the requirements of HIPAA requires most businesses to set up strong processes, methods and controls to assure auditors that the security and integrity of PHI is assured. The specific technical rules are fairly prescriptive, and systems that are in scope for HIPAA should meet both the Act's intention and the implementation instructions as put forth in each section. Below, we illustrate how Tripwire products help address secure processes as dictated by HIPAA Section 164. Additionally, we can show not only how to reach compliance, but maintain it over the long term.

And why is continuous compliance important? Even if an organization is compliant today, unforeseen change is very likely. Most organizations have IT systems that must be updated, modified and maintained to keep running smoothly, which introduces high likelihood that it will drift out of compliance with HIPAA rules.

Fortra's Tripwire has observed that most organizations need both a compliance monitoring system and a change control process that assures only authorized change is introduced to the systems in scope. To demonstrate system integrity one must show a not only a process, but evidence (reports and logs) that assures only authorized change occurs.

Healthcare industry observers see increases in healthcare cyber attacks. Security issues with highly connected electronic health records (EHR) systems and the advent of web-based health record repositories are likely to push new and enhanced rules for electronic PHI (ePHI) and expanded definitions of who is a CE. Are you ready?

Tripwire Solutions and HIPAA

Tripwire solutions offer highly automated foundational controls to meet the security requirements of HIPAA (Section 164), reducing time spent fighting fires caused by poor network and data security practices, and enhancing the data security of ePHI. Tripwire's real time and continuous foundational controls (which include security configuration management, vulnerability management and log management) assure you do not drift from compliance, and are consistently compliant.

Core to the Tripwire solution for HIPAA is high integrity systems management, a policy-based solution that allows you to programmatically analyze critical changes and settings to determine if they are authorized and compliant. Because integrity monitoring is being performed as change occurs, you can actually achieve a continuous state of compliance. Tripwire has a solid track record with many compliance standards (CIS, ISO 27001, PCI, FISMA/NIST, NERC CIP, SOX, COBIT, DISA) as well as HIPAA, and offers over 150 policy templates and audit-ready reports to support these standards.

We also recognize that many healthcare organizations are aligning to National Institute of Standards (NIST) guidelines and framework as well for a security strategy with over 47% healthcare organizations adopting NIST.[3] We encourage you to read our Achieving FISMA brief and other NIST-related briefs.

References

1. http://www.beckershospitalreview.com/healthcare-information-technology/10-largest-hipaa-settlement-fines.html
2. http://securityaffairs.co/wordpress/54666/security/healthcare-cyber-security.html
3. HIMSS Survey 2016

Fortra's Tripwire Helps You Achieve and Maintain HIPAA Section 164

Requirement	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
§ 164.306 Security standards: General rules.				
(a) General requirements. Covered entities and business associates must do the following:				
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Tripwire monitors systems for any unauthorized changes, and discovers and prioritizes vulnerabilities to ensure health data is not compromised. Organizations can correlate events with changes that impact IT policies.	Provides	Provides	Supports
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Tripwire detects unauthorized changes, and discovers and prioritizes vulnerabilities. Organizations can correlate events with changes that impact IT policies.	Provides	Provides	Supports
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Tripwire detects unauthorized changes, and discovers and prioritizes vulnerabilities. Organizations can correlate events with the changes that impact IT policies.	Provides	Provides	Supports
(4) Ensure compliance with this subpart by its workforce.	Tripwire provides policies and documents to ensure certain security efforts.	Provides	Provides	Validates
§ 164.308 Administrative safeguards.				
(a) A covered entity or business associate must, in accordance with § 164.306:				
(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Tripwire monitors systems for any unauthorized changes, and discovers and prioritizes vulnerabilities to ensure health data is not compromised. Organizations get real-time, conditional alerting, which enables them to correlate events with the changes that impact IT policies and security events.	Provides	Provides	Supports
(ii) Implementation specifications:				
(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Tripwire discovers and prioritizes vulnerabilities. Tripwire assesses if your systems are hardened (secure configurations).	Provides	Provides	Supports
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Tripwire discovers and prioritizes vulnerabilities. Tripwire assesses if your systems are hardened (secure configurations).	Provides	Provides	Supports
(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Tripwire can identify infrastructure that has drifted from established secure configurations.	Provides		Validates

Requirement	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Tripwire provides system log information, to support investigations.			Provides
(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Tripwire tracks authorized and unauthorized activities.	Provides		Provides
(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	Tripwire monitors systems for any unauthorized changes, and discovers and prioritizes vulnerabilities to ensure health data is not compromised.	Provides	Provides	Provides
(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Tripwire tracks authorized and unauthorized activities.	Provides		Validates
(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.				
(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.	Tripwire monitors systems for any unauthorized changes, and discovers and prioritizes vulnerabilities to ensure health data is not compromised. Tripwire offers log information for investigations.	Provides	Provides	Provides
(ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Tripwire monitors systems for any unauthorized changes and discovers and prioritizes vulnerabilities to ensure health data is not compromised. Tripwire offers log intelligence, to support investigations.	Supports	Supports	Provides
C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Tripwire maintains system baselines to enable rollbacks if systems have been corrupted.	Supports		
(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	Tripwire can support the testing process with its monitoring capabilities.	Supports		

Requirement	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
§ 164.312 safeguards.				
A covered entity or business associate must, in accordance with § 164.306:				
(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Tripwire tracks authorized and unauthorized activities.	Supports		
(2) Implementation specifications:				
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.				
(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Tripwire maintains system baselines to enable rollbacks if systems have been corrupted.	Supports		
(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Tripwire tracks authorized and unauthorized activities.	Supports		
(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	Tripwire can alert if encryption is on or off. Tripwire validates and reports on the removal of, or changes to, certain types of data, such as cryptographic files and keys, data files, and database tables.	Supports		
(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Tripwire addresses security audit settings and controls that pertain to audit-log behavior. Tripwire monitors system activity and can determine the specific user accounts associated with those events.	Supports		Supports
(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Tripwire (either out of the box or customized) addresses system integrity of information systems that maintain electronic protected health information. In particular, Tripwire features watch files and settings for these controls, and will alert when changes to them take a system out of compliance. Tripwire discovers and prioritizes vulnerabilities.	Provides	Provides	
(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Tripwire addresses security mechanisms that are used to authenticate a system that maintains protected health data. The Tripwire change audit feature monitors system activity, and can determine if and when those controls were changed.	Supports		

Requirement	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire LogCenter
(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Tripwire tracks authorized and unauthorized activities.	Supports		
(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Tripwire tracks authorized and unauthorized activities.	Supports		
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Tripwire addresses security services and security settings that are used to assure system and data integrity. The Tripwire change audit feature monitors system activity and can determine if and when those controls were changed, or take the system out of compliance. Organizations can correlate events with the changes that impact IT policies	Supports		Supports
(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Tripwire can alert if encryption is on or off. Tripwire validates and reports on the removal of, or changes to, certain types of data, such as cryptographic files and keys, data files, and database tables.	Supports		
(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Tripwire supports the rapid detection of data breaches by monitoring systems and discovering vulnerabilities. Tripwire collects, analyzes and correlates log data, enabling IT to detect and respond quickly to security events.	Supports	Supports	Supports

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.