Health Insurance Portability and Accountability Act (HIPAA)

Being a healthcare provider in the United States (a covered entity in HIPAA terminology) requires compliance efforts. The aim of these efforts is to reduce the threat of a breach and to ensure the confidentiality, integrity, and availability of critical and private patient information. Even though HIPAA mandates specific physical, technical, and administrative controls, the smart and thoughtful implementation of essential security controls not only provides for HIPAA compliance, but it also propels a hospital, a physician's clinic, or a health insurance provider into a cyber resilient state.

Healthcare Security Threats and Solutions

There are many examples why protecting and securing critical electronic health information is more important than ever before. Cyber-attacks targeting the health sector occur regularly and show no sign of slowing down, with many cyber criminals shifting their tactics to avoid detection. It doesn't matter whether their aim is to extort money (as we have seen with the various ransomware attacks) or to extract critical information (the attempts to breach vaccine research). In fact, the latest research from HIPAA Journey found a **196% increase in reported healthcare breaches in 2019**, resulting in more than **41,335,889 breached records**. The average cost of a breached healthcare record is $429 compared to the average cost per breached non-healthcare record, which is $150, making ePHI that much more damaging.

The solution healthcare organizations elect to implement should not only provide the needed technical HIPAA compliance, but it also needs to provide the establishment of a stable base to build secure future digital solutions on. The solution must provide the essential, all-encompassing controls, empowering a cyber-resilient healthcare organization to provide health services despite being under attack.

Netwrix solutions combine the essential security controls prescribed by leading frameworks such as HIPAA/HITECH and the Center for Internet Security (CIS), including real-time file integrity monitoring, vulnerability management and log intelligence with the operational discipline of change management and control.

Netwrix products continuously monitors systems for any unauthorized or unapproved changes and prioritizes vulnerabilities to ensure health data is not compromised. This includes preventing the introduction of malware, or even worse, ransomware, which could have potentially devastating consequences on businesses and even human lives.

Technical HIPAA Requirements

Learn more about the technical requirements as stated in HIPAA and which requirements Netwrix can help your organizations fulfill.

HIPAA 164.306 Security standards: General rules	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Provide control over any change happening in the infrastructure, enable the detection of unwanted change, of actions that might affect the C-I-A triad. As a result, C-I-A posture is strengthened. Identify vulnerabilities prior to an attack enhancing the overall cyber security posture making it more difficult for an attacker to use known exploits, reducing the risk of attack.	✓	✓	
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Compare any change of settings, files, or configuration with a list of known 'good' or approved changes protecting the security and the integrity of ePHI addressing even unknown attacks. Checking the infrastructure for vulnerabilities tackles reasonably anticipated attacks, as they are quite often attempting to exploit known vulnerabilities.	✓	✓	
3. Ensure compliance with this subpart by its workforce.	The solution monitors change of any asset by any user, it enables the enforcement and thus maintains compliance.	✓		

HIPAA 164.308 Administrative safeguards	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
1. i. Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	**Implementing Change Control is a proven policy and tested procedure to prevent, detect, contain, and correct violations. Vulnerability Management augments the prevention of security violations as it detects vulnerabilities in an infrastructure, provides correction information, reducing the attack surface.**	✓	✓	
1. ii. 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.	Uses CIS controls to identify risks related to insecure devices and services in the infrastructure. Scanning for vulnerabilities.	✓	✓	
1. ii. 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).	Provides control over any change happening in the infrastructure, enables the detection of unwanted change, of actions that might affect the C-I-A triad. As a result, C-I-A posture is strengthened. Identifies vulnerabilities prior to any attack enhancing the overall cyber-security posture making it more difficult for an attacker to use known exploits, making the organization as less viable target.	✓	✓	

HIPAA 164.308 Administrative safeguards	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
1. ii. 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.	Change Control enables the detection of user activity which violates security policies, a basic step needed to apply sanctions.	✓		
1. ii. B. 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.	Change Tracker's and Greenbone Enterprise's logs can be reviewed and filtered in the products as well as forwarded to a third-party log analyzing solution.	✓	✓	

HIPAA	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
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.	Deploy effective hardening to the end point to ensure only authorized users have access to resources and auditing is configured to track successful and failed access attempts. Deploy Netwrix Log Tracker to collect audit information in a central repository.	✓		✓
3. ii. C. Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Deploy local user tracking to gather lists of current users and groups on individual systems and run reports against groups which look for the presence of a specific user. Utilize process output tracking to gather user data from systems and applications. Incorporate user-based process output tracking into a baseline report to compare against a system or groups of systems.	✓		
164.308 Administrative safeguards				
1. i. Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Implementing Change Control is a proven method to prevent, detect, contain, and correct violations. In addition to Change Control, Vulnerability Management augments the prevention of security violations as it detects vulnerabilities in an infrastructure, provides correction information, and reduces the overall attack surface of a covered entity.	✓	✓	

HIPAA	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
5. ii. B. Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	Change Control enables the detection of malicious software by monitoring all unplanned changes across all systems.	✓		
5. ii. C. Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Use Change Tracker's CIS reports to configure the correct level of auditing on systems. Use the auditing data produced by the Change Tracker hardening to collate logon information.			✓
5. ii. D. Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	Change Control can monitor password quality and settings for password management. Greenbone Enterprise checks for the use of default passwords.	✓	✓	
6. i. Standard: Security incident procedures. Implement policies and procedures to address security incidents.	Uses CIS controls to identify risks related to unsecure devices and services in the infrastructure. Scanning for vulnerabilities.	✓	✓	
6. ii. D. 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.	Change Tracker can identify known security issues like insecure configurations, reports them and recommend mitigation steps. Greenbone enterprise can identify known vulnerabilities, reports about them and supports mitigation efforts.	✓	✓	

HIPAA	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
7. ii. 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.	Harden the infrastructure assets to ensure systems are fit for purpose and then monitor for change actively.	✓		
8. Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Periodic or continuous technical evaluation is a basic feature of Change Tracker and Greenbone Enterprise.	✓	✓	
164.310 Physical safeguards				
A covered entity or business associate must, in accordance with § 164.306:	Change Tracker allows for the monitoring of baselines, the continuous monitoring of updates, whether a device is connected and if it is configured and operating according to specs. It can verify whether logs of access control devices used in Building Management Systems have been altered.	✓		

HIPAA 164.312 Technical safeguards	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
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).	Use Change Tracker CIS reports to configure the correct level of systems auditing. Use the auditing data produced by the Change Tracker hardening to collate logon information. Audit successful access against a known allowed list.	✓		✓
2. ii. Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Uses CIS controls to identify risks related to insecure devices and services in the infrastructure. Scanning fo Use Change Tracker CIS reports to configure the correct level of systems auditing. Deploy baseline reporting to collect preferred system state.	✓		✓
2. iv. Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	Change Tracker supports the requirement by verifying whether a certain asset is encrypted as needed.	✓		
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.	Use Change Tracker CIS reports to configure the correct level of systems auditing. Use the auditing data produced by the Change Tracker hardening to collate logon information. Audit successful access against a known allowed list.	✓		

HIPAA 164.312 Technical safeguards	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
c.1. Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Change Tracker detects changes to files, settings, and alerts operations to unwanted change.	✓		
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.	Change Tracker detects changes to files, settings, and alerts operations to unwanted change.	✓		
b. 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.	Harden the end point to ensure only authorized users have access to resources and auditing is configured to track successful and failed access attempts. Deploy Netwrix Log Tracker to collect audit information in a central repository.	✓		✓
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.	Harden the end point to ensure only authorized users have access to resources and auditing is configured to track successful and failed access attempts. Deploy Netwrix Log Tracker to collect audit information in a central repository.	✓		✓

HIPAA 164.312 Technical safeguards	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
2. 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.	Change Tracker detects changes to files, settings, and alerts operations to unwanted change.	✓		
2. ii. Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Change Tracker detects changes to files, settings, and alerts operations to unwanted change, ensuring that any changes to encryption settings is identified.	✓		

HIPAA 164.404 Notification to individuals	Netwrix Solution	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
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).	Change Tracker can identify known security issues like insecure configurations, reports them and recommends mitigation steps. Greenbone Enterprise can identify known vulnerabilities, reports about and supports mitigation efforts.	✓	✓	

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social