



How to meet HIPAA compliance and achieve a Cyber Resilient State with NNT

Being a healthcare provider in the United States – a covered entity in HIPAA speak – 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**, it propels a hospital, a physician's clinic, or a health insurance provider into a cyber resilient state.

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 price of a breached healthcare record costs \$429 compared to the average cost per breached record, which is \$150, making ePHI that much more attractive to attackers. Next to consider are the consequence of downtime and the cost associated with that, as the analysis of Comparitech shows.

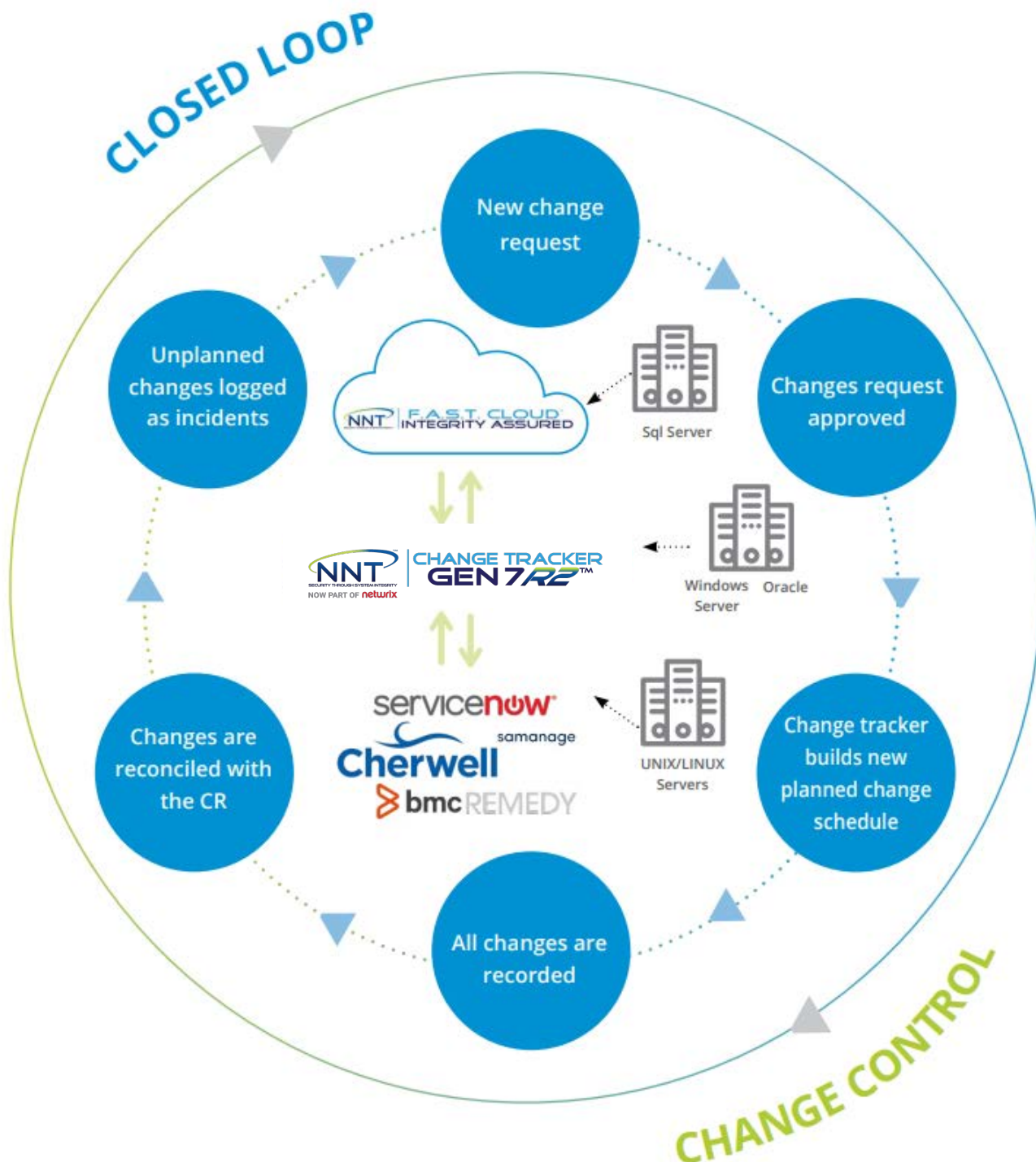
Looking beyond that, as the healthcare sector is looking at ways to reap benefits from digitalization for treatment efficacy and in a patient's journey through healthcare:

- ➔ By providing mobile apps and platforms for medical services
- ➔ By employing artificial intelligence and data analytics tools for patient-centric care programs
- ➔ By using Internet-connected sensors for a feedback loop between patients and clinicians

Attackers will see many more attack vectors to exploit. The solution healthcare organizations elect to implement should not only provide the needed technical HIPAA compliance, it also needs to provide the establishment of a stable base to build those 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.



NNT & HIPAA COMPLIANCE



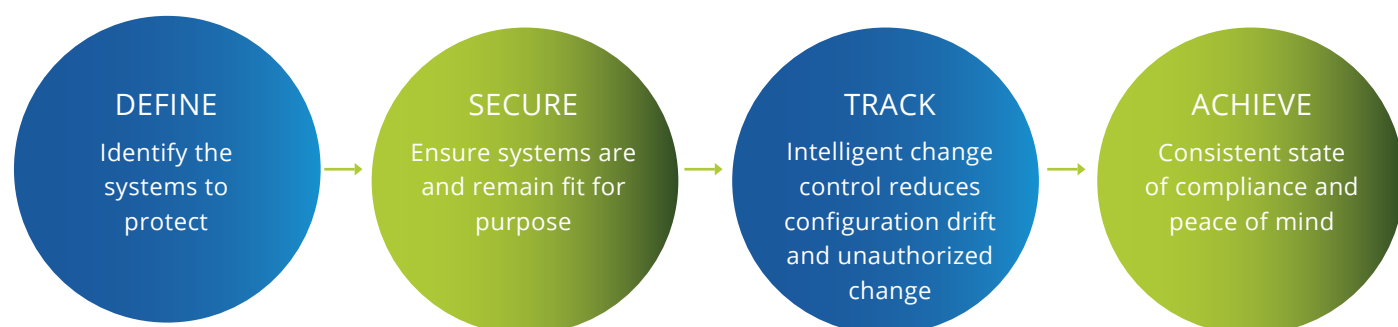
NNT's SecureOps™ technology suite can help your organization achieve and maintain a state of resilience, to ensure the integrity of all your systems, including servers, critical workstations, and network devices, and cyber-physical devices with the ability to protect against internal and external threats. NNT 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.

NNT 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.

KEY FEATURES & BENEFITS

- ➔ Context-based File Integrity Monitoring and File Whitelisting to ensure that change activity is analyzed and validated in real-time
- ➔ Intelligent pattern matching, self-learning change DNA technology to determine whether changes are suspicious or potentially harmful
- ➔ Forensic detail of changes including who made the change, how they changed, and where they originated from
- ➔ Real-time CIS and DISA STIG configuration hardening to ensure systems remain securely configured at all times
- ➔ Continuous compliance and assurance with customizable or pre-built, audit-ready HIPAA reports to help you save limited time and resources and jumpstart your compliance audit
- ➔ Baseline oriented management to fix baseline configuration settings that make up your hardened build standard and identify any drift
- ➔ Change noise reduction by more than 90%, leaving unwanted, unexpected, and potentially malicious changes for you to review and remediate
- ➔ Vulnerability Trackers scans for all known vulnerabilities using over 80,000 automated network vulnerability tests

How Change Tracker Works





TECHNICAL REQUIREMENTS

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

HIPAA Compliance Requirement	Does NNT Address this Requirement?	How NNT Addresses this Requirement
§ 164.306 Security standards: General rules.		
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.	✓	<p>CT (Change Tracker) : providing 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</p> <p>VT (Vulnerability Tracker) : identifying vulnerabilities prior to any attack enhances the overall cyber security posture making it more difficult for an attacker to use known exploits. An attacker would need to spent more time and effort to infiltrate, making the organization as less viable target.</p>
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.		<p>CT: comparing any change of settings, files, or configuration with a list of known ‘good’ or approved changes protects the security and the integrity of ePHI addressing attacks unknown so far</p> <p>VT: Checking the infrastructure for vulnerabilities tackles reasonably anticipated attacks, as they are quite often attempting to exploit known vulnerabilities.</p>
(3) Ensure compliance with this subpart by its workforce.	✓	<p>CT: as the solution can monitor change on any asset by any user, it enables the enforcement and thus maintain compliance</p> <p>VT: n.a.</p>
§ 164.308 Administrative safeguards.		
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.	✓	<p>CT: Implementing Change Control is a proven policy and tested procedure to prevent, detect, contain, and correct violations. Example: CIS controls can be used to baseline the systems.</p> <p>VT: 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.</p>

<p>(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.</p>		<p>CT: using CIS controls to identify risks related to unsecure devices and services in the infrastructure</p> <p>VT: scanning for vulnerabilities</p>
<p>(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).</p>		<p>CT: providing 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</p> <p>VT: identifying vulnerabilities prior to any attack enhances the overall cyber security posture making it more difficult for an attacker to use known exploits. An attacker would need to spent more time and effort to infiltrate, making the organization as less viable target.</p>
<p>(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.</p>		<p>CT: Change Control enables the detection of activities of users which violate the security policies, a basic step needed to apply sanctions</p> <p>VT: n.a.</p>
<p>(1)(ii)(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.</p>		<p>CT: CTs logs can be reviewed and filtered in the solution as well as forwarded to a log analyzing solution</p> <p>VT: VTs logs can be reviewed and filtered in the solution as well as forwarded to a log analyzing solution</p>
<p>(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.</p>		<p>Ensure that the workforce is correctly organised and assigned the least privileged permissions for their role.</p> <p>CT: Deploy proper hardening to the end point to ensure only authorised users have access to resources and auditing is configured to track success and fail attempts. Deploy NNT Log Tracker to collect audit information in a central repository.</p>
<p>(3)(ii)(C) (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.</p>		<p>CT: Deploy local user tracker to gather lists of current users and groups on individual systems and run reports agent groups which look for the presence of a specific user.</p> <p>Utilise the process output tracker 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.</p>

§ 164.308 Administrative safeguards.

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	✓	<p>CT: Implementing Change Control is a proven policy and tested procedure to prevent, detect, contain, and correct violations. Example: CIS controls can be used to baseline the systems.</p> <p>VT: 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.</p>
(5)(ii)(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	✓	<p>CT: Change Control enables the detection of malicious software</p> <p>VT: n.a.</p>
(5)(ii)(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	✓	<p>CT: Use Change Tracker CIS reports to configure the correct level of auditing on systems.</p> <p>LT: Use the auditing data produced by the Change Tracker hardening to collate logon information.</p>
(5)(ii)(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	✓	<p>CT: Change Control is able to monitor the password quality and settings for password management</p> <p>VT: Checks for default passwords</p>
(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.	✓	<p>CT: using CIS controls to identify risks related to unsecure devices and services in the infrastructure</p> <p>VT: scanning for vulnerabilities</p>
(6)(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.	✓	<p>CT: is able to identify known security issues like insecure configurations, reports them and supports mitigation efforts</p> <p>VT: is able to identify known vulnerabilities, reports about and supports mitigation efforts</p>
(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.	✓	<p>CT: Deploy hardening to the infrastructure assets to ensure systems are fit for purpose and then monitor for change actively.</p>

§ 164.308 Administrative safeguards.

(8) Standard: Evaluation. Perform a periodic technical and nontechnical 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.



CT: periodic or continuous technical evaluation is a basic feature

VT: periodic or continuous technical evaluation is a basic feature

§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:



CT: Allows for the monitoring of baselines, the continuous status update whether a device is connected and configured according specs and the environmental specs. Can verify whether logs of access control devices used in Building Management Systems have been altered

§ 164.312 Technical safeguards.

(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).



CT: Use Change Tracker CIS reports to configure the correct level of auditing on systems.

LT: 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.



CT: Use Change Tracker CIS reports to configure the correct level of auditing on systems.

LT: 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.



CT: supports the requirement by verifying whether a certain asset is encrypted as needed

VT: n.a.

(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.



CT: provides the required functionality, records activity at a very detailed level.






VT: n.a.

(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.




CT: detects changes to files, settings, and alerts about unwanted change

VT: n.a.

<p>(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.</p>		<p>CT: detects changes to files, settings, and alerts about unwanted change</p> <p>VT: n.a.</p>
<p>(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.</p>		<p>Ensure that the workforce is correctly organised and assigned the least privileged permissions for their role.</p> <p>CT: Deploy proper hardening to the end point to ensure only authorised users have access to resources and auditing is configured to track success and fail attempts. Deploy NNT Log Tracker to collect audit information in a central repository.</p>
<p>(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.</p>		<p>Ensure that the workforce is correctly organised and assigned the least privileged permissions for their role.</p> <p>CT: Deploy proper hardening to the end point to ensure only authorised users have access to resources and auditing is configured to track success and fail attempts. Deploy NNT Log Tracker to collect audit information in a central repository.</p>
<p>(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.</p>		<p>CT: detects changes to files, settings, and alerts about unwanted change</p> <p>VT: n.a.</p>
<p>(2)(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.</p>		<p>CT: detects changes to files, settings, and alerts about unwanted change; can be used to control that settings for encryption are not changed</p> <p>VT: n.a.</p>

§ 164.404 Notification to individuals.

<p>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).</p>		<p>CT: is able to identify known security issues like insecure configurations, reports them and supports mitigation efforts</p> <p>VT: is able to identify known vulnerabilities, reports about and supports mitigation efforts</p>
--	---	---



Contact us



☎ US - (844) 898-8362, UK - 01582 287310

✉ info@nntws.com

🌐 www.newnettechnologies.com

[Schedule a free consultation](#)

[Request a Demo](#)