HIPAA-HITECH Security Rule

Non-Stop Compliance/Continuous Breach Detection is Prescribed

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

©New Net Technologies

www.nntws.com

SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

Abstract

Our medical, health and personal information should remain private.

While the principle of Doctor-Patient confidentiality has always been regarded as sacrosanct, the electronic age has inevitably led to greater ease of access to all information, including confidential patient details a.k.a. electronic protected health information.

This whitepaper discusses the legislated protective measures of the HIPAA Privacy and Security Rules and how best to implement and automate compliance.

Know your rights and learn what HIPAA means for you.

Do you need to take HIPAA seriously?

- New York and Presbyterian Hospital (NYP) has agreed to pay OCR $3,300,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules

- Parkview Health System, Inc.will pay $800,000 and adopt a corrective action plan to address deficiencies in its HIPAA compliance program

- Columbia University (CU) has agreed to settle potential violations of HIPAA Privacy and Security Rules, including a $1,500,000 monetary settlement

source: Department of Health and Human Services

Do you need to take HIPAA seriously?

HIPAA and the subsequent HITECH acts were introduced to provide some legislated rules and muscle to ensure that personal medical details remain private.

Naturally, the primary concern is with policing access to patient data within hospital facilities, making sure that health care system-users are provided with ‘least privilege’ rights, and that systems are managed in such a way that security vulnerabilities are mitigated and would-be hackers are kept out.

However, one of the main issues is that inevitably, Health care providers need to share patient details with Insurers and Health care Plan providers, including Government bodies such as Medicare and Medicaid.

And then there are also any number of other parties who will have access to health care records – nursing homes, pharmacies, lawyers, accountants, IT Services Providers and so on.

Each time access is provided to health care records, the potential for a loss of confidentiality increases.

The HIPAA Privacy Rule clarifies the rights of the individual with respect to controlling access, integrity and privacy of their heath information.

The 2013 HIPAA Omnibus rules made it clear that sub-contractors and associated business partners were *equally* accountable to HIPAA standards of governance.

In other words, the burden of HIPAA compliance now applies to everyone.

Figure 1: HIPAA and HITECH

The era of electronic protected health information (commonly referred to as ePHI) has brought numerous benefits to everyone in terms of improved accuracy and clarity of patient records and the streamlining of the ‘healthcare supply chain’ of insurers, medical facilities and clinicians.

But this has also introduced a much greater need for governance and stewardship of this precious data.

If your organization proves ultimately to be responsible for a breach of patient privacy, expect to feel the full weight of a HIPAA lawsuit.

> “
> ## HIPAA Security Rule
>
> The ***HIPAA Security Rule*** establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity.
>
> The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
>
> ”

HIPAA Requirements Summary – Privacy Rule, Security Rule

Alongside the procedural requirements – appointment of a Privacy Officer responsible for the development of written Privacy Policies and Procedures and for ensuring all personnel are thoroughly trained – there must also be a complaints procedure implemented together with provision for mitigation of losses in the event of a breach, and a proper record governance and destruction program.

Lots of paperwork, guides, manuals, training workshops, forms and questionnaires.

But where the HIPAA rules becomes more challenging to interpret and implement is where technical data safeguards are required.

Recognition that electronic patient records are as easy to copy and transfer as any other data files, coupled with the acknowledgment that hacking and malware are so prevalent has led to the HIPAA Security Rule.

Controls for HIPAA Security and Security Best Practices

In many respects securing ePHI is no different to securing other forms of confidential data such as payment card details, product blueprints and financial reporting information. As a result InfoSec teams in the health care industry are encouraged to adopt security controls designed to protect the confidentiality, integrity and availability of electronic protected health information (ePHI) which are similar to the security best practices used for other GRC security standards, for example, SOX or PCI.

Perimeter firewalling, identity and authentication management, data encryption, establishment of a hardened build standard with FIM to verify its integrity, plus auditing of user activity are all standard security best practices that should be employed in any organization, but are especially important for protecting ePHI data.

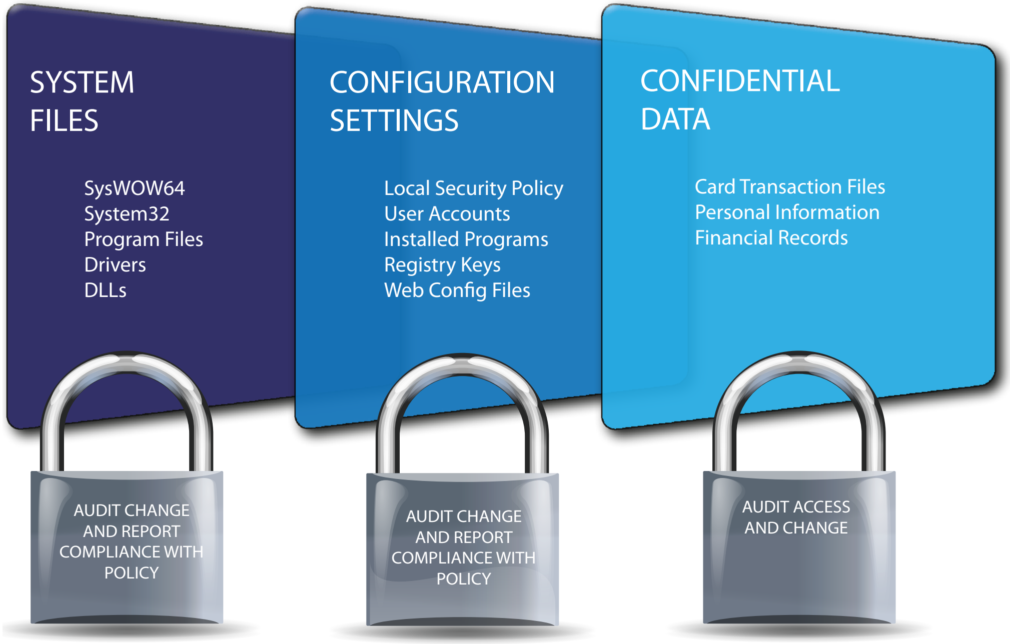

Figure 2: The Anatomy of FIM - File Integrity Monitoring has three key dimensions - protecting system and program files, protecting configuration settings and protecting confidential data. These three dimensions require different technologies and approaches to cater for the varying demands of access and change detection

The general guidance offered is to consult NIST SP 800 and work towards compliance with the 800-53 controls.

Integrity of software and platforms using FIM is mandated to ensure that the threat of malware and hacker activities can be mitigated where possible.

In addition, file integrity monitoring ensures that, if a systems breach is successful, it will at least be detected and reported.

This damage-limitation contingency may end up being the difference between either a stressful few hours spent dealing with a breach, or millions of dollars paid out in settlements and months of stress dealing with investigators and auditors.

File Integrity Monitoring Agent versus Vulnerability Scanning Appliance - A contained breach is far better (and much less expensive to clean-up after) than a major breach

> *If you only scan periodically, you could be left exposed for days or weeks*

Whereas most organizations will use vulnerability scanner technology such as Qualys, Rapid 7 or Outpost 24, the better option is to use an agent-based solution that can operate continuously. Why is an agent better? Any snapshot scan is only as good as the time it as run, and with breaches able to cause massive damage within only a short space of time, speed of detection and remediation is critical.

Agent-based file integrity monitoring also has an advantage in being able to maintain a complete system image - all files and registry settings, including security and audit policies, all software/packages installed, services or daemons enabled, running processes and user accounts - can be tracked for changes.

A breach will typically develop in a series of steps, incrementally invading the network, laying the groundwork on one device, downloading more malware files as the hacker progresses deeper into the IT estate and searches out more sensitive data. As such, a breach may only make very subtle changes, so monitoring the complete spectrum of system attributes is vital; early detection and remediation is critical.

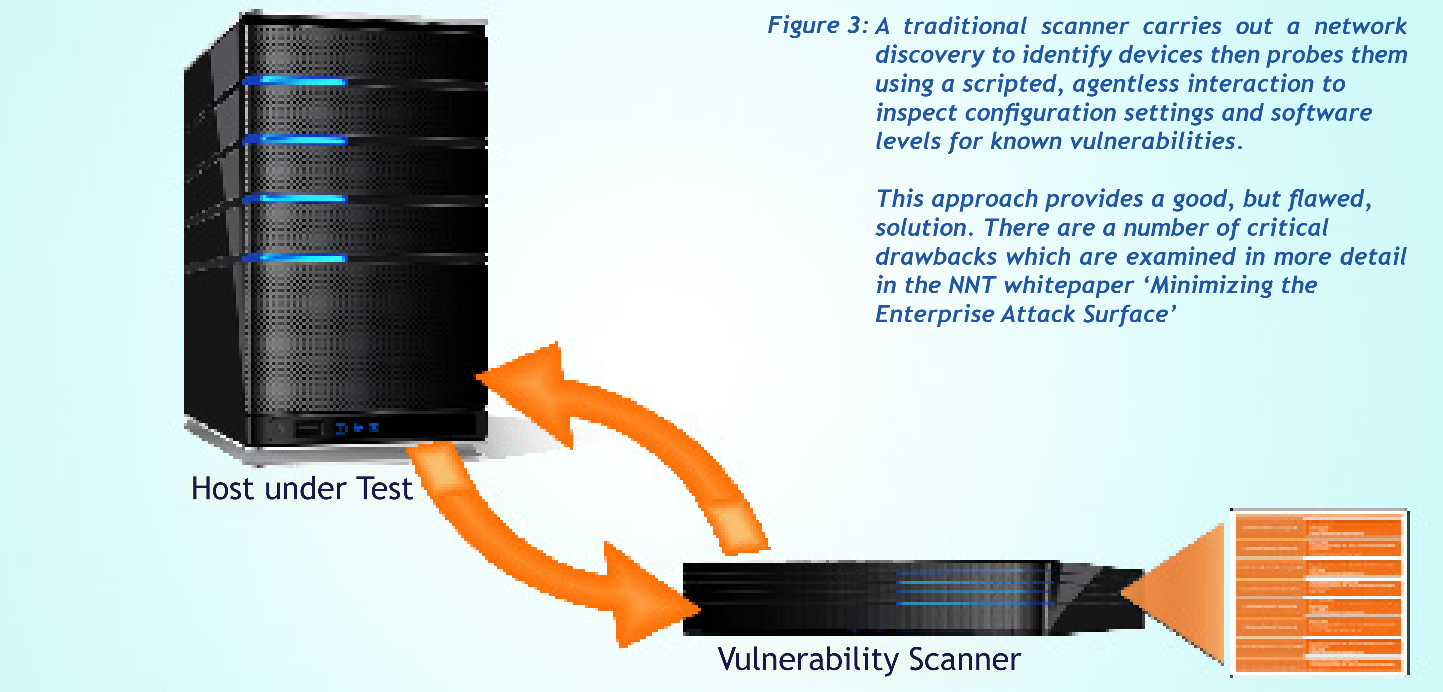

Figure 3: A traditional scanner carries out a network discovery to identify devices then probes them using a scripted, agentless interaction to inspect configuration settings and software levels for known vulnerabilities.

This approach provides a good, but flawed, solution. There are a number of critical drawbacks which are examined in more detail in the NNT whitepaper 'Minimizing the Enterprise Attack Surface'

A typical vulnerability scanner will only report how susceptible a system is to known exploits, but won't baseline the entire file-system to sniff out Trojan malware infiltration or other breach 'fingerprints'.

Considering that in the case of zero day malware, Anti-Virus is also be blind to this kind of breach, this is why FIM is a key line of defense in HIPAA compliance.

If you only scan periodically, you could be left exposed for days or weeks.

And, in the event that a breach is successful, a real-time alert that allows damage to be shut down fast could be the difference between a near-miss and an expensive data-loss catastrophe.

About NNT

NNT Change Tracker Gen provides continuous protection against known and emerging cyber security threats in an easy to use solution, offering true enterprise coverage through agent-based and agentless monitoring options.

- NNT analyzes every configurable component within your IT Estate and allows you to define a 'Known, Good, Secure and Compliant State' for all of your in scope systems.

- NNT-Change Tracker scans your devices and compares them to a standard policy, either user defined or based on an industry standard such as the Center for Internet Security (CIS).

- Policies can be automatically assigned based on the device type or priority via a centrally managed console.

- Gen7 is able to fully automate change approval for you, using the NNT FAST (File Approved-Safe technology) that combines unique intelligent change control knowledge base and whitelists.

- With NNT's real-time capabilities, unlike traditional scanning or exclusively agentless technologies, potential breaches to systems or policies are spotted immediately.

NNT Change Tracker Gen 7 helps you to prevent security breaches of your systems by providing you with a powerful feature-rich, easy to use and affordable solution for validating, achieving and maintaining compliance with corporate governance or security standards.

www.nntws.com

©New Net Technologies

UK Office - Spectrum House,
Dunstable Road, Redbourn,
AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place,
Suite 10115, Naples, Florida
34108
Tel: +1-888-898-0674

Conclusion - The NNT View

The HIPAA Omnibus revisions make it clear that HIPAA and HITECH isn't just aimed at Health care companies. Any associated organization working with patient information is subject to the HIPAA Privacy and Security rules and will be liable for compensation in the event of any breach of confidentiality.

HIPAA and HITECH Security Rule-compliance is as complex as any other compliance initiative. However, since the controls required to protect ePHI data are much like the procedures and technology needed to provide security to cardholder data and financial data, this provides an opportunity to assimilate security best practices from other compliance programs.

This means that, say, an insurance company is likely to be subject to HIPAA, and PCI DSS and SOX but will be able to leverage similar controls and technology to underpin security best practices.

Finally, with the level of fines and loss of public confidence in any organization deemed responsible for a breach, it is more critical than ever to ensure that compliance with the HIPAA Security Rule can be proven. Measures such as system hardening and file integrity monitoring must be properly operated in order to head-off the full range of modern threats. While 100% protection can never be guaranteed, meeting your compliance obligations is the minimum 'safe harbor'.

Given that the risk of a breach is always present, the best solution is to use real-time, continuous FIM agent technology to monitor for vulnerabilities and any intrusion of the host.

This approach not only provides non-stop system protection but ensures that, if a breach is successful, any data loss can be minimized through swift intervention.

It might just save your organization.

NNT Change Tracker Enterprise - Real-Time, continuous FIM...and Certified by the Center for Internet Security

- Change Tracker Enterprise has been certified by the CIS which means you can trust NNT to accurately deliver the most comprehensive, consensus-derived hardening checklists

- NNT provide CIS Benchmark checklist coverage for all Windows, Unix and Linux Operating Systems, SQL Server and Oracle Database Systems, and for Network Devices and appliances such as Cisco ASA firewalls

- Compliance is continuously enforced meaning vulnerabilities are highlighted more quickly than with traditional vulnerability scanners

- Better still, NNT Change Tracker Enterprise provides continuous real-time FIM across all system, application, driver and configuration files providing peace of mind that system integrity is being maintained

- And if the worst case scenario does happen and your systems are breached or infected with malware, this will be detected within seconds, minimizing damage and costs

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com