opentext™ | Cybersecurity

Position Paper

Security and HIPAA Compliance: Meeting the Challenge of Securing Protected Health Information

As the need to ensure the security of sensitive health information grows, so must security and compliance teams look to more integrated approaches to both reduce risk and enable streamlined and efficient user workflows.

This position paper looks at the most important elements of securing sensitive health information and meeting HIPAA compliance requirements in a scalable and cost-effective way. The paper also provides an overview of the HITECH Act, which addresses the privacy and security concerns associated with the electronic transmission of health information, in part through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Table of Contents

Changing Threats to Patient Information

Protecting sensitive data, especially "individually identifiable health information" such as that covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1], is one of the most significant challenges facing security and compliance professionals in the healthcare industry.

The risks to data have grown along with:

- Parallel increases in the technical expertise of external attackers
- Unmanaged access to patient information by trusted healthcare staff
- Ever greater complexity of the IT landscape due to virtualization, cloud computing, mobility, bring-your-own-device (BYOD) and other disruptive technologies

While IT security teams scramble to respond, they do so in an environment where the pressure to make clinical and hospital workflows more efficient continues to dominate strategic planning—even as the penalties and fallout for breaches grows more severe. Healthcare professionals will seek technology solutions and processes that enable them to work faster, improve patient outcomes, and enhance overall quality of care while still enabling the organization to meet its financial objectives. The end result is that IT security teams are forced to balance the demand for workflow efficiency and productivity with the need to secure patient data.

Often, the balance is upset and a breach, with concomitant breach penalties, results. Case in point, in May 2013, Idaho State University (ISU) agreed to pay $400,000 to the U.S. Department of Health and Human Services (HHS) to settle alleged HIPAA violations. The settlement involved the breach of unsecured electronic protected health information (e-PHI) of approximately 17,500 patients. The e-PHI of these patients was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU[2].

While IT security teams scramble to respond, they do so in an environment where the pressure to make clinical and hospital workflows more efficient continues to dominate strategic planning—even as the penalties and fallout for breaches grows more severe.

1. U.S. Department of Health and Human Services, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules," **www.hhs.gov/ocr/privacy/** (accessed 6/1/13).
2. U.S. Department of Health and Human Services, "Idaho State University Settles HIPAA Security Case for $400,000," **www.hhs.gov/ocr/privacy/hippa/enforcement/examples/isu-agreement-press-release.html** (accessed 6/12/13).

Meeting the Challenge of HIPAA

While the information security demands of HIPAA are broad and cover everything from policy to physical access controls, many healthcare providers are finding that the most difficult demands are very much in line with other compliance mandates. These demands focus on controlling who has access to patient information within hospital and clinical IT infrastructures, and monitoring the activities of those users (for example, nurses, doctors, clinicians, billing specialists or administrative support personnel), especially those with broad privileges. IT must then securely manage these privileges to reduce organizational risk.

These areas provide the greatest, most direct data protection benefits if organizations address them correctly. If left unprotected, critical data such as patient health information can put hospitals, physicians, insurance providers, IT professionals and others at risk of fines and reputational damage. In the worst cases, it puts the patients themselves at risk of misdiagnosis or even death.

If left unprotected, critical data such as patient health information can put hospitals, physicians, insurance providers, IT professionals and others at risk of fines and reputational damage. In the worst cases, it puts the patients themselves at risk of misdiagnosis or even death.

HITECH Act: Extending the Privacy and Security Provisions of HIPAA

Congress enacted Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[3] as part of the American Recovery and Reinvestment Act of 2009. The act addresses the privacy and security concerns associated with the electronic transmission of health information. Several significant changes were brought about as a result of the act, all acting synergistically to enforce compliance to HIPAA requirements. Among the most relevant changes, the HITECH Act:

- Extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities.
- Introduces the first federally mandated data breach notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured protected health information (PHI) occurs.
- Significantly increases the penalty amounts the HHS Secretary may impose for violations of the HIPAA rules and encourages prompt corrective action. The act also requires that covered entities include these changes in any business associate agreements.
- Implements new rules for the accounting of disclosures of a patient's health information. For example, it extends the current accounting for disclosure requirements to treatment information and payment and health care operations when an organization is using an electronic health record (EHR).

3. U.S. Department of Health and Human Services, "HITECH Act Enforcement Interim Final Rule," **www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html** (accessed 6/1/13).

HIPAA Meets HITECH

Combined, HITECH and HIPAA provide even stronger incentives for any organization to secure electronic health records. The financial penalties grew from no more than $25,000 in fines to a maximum of $1.5 million in fines for the most egregious violations[4].

With the passing of HITECH, there are now different categories of offenses. The revised penalties per violation during a single calendar year are:

- Entity did not know about violation: $100-$50,000/maximum $1,500,000
- Entity had Reasonable Cause: $1000-$50,000/maximum $1,500,000
- Entity demonstrated Willful Neglect, but corrected the security issue in a timely manner: $10,000–$50,000/maximum $1,500,000
- Entity showed Willful Neglect and failed to correct the security issue: $50,000/maximum $1,500,000

More people and organizations than you may think fall under both HIPAA and HITECH rules.

Are HIPAA and HITECH in Your Future?

More people and organizations than you may think fall under both HIPAA and HITECH rules. There are the obvious practitioners: the healthcare providers. That includes medical facilities, physicians, alternative health practitioners, dentists, chiropractors, nursing homes and pharmacies. That group also includes health plans such as health insurance companies, health maintenance organizations (HMOs), company health plans, and government programs that pay for healthcare. Less known but certainly covered are clearinghouses that process any health information they receive or send in a standard electronic format.

Key Areas of Risk

According to a 2012 Healthcare Information and Management Systems Society (HIMSS) security survey[5], almost two-thirds of respondents (64 percent) reported that their organization conducted an audit of their IT security plan at least annually. Yet despite this due diligence, nearly a quarter of the respondents reported their organization had sustained a security breach in the past year. The majority of the respondents (32 percent) reporting breaches were hospitals rather than physician practices. This is attributable to the fact that hospitals have more patients to manage and typically have large groups of rotating staff or students with access to data (often off-premises) from unmanaged computing devices, all of which contributes to higher risk to the security and privacy of patient information.

4. U.S. Department of Health and Human Services , Office of the Secretary, “Federal Register, Vol. 74, No. 209, Friday, October 30, 2009, Rules and Regulations,” **www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf** (accessed 6/1/13).
5. U.S. Department of Health and Human Services, “Idaho State University Settles HIPAA Security Case for $400,000,” **www.hhs.gov/ocr/privacy/hippa/enforcement/examples/isu-agreement-press-release.html** (accessed 6/12/13).

Specifically, three key areas of risk to the security and privacy of e-PHI are:

- Controlling access to patient information in a robust and well-managed way
- Monitoring the activity of healthcare staff, especially those with broad privileges
- Managing who has access to patient information and the systems where it resides

By using an integrated and secure approach to these three areas, IT security teams can most directly reduce the risk of breach and the impact of an audit.

Controlling Access

Access control is fundamental to the ability of any hospital, insurance provider, healthcare clearinghouse or other organization to secure e-PHI. Organizations must implement access control in such a way as to enable hospital and clinic staff to access the information they need, when they need it, in a way that doesn't slow them down but actually helps them to work faster and with greater convenience. At the same time, organizations must restrict healthcare practitioners from overly broad access or access that extends beyond the time necessary for them to perform their functions. However, access controls that slow down or burden hospital or clinic staff will face deployment challenges and encourage healthcare practitioners to seek social workarounds.

Organizations must implement access control in such a way as to enable hospital and clinic staff to access the information they need, when they need it, in a way that doesn't slow them down but actually helps them to work faster and with greater convenience.

The problem that many organizations face is that identifying who has access to systems containing sensitive patient information is often difficult. Additionally, over time, users often acquire access rights that far exceed those they need for their current role. Further, for clinicians and hospital personnel, if sharing of credentials in violation of policy helps them to improve patient outcomes, they will always view security as secondary to their need for better clinical care.

Likewise, reliable deprovisioning of access for all healthcare workers as they leave the organization is an essential component of a secure e-PHI implementation. Studies indicate that changes in staff often leave organizations open to attack from former healthcare workers or contractors who retain access, in some cases for months or years after they have changed roles or have left the organization.

To fulfill HIPAA requirements, healthcare organizations and their auditing teams need the ability to quickly and accurately report on and review who has access to systems and what level of access they have.

Without clearly defined processes and communication channels to manage and report on user access, organizations will find that more healthcare and IT personnel have access to sensitive patient information than is necessary. To fulfill HIPAA requirements, healthcare organizations and their auditing teams need the ability to quickly and accurately report on and review who has access to systems and what level of access they have. As a result, hospitals, clinics, insurance providers, doctors and other healthcare practitioners will be able to ensure that they:

- Enforce the minimum level of access
- Remove inappropriate access to systems and resources
- Delete inactive or stale accounts
- Enforce secure deprovisioning

Monitoring Healthcare Personnel with Broad Privileges (Privileged Users)

While managing access is important, protecting information, especially the highly sensitive patient information covered under HIPAA, relies on having visibility into the activity of personnel within the IT infrastructures of covered entities, particularly those personnel with broad privileges.

Per the HIPAA statute, covered entities include[6]:

- **Healthcare providers.** Doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies
- **Health plans.** Health insurance companies, HMOs, company health plans, government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs
- **Healthcare clearinghouses.** This includes entities that process nonstandard health information they receive from another entity into a standard (standard electronic format or data content), or vice versa.

Real-time monitoring of healthcare personnel with broad privileges has presented significant challenges in the past, especially around system performance and event detection. As a result, many organizations have adopted less complete solutions that rely on simply tracking changes to files on a periodic basis.

By implementing restrictions on how they grant privileges, and by delegating only those privileges essential to perform tasks, healthcare organizations can significantly reduce the scope of risk to sensitive patient information, and the probability of a malicious or accidental breach.

The problem with this approach is that it misses the most vital information:

- **Who** made the change?
- **What** was changed within the file?
- **When** was the change made?
- Was this change an authorized change?
- From **where** was the change made?

To protect patient information from unauthorized access and change, healthcare organizations must have the ability to monitor privileged-user activity for files, systems and essential infrastructure components such as Active Directory.

Managing Privileges

Monitoring healthcare personnel with broad privileges is one aspect of reducing the risk to protected health information. Every bit as important, though, is the ability to reduce the number of healthcare personnel who have these privileges. By implementing restrictions on how they grant privileges, and by delegating only those privileges essential to perform tasks, healthcare organizations can significantly reduce the scope of risk to sensitive patient information and the probability of a malicious or accidental breach. Secure privilege delegation is the best approach to limiting who has access to patient information and the systems that house this information because it defines and grants only those privileges essential to any task.

6. U.S. Department of Health and Human Services, "For Covered Entities and Business Associates," **www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/** (accessed 6/18/13).

An even more secure approach is to grant those privileges only for the specific time required to perform the task. While this just-in-time delegation has been difficult to achieve in the past, the combination of secure privilege management tools and process automation technology provides the benefits of both reduced risk and reduced workload for user and privilege management.

Solutions for Meeting the Challenge of HIPAA

OpenText™ provides a number of well-integrated solutions that help reduce risks to sensitive healthcare information and streamline and simplify the work of meeting and reporting on compliance to HIPAA.

OpenText provides a number of well-integrated solutions that help reduce risks to sensitive healthcare information and streamline and simplify the work of meeting and reporting on compliance to HIPAA.

These solutions include:

NetIQ Secure Configuration Manager by OpenText—provides configuration assessment against best practices and out-of-the-box compliance checks for standards such as HIPAA. It also enables user-entitlement reporting to ensure that only those users who require access to systems have it.

Sentinel by OpenText—presents a single, central location for security event management, log aggregation and forensic analysis. The ability of ArcSight to detect activity on critical hosts provides a singularly powerful approach to securing protected information and detecting unauthorized activity, as well as producing analysis and reports to document and support compliance.

NetIQ Directory and Resource Administrator by OpenText—enables secure delegation of privileges to reduce the risk from privileged-user activity, one of the most significant sources of risk to protected information.

NetIQ Change Guardian by OpenText—enables real-time detection of access, changes and privileged-user activity across multiple servers, operating systems, devices and applications, including Microsoft Windows, Active Directory, UNIX and Linux. When integrated with security information and event management (SIEM) solutions such as Sentinel, the solution enables powerful detection of events, a reduction in reporting of non-significant events, and real-time response to risky activity.

NetIQ Privileged Account Manager by OpenText—limits unauthorized transactions and access to health care data by delivering privileged-user management and tracking across all Windows, UNIX and Linux environments. It works by allowing administrators to centrally define the commands that privileged users are able to execute on platforms, ensuring that only authorized users can perform specific administration tasks.

NetIQ Access Manager by OpenText—provides authorized users with intelligent access to secured applications and information based on who they are, what devices they are using

and where they are located. It provides a single sign-on experience to internal and cloud-hosted applications, making access secure and convenient by allowing only authorized users, while eliminating the need for users to save passwords in an unprotected format.

NetIQ SecureLogin by OpenText—offers a single sign-on (SSO) solution that allows healthcare personnel to access local and network resources using a single set of credentials. Upon login, the solution automatically authenticates users to all of their applications and resources to create an optimal user experience that is both easy and fast.

OpenText security, identity and access management solutions can help you more easily secure sensitive patient information, protect against damaging breaches and comply with HIPAA regulations.

Mapping to HIPAA

OpenText security, identity and access management solutions can help you more easily secure sensitive patient information, protect against damaging breaches and comply with HIPAA regulations.

Here are some of the ways that a partnership with OpenText can reduce risk and streamline compliance:

Section 164.308(a)(1)(i)
Implement policies and procedures to prevent, detect, contain and correct security violations.

NetIQ Secure Configuration Manager—enables the detection of misconfigured systems, one of the most common causes of security policy violation.

Section 164.308(a)(1)(ii)(D)
Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

Sentinel—enables the collection, aggregation, analysis and long-term secure storage of activity logs for both systems and end users.

Section 164.308(a)(3)(ii)(B)
Implement procedures to determine that the access of an employee to e-PHI is appropriate.

NetIQ Access Manager—provides access to authorized users from wherever they are located and provides access only to the resources users need to do their jobs.

Section 164.308(a)(3)(ii)(C)
Implement procedures for terminating access to e-PHI when an employee leaves your organization.

NetIQ Directory and Resource Administration—helps to create, modify and delete user accounts efficiently by automating tedious Active Directory management processes.

Section 164.308(a)(4)(i)
Implement policies and procedures for authorizing access to e-PHI that are consistent with the applicable requirements of subpart E of this part.

NetIQ Directory and Resource Administrator and NetIQ Change Guardian—together provide the ability to securely delegate privileges to access information, in order to enforce policies and detect unauthorized changes to those policies before protected information is exposed.

Section 164.308(a)(5)(ii)(C)
Implement procedures for monitoring login attempts and reporting discrepancies.

Sentinel—provides real-time detection and reporting of login activity for normal users and privileged administrators.

Section 164.308(a)(5)(ii)(D)
Implement procedures for creating, changing and safeguarding passwords.

NetIQ SecureLogin—allows your organization to strengthen its password policies. With only one password to remember, you can require your users to have more secure—or even randomly generated—passwords rather than passwords that are simply easy to remember.

With only one password to remember, you can require your users to have more secure—or even randomly generated—passwords rather than passwords that are simply easy to remember.

Section 164.308(a)(6)(ii)
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; and document security incidents and their outcomes.

Sentinel and NetIQ Change Guardian—together enable faster detection and response to security events and potential threats. SIEM solutions can be limited by their dependence on native logs. NetIQ Change Guardian extends the capabilities of Sentinel by providing the who, what, when and where of unauthorized access and change in real time to security teams.

SIEM solutions can be limited by their dependence on native logs. NetIQ Change Guardian extends the capabilities of ArcSight Sentinel by providing the who, what, when and where of unauthorized access and change in real time to security teams.

Section 164.312(b)
Implement audit controls, hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.

NetIQ Change Guardian—monitors privileged-user activity in real time on protected systems.

Section 164.312 (c)(2)
Implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner.

NetIQ Change Guardian—enables real-time change monitoring for critical systems and information.

Conclusion

Reducing the impact of compliance mandates is a significant challenge that security teams must meet if they are to effectively focus their efforts on critical tasks such as securing sensitive patient information. At the same time, good security will assist them in meeting those compliance mandates. As mentioned in the HIPAA Security Rule itself:

> *"It should be noted that the implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as lack of adequate security can increase the risk of violations of standards."*

By focusing efforts in the key areas of controlling access, monitoring healthcare personnel with broad privileges (privileged users) and managing privilege delegation, organizations can reduce the net risk to themselves and sensitive health information, which in turn eases compliance with standards such as HIPAA and the HITECH Act.

OpenText provides a range of solutions to help security teams manage these risks, to provide greater visibility to risk, and to enable more streamlined compliance with standards like HIPAA. Using OpenText's expertise in building and maintaining secure solutions provides the most direct, cost-effective path to greater security and simplified compliance.

Customers and partners choose OpenText to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly distributed business applications.

About OpenText

OpenText provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of OpenText™ Cybersecurity, an OpenText line of business.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.