HAYES
MANAGEMENT CONSULTING
Optimizing the business of healthcare

WHITE PAPER

Mitigating Organizational Risk:

7 Step IT Security Assessment Plan

Table of Contents

Overview

Since 2009, almost 42 million people have had their electronic protected healthcare information (ePHI) compromised by HIPAA privacy and security breaches.[1] The number of health records breached has jumped by 138 percent since 2012.[2] Last year, 4.5 million patients of Community Health Systems in Tennessee had their information stolen by cybercriminals - the largest ePHI breach of 2014.[3] In 2015, Anthem's database of 80 million people across 14 states was hacked and 11 million people have had their identity exposed when Premera was breached.[4] In a survey conducted by the Healthcare Information Management Systems Society (HIMSS), 68 percent of respondents reported a recent attack on their facility.[5]

As electronic record keeping in the healthcare industry becomes more prevalent, the risks and breaches are rising as well. The evidence continues to mount. Not only do these security leaks affect patient confidentiality, they're also hitting healthcare organizations in the wallet. New York Presbyterian Hospital and Columbia University were fined with a $4.8 million settlement as a result of the disclosure of the ePHI of 6,800 patients.[6]

With reduced revenue and shrinking margins already buffeting the healthcare industry, organizations can ill afford to absorb the financial impact of an ineffective IT security system. Moreover, it is an increasing concern to the Boards of Directors of such facilities regarding their fiduciary responsibilities and the effects breaches have on their patients that could result in a potential competitive disadvantage.

In an effort to ensure the security of patient data, the Department of Health and Human Services (HHS) adopted what is commonly known as the Security Rule to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). All healthcare organizations must comply with the rule that specifically focuses on protecting the confidentiality, integrity, and availability of ePHI. Part of that compliance requires organizations to conduct an annual assessment to analyze the effectiveness of their IT security systems. Not only is this assessment mandatory, but with the threat of heavy financial penalties for security breaches looming, it's also smart business.

It's important to stress that while the risk assessment is a crucial component of your IT security framework, it's not a panacea. No environment today or in the foreseeable future will be totally secured. What is important, however, is that healthcare organizations acknowledge and understand IT security in the new world of electronic/social communication.

A comprehensive, effective risk assessment program requires detailed planning and disciplined implementation based on strategy, governance and organizational education. It is not just ticking off boxes in a generic questionnaire. Each organization must document all IT plans, processes, and policies to support potential audits. Assembling this level of detail offers concrete proof that the organization has implemented a comprehensive working program rather than simply responding with "vaporware acknowledgement."

Following is a seven-step process that can be incorporated into an overall risk management framework to evaluate an IT security system along with actions that can be taken to minimize the potential for expensive and embarrassing breaches.

The Security Rule Basics

The HIPAA security rule guides healthcare organizations and their providers in their efforts to guard against and react to potential security issues. The rule focuses on protecting the confidentiality, integrity, and availability of ePHI. HIPAA mandates any ePHI that a covered entity creates, receives, maintains, or transmits must be protected against threats, hazards, and impermissible uses or disclosure.

> *"A key requirement of the security rule is that an organization establish measures to reduce risk to a reasonable and appropriate level. The actions must protect ePHI against those risks that can be "reasonably anticipated."*

An organization is responsible and required to document all processes as it relates to IT security, including IT security strategy, policy, education, assessment processes and silent documentation, as well as subsequent remediation processes and plans.

The Risk Management Framework

An effective Risk Management Framework (RMF) methodology that provides healthcare organizations with a disciplined, structured, extensible, and repeatable process for minimizing risks to ePHI begins at the top. Organization leaders must drive the security process to ensure that all levels of the organization "buy in."

Unfortunately, a recent survey of the National Association of Corporate directors revealed that a third of healthcare board members have "little

knowledge" about cybersecurity risks.[7] Leadership needs to develop a more comprehensive understanding of the problem and lead the change management process to addresses the threats more effectively. Developing a detailed RMF – which includes a comprehensive risk assessment program - is a crucial step on the road to minimizing risks.

The RMF can be applied to both new and legacy environments and information and should consider effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, and regulations.

Implementation of the RMF will support compliance with the security rule by:

- Ensuring appropriate selection of methods and controls which adequately and appropriately protect ePHI
- Establishing compliance strategies that match the size and structure of the organization
- Providing guidelines on best practices for developing and implementing a risk management program
- Creating appropriate documentation that demonstrates effective compliance

The RMF or risk assessment program is not a simple survey of all relevant departments regarding ePHI. It must be a process that is implemented in the organization at all levels.

The program entails a significant, concerted, and integrated approach that requires:

- Development of an IT security strategy integrated with the IT strategy and organization business strategy
- Development of an IT security governance process and ownership
- Development and/or review of IT security policies, procedures and standards
- Education and training at all levels within the organization including organizational board members
- Leveraging current ongoing organizational processes such as business impact analyses and disaster recovery plans that are aligned to support the IT security assessment/impact approach

A Seven Step Assessment Plan

Performing a comprehensive risk assessment is often viewed as one of the most important components of the security rule and a key component of a RMF. The assessment helps identify the risks of someone compromising the confidentiality, inappropriately editing or deleting, or limiting the availability of ePHI.

Regardless of the methodology used to conduct risk assessments, there are certain key elements that must be included. The following plan incorporates seven mandatory components of a risk assessment process.

1. Establish Scope

The first step in the process establishes the scope of the assessment. The risk analysis must include all the ePHI that an organization creates, receives, maintains or transmits. Data stored on hard drives, laptops, backup tapes, smart cards, and other portable electronic media whether resident on premise or in the cloud must be subject to the assessment.

Depending on the organizational environment-size and/or complexity, two levels of assessment may be required. First an environmental impact analysis of the relationship between all units/affiliates within the organization and the "parent" needs to be documented. Second, the organization must conduct an inventory of each department/unit to determine where the "ePHI lives" within the unit and develop detailed documentation for the applications used by the department /unit. The important take away is that -DOCUMENTATION - is critical to support findings for any subsequent third party audit.

2. Gather Information

To fully determine the scope of the assessment, organizations must gather information as to how their ePHI is stored, received, maintained or transmitted, and more importantly how it is being protected today. Note that ePHI is more than just medical records and includes such information as appointments, billing, and insurance claims. An organization must also include data stored on copiers, mobile devices, EHR, and CD's.

The flow of ePHI must also be determined. Information is constantly moving to other physicians, the patient, other providers, a backup facility, or offsite location. Evaluating data transfer is

also important whether by email, fax, shared network drives, direct exchange, or over a health information network or exchange. Also, all business associate agreements regarding the security of data between the organization and the associate need to be reviewed and documented.

The information-gathering step is essential to ensure that vulnerabilities and threats are correctly identified. For example, incorrectly assuming a control is in place or not identifying portable media being used to house ePHI can cause the assessment to miss potential vulnerabilities.

During this stage, it's important that everyone in the organization understands the terms being used. There should be a documented vocabulary that is circulated and commonly understood. This becomes critical when follow-up audits are conducted by outside third parties.

During the assessment, the team asking the questions should understand the process well enough that they can follow up with a "deep dive" investigation on issues that may uncover intrusion threats and vulnerabilities. The team should probe to reveal application "owners" and determine if those apps are sufficiently integrated into the IT infrastructure. At this point, the information gathering should be a forensic assessment and analysis of the organization regarding IT security.

Once data collection is complete, all findings must be fully documented.

3. Identify Threats and Vulnerabilities

Following data collection, the assessment then moves on to identify potential threats and vulnerabilities.

Threats can be human -- hackers or disgruntled employees -- or natural and environmental like floods, fires, or power outages. Vulnerabilities are weaknesses in the security controls of an organization that could cause an incident. These could include things like unencrypted computers or a weak password policy, a pattern of failing to follow approved security processes, or the lack of security procedures. Any of these could result in unauthorized personnel accessing ePHI.

Part of the identification step includes assessing current security controls to determine if the implemented or planned controls will minimize or eliminate risks to ePHI. This involves reviewing the existing administrative, technical, and physical safeguards installed to protect the security of the system.

This phase should also include intrusion detection to identify potential threats by breaking through firewalls. This means testing to determine if someone can hack into your system from the outside. This testing can be done easily using third party software.

Once identified, potential threats and vulnerabilities should be noted in the final summary risk assessment report.

4. Determine Likelihood of Threats Exploiting a Vulnerability

The next major step in measuring the level of risk is to determine the likelihood of a threat successfully exploiting a vulnerability. These plausible threats must then become the focus of additional controls and procedures since according to the security rule these are the threats that can be "reasonably anticipated" to occur. It is the responsibility of the organization to establish safeguards to minimize or eliminate these particular threats.

While massive, targeted breaches capture all the headlines and attention, most organizations need to be aware of less wide spread attacks. According to a report from Symantec, non-targeted attacks still make up the majority of malware attacks, having grown by 26% in 2014. The report says more than 317 million new pieces of malware were created in 2014 -- translating to nearly one million new threats each day.[8]

5. Estimate Risk Levels

The organization must also assess the impact of these potential threats to ePHI in terms of confidentiality, unauthorized access, and ability to alter data or ensure ongoing availability of information. All potential impacts must be documented and categorized as high, medium, or low in relation to how likely they are to occur.

Developing a risk-level matrix by classifying both threat likelihood and potential impact on a scale of high-medium-low will help determine the overall risk level of the organization. Using this type of matrix helps prioritize the actions to take to address identified risks.

Rating risk levels is subjective and will vary from one organization to another. That is acceptable as long as these definitions are documented and the organization is able to explain the ratings and how each potential threat was categorized.

6. Document Assessment Results

Once the risk assessment has been completed – threat sources and vulnerabilities identified, risks assessed and classified – the results must be documented. This will include a list of suggested security controls and recommended corrective actions to be implemented to mitigate risks.

Although the documentation process does not need to be overly complex, it must be clear, comprehensive, and detailed. Outside auditors will want to know how the assessment was developed, as well as who performed it. As with most programs, the documentation needs to provide a defined audit trail back to the source of every finding so it can pass any outside audit test.

7. Implement Ongoing Reviews

The process of securing ePHI doesn't end with the completion of the initial risk assessment. Organizations evolve over time and implemented corrective actions can sometimes fall by the wayside. That's why leadership must continue to conduct reviews on a regular basis. At minimum, a risk analysis should be conducted at least once annually. Depending on the size and complexity of the organization, doing a review multiple times in a year may be most appropriate.

Remediating Assessment Findings

Follow up actions as a result of the assessment are crucial to mitigating risks on an ongoing basis. Leaders should take into account the size, operations, and available resources of the organization when developing a corrective action plan to minimize security risks.

Process

All processes affecting ePHI security should be reviewed in the assessment phase. When it comes to process issues and their impact on IT security, there are only three alternatives – the current process is faulty, people are failing to follow the process, or there is no process at all in place. In the first case, the process must be changed to eliminate the discovered risk. In the second, training may need to be increased, and in the third, a process must be developed for everyone to follow.

Process can be related to systems –- password and nightly shut down procedures for example -- or they can relate to physical safeguards within the organization –- locked doors and file cabinets for instance.

As processes are changed or developed it's important to get input from the people involved in performing the tasks on a regular basis. Helping to create effective processes gives staff a sense of ownership, increasing the chances they'll be followed.

A systematic approach to change management helps people throughout an organization adjust to new behaviors and skills. By formally setting expectations, employing tools to improve communication, and proactively seeking ways to reduce misinformation, stakeholders are more likely to accept and embrace the change.

People

Implementation of new policies and procedures require in-depth communication and training. It begins with strong executive leadership communicating the vision and selling the business case for change. Staff can then better understand the reasons for change and help them "buy in" to each process. This ensures that corrective actions take hold and are effective. Proper training and communication on systems will help avoid individuals taking unauthorized shortcuts that could expose the organization to a security breach.

Organizations should also conduct awareness training to explain the consequences of breaches in security -– both to the organization in the form of financial penalties and to the patients in terms of compromised privacy and confidentiality. Having everyone in the organization on alert to potential breaches will minimize threats and enhance overall security.

For an IT security program to be effective, everyone at every level of the organization needs to be on the same page. It's critical going forward that executives, compliance, and training units be tightly integrated. Ensuring cybersecurity needs to be one of the all-encompassing guidance principles of the organization. When it involves IT security, people's thinking needs to be more broadly based as opposed to narrowly focused on their particular space.

Technology

HHS recommends several focus areas when it comes to technical safeguards to ePHI. They include:

- Access control: Implement unique user identification, emergency access procedure, automatic logoff, and encryption and decryption
- Audit controls: Install hardware, software, and procedural mechanism that record and examine activity in IT systems that contain ePHI
- Integrity: Establish policies and procedures to protect ePHI from improper alteration or destruction
- Person or Entity Authentication: Institute procedures to verify the identity of anyone seeking access to ePHI. This can be accomplished with a smart card, token, key, or something biometric like fingerprints, or voice, facial, or iris patterns.
- Transmission Security: Ensure security during transmission of ePHI using encryption and network communication protocols

The response to each of these five areas should be well documented as to the status and future direction that the organization is and will be taking

Summary

Protecting and securing ePHI has never been more critical. Mayo Clinic CISO Jim Nelms told the Wall Street Journal that healthcare information "is often harder to protect than financial information" because of the complexities related to diverse medical devices and physician information sharing practices.[9]

To meet this challenge, the entire culture of healthcare needs to change. Developing a comprehensive assessment program and tightly integrating it into your overall risk management framework can play a significant role in minimizing your chances of being breached.

A detailed assessment and follow-up remediation processes forms the beginning of a solid foundation to build an effective security control program necessary to protect ePHI. The privacy and confidentiality of your patients as well as the financial health of your organization depend on it.

About Hayes

Hayes Management Consulting is a leading, national healthcare consulting firm and software developer that partners with healthcare organizations to streamline operations, improve revenue and enhance technology to drive success in an evolving landscape. To learn how Hayes can help you, call 617-559-0404 or email requestconsultant@hayesmanagement.com.

Sources

[1, 3] *Biggest HIPAA breaches of 2014*, by Erin McCann, HealthcareIT News, December 26, 2014

[2] *HIPAA data breaches climb 138 percent*, by Erin McCann, HealthcareIT News, February 6, 2014

[4] *Your Guide to Medical Breaches: Anthem, Premera and CareFirst*, by Clark Howard, May 21, 2015, Money in your Pocket.

[5, 7, 9] *Board members at healthcare organizations lack understanding of cybersecurity risks*, by Katie Dvorak, FierceHealthIT, July 6, 2015

[6] HHS.gov Press Release, May 7, 2014

[8] *2015 Internet Security Threat Report*, Symantec

HAYES
MANAGEMENT CONSULTING
Optimizing the business of healthcare

1320 Centre Street
Newton Center, MA 02459-2400
617-559-0404
info@hayemanagement.com
www.hayesmanagement.com