HIPAA:

Five steps to ensuring your risk assessment complies with OCR guidelines

Authors

Janice Ahlstrom, CPHIMS, FHIMSS, CCSFP, RN, BSN
Director – Risk, Internal Audit and Cybersecurity
janice.ahlstrom@bakertilly.com

Kenneth Zoline, CISSP
Manager – Technology Risk and Cybersecurity
kenneth.zoline@bakertilly.com

ahia

bakertilly
now, for tomorrow.

The information on the following pages highlights the essential components of a HIPAA risk analysis as required by the Office of Civil Rights (OCR) and shares a cost effective approach to completing a risk analysis annually.

HIPAA: Five steps to ensuring your risk assessment complies with OCR guidelines

HIPAA and healthcare technology have changed significantly over the past 20 years. *See timeline on page 5*. Covered entities and their business associates face an ever-evolving risk environment in which they must protect electronic protected health information (ePHI). Although healthcare security budgets may increase this year, the cost of implementing and maintaining adequate security controls to protect an entity's ePHI far exceeds what is often budgeted. As a result, some ePHI may be under-protected and vulnerable to data breach. A long-term, consistent and cost-conscious approach to HIPAA compliance is needed.

Current state of healthcare

HIPAA's role and importance continues to rise with the value of the data it was created to protect. Healthcare providers are increasingly targeted by cybersecurity attacks, and patient data now commands more than credit card accounts on the black market and dark web. Distributed denial-of-service (DDoS), ransomware, malware, phishing and rogue software are frequently used in cyberattacks launched against hospitals and other healthcare entities.

The message is clear: if you are responsible for securing patient and proprietary healthcare information, you cannot afford to be unprepared.

According to the Ponemon Institute's **Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data**, nearly 90 percent of surveyed healthcare organizations suffered a data breach in the past two years. The average cost of a data breach for the surveyed healthcare organizations exceeded $2.2 million. The projected cost of all data breaches for the healthcare industry surpassed $6.2 billion.[1]

In 2016 the U.S. Department of Health and Human Services (HHS) reported that over 12 million patient health records were breached.[2] The department's Office for Civil Rights (OCR) levied over $24 million in fines and a prison sentence was ordered for inappropriately obtaining ePHI.[3]

Risk analysis: The foundation of an effective HIPAA compliance plan

Risk analysis is one of four required HIPAA implementation specifications that provide instructions to implement the Security Management Process standard. To further clarify risk analysis, the OCR released guidance on the risk analysis requirement in July 2010. The HIPAA Security Rule states that an organization must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the organization.

Additionally, security risk analysis must be performed in order to comply and attest to Meaningful Use of electronic health records as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

With the OCR increasing enforcement efforts with a second year of random audits for both covered entities and their business associates related to HIPAA compliance, risk analysis plays a critical role. Organizations need to comply with the HIPAA risk analysis requirement if they are to be fiscally responsible and avoid returning Meaningful Use Medicare and Medicaid payments, avoid OCR fines and avert the cost of breach notification efforts.

Risk analysis – Five steps to getting it right

Today, we find a range of compliance issues and tools used to conduct risk analysis when providing services. Often, HIPAA risk assessment reports do not meet the guidance defined by OCR or support complete review of the security rule controls. Checklists of policies and procedures, penetration test results and IT assessments barely scratch the surface of the data security safeguards. The wide variance in HIPAA risk analysis scope and reporting suggests that many organizations may not truly understand the HIPAA Security Rule and how to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the organization as defined by the OCR. The five steps below should put you on the right track to be compliant with OCR guidelines.

1. Evaluate your current HIPAA risk assessment

The following components should be included in your current risk assessment efforts:

- Identification of assets that create, store, process or transmit ePHI and the criticality of the data
- Identification of threats and vulnerabilities to ePHI assets, the likelihood of occurrence and the impact to the organization along with a risk rating
- Evaluation and documentation of the administrative, physical and technical safeguards for the organization, by department where applicable, and for each application with ePHI
- Evaluation and documentation of the security measures currently used to safeguard ePHI. Are the controls configured and used properly? What are the vulnerabilities?
- Evaluation of HIPAA policies and procedures – are the documents dated, signed, reviewed periodically and available?

If all of the above items are not included in the scope of your risk assessment, the assessment may not be acceptable with an OCR audit.

2. Select the right HIPAA risk assessment tool

The OCR highlights two tools in its 2010 guidance that provide a framework for risk assessment:

Security Risk Assessment Tool (SRA) - developed by the Office of the National Coordinator (ONC) for Healthcare Information Technology. The ONC's SRA user guide walks users through 156 questions with resources to help understand the context of each question. It also allows users to factor in the likelihood and impact to ePHI in the organization. The tool functions on mobile devices as well. It can be downloaded from HealthIT.gov. The tool is geared towards smaller practices and while a good starting point, it does not take into consideration many of the complexities of larger organizations.

Risk Assessment Toolkit - developed by a team of Health Information Management Systems Society (HIMSS) professionals. The HIMSS Risk Assessment guide and data collection matrix contains a PDF user guide, Excel workbooks with NIST risk analysis references, application and hardware inventory workbooks, HIPAA Security Rule standards, implementation specifications and a defined safeguards workbook. The safeguards are numbered 1-92 and correspond to the Security Scorecard workbook. The scorecard differentiates numbered safeguard components to be assessed for the organization, by department and within applications that contain ePHI. The HIMSS Risk Assessment toolkit is available at: http://www.himss.org/himss-security-risk-assessment-guidedata-collection-matrix. The tool includes NIST Special Publication 800-30 Revision 1 guidance for completing a risk assessment.

Regardless of the tool chosen to help with the assessment, the most important aspect of the risk analysis is taking an open and honest view of the threats and vulnerabilities to the environment.

Selecting a third-party HIPAA risk assessment partner

If your organization lacks the knowledge, experience or requisite training to perform a HIPAA risk assessment, we recommend engaging security specialists who understand healthcare, healthcare technology and the HIPAA Security Rule. However, it is often hard to find all of these skills in one person. Often, it is a team of two or more individuals who together have this knowledge and the right skills to provide the best service.

When assessing resources,

- Understand how long the vendor has been providing these services
- Understand the types of certifications and qualifications the vendor has
- Be sure the resources have years of experience providing security, risk and compliance services
- Look for qualified professionals with certifications such as: CISA, CPHIMS, CCSFP, CISSP, HCISSP, CIPT, CISM, ISSMP or CCSFP

3. Determine the risk analysis frequency

One of the most prevalent challenges in complying with the HIPAA Security Rule's risk analysis requirement is determining the frequency or triggering conditions for performing a risk analysis.

The HIPAA Security Rule and 2010 OCR risk analysis guidance state that risk analysis should be "ongoing" to document and update security measures as needed. The security rule states that continuous risk analysis should be completed to identify when updates are needed. OCR guidance notes that the frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every three years) depending on circumstances of their environment. Typically, covered entities that are attesting to Meaningful Use and complying with the spirit of the security rule will conduct an annual HIPAA risk assessment.

4. Perform the risk assessment: insource or outsource

HIPAA does not specify who should perform the risk assessment. Some organizations insource, some outsource and some do both – alternating between insourcing and outsourcing. For example, an organization may hire external resources to conduct the HIPAA risk assessment every other year, and on the off year the organization may choose to conduct it internally. Where practical, a separation of duties should exist between the HIPAA risk assessment team and the systems implementers and operations staff. **Hiring an outside professional to conduct the risk analysis reduces risk by providing an impartial assessment from someone who was not involved in the implementation of your systems or the development of your policies, procedures and security controls.** (*See sidebar for selection tips.*)

5. Support cost savings without sacrificing risk assessment quality

How do you contain costs in performing a HIPAA risk analysis? Use an industry standard tool for assessment and stick with it. The industry standard tools also help to define a clear scope of effort. Often organizations can become disconcerted trying to conduct a self-assessment with a previous year's report provided by an outside professional.

A practical approach for risk assessment

Year 1	Conduct the assessment with an external professional(s) Define internal resources in your organization and be sure they are educated on use of the assessment toolkit - make it part of the risk assessment service engagement
Year 2	Conduct an internal self-assessment using the selected toolkit Consult your year one external professional, should you require guidance
Year 3	Benefit from additional cost savings beyond doing the year two assessment internally by engaging the same external professional(s) for the year three assessment for less cost than in year one - as long as the scope of your environment has remained stable The toolkit being used will be familiar to everyone involved and previous assessment information will be documented and ready for efficient review and analysis

Final analysis: What could be missed, overlooked or found?

Healthcare organizations must implement strong data security safeguards. Doing so supports compliance with the HIPAA Security Rule, reduces risk and helps ensure the confidentiality, integrity and availability of the ePHI the organization creates, receives, maintains or transmits. Conducting internal risk analysis along with annual risk assessments that leverage a professional services provider every other year also reduce risk and maximize the value of the resources engaged. Finally, leveraging an industry standard toolkit will help your organization be comfortable with conducting self-assessments on alternating years while saving time and money.

In providing HIPAA analysis and compliance services, we consistently find some areas of noncompliance while other areas can be unique given the size, structure or evolution of an organization. Below is a starter checklist of areas you may want to consider when conducting your HIPAA risk analysis.

- □ Do you have a documented data classification standard defining what ePHI is? Are all ePHI assets identified? Does this list include legacy data stores?
- □ Do you copy un-redacted production patient data to your test or development environments? If so, what access and auditing controls have you put in place to secure and monitor the test and development environments?
- □ Are all servers located in a physically secure data center? Yes, we still find servers under desks in ancillary departments that are often not up-to-date with current patches. Often this occurs in specialty areas where software specific to a department or treatment modality is in use. A server under the desk of an ancillary department is not afforded the physical, technical and environmental protections that your data center can provide.
- □ Does your intranet collaboration site (e.g., SharePoint) contain ePHI? Often during an implementation project documents are stored on a SharePoint site. At go-live screen prints with ePHI are captured with go-live issues documentation. Are screen prints with ePHI stored on your Intranet or in email folders?
- □ How are software vendors accessing your systems? Who from the vendor team has access?
- □ Have you tested backups of your systems, can you truly restore from backups?
- □ What detective controls let you know when student nurses, residents and volunteers with access to your systems are no longer engaged with your facility?
- □ Do information services staff use shared root and administrator accounts? How often is the local Windows administrator account password changed?
- □ Do you have workstations or application software with ePHI that have no session inactivity timeouts set on them? Have you assessed this in all ancillary departments?
- □ Is HIPAA security responsibility written into your employee job descriptions?
- □ Does anyone outside of information services have administrator rights to ePHI application software?

Sources list

[1] http://www.healthcareitnews.com/news/cost-data-breaches-climbs-4-million-healthcare-events-most-expensive-ponemon-finds - cost of data breaches

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[3] http://www4.toledoblade.com/Courts/2016/10/19/Ex-therapist-gets-2-years-probation-Patient-records-accessed-illegally.html - prison sentence information

HIPPA TImeline

1996

How HIPAA evolved

The Healthcare Insurance Portability and Accountability Act (HIPAA) was signed in **August 1996**. Goals of the legislation were to: improve the portability and accountability of health insurance coverage, reduce waste, fraud and abuse in health insurance and healthcare delivery.

The **early to mid-2000 years** saw the development of HIPAA collaboratives and coalitions. This brought together technology, legal, clinical, security and health information management professionals to define HIPAA's impact on their organizations, develop tools, policies and procedures to achieve HIPAA compliance. Many organizations took HIPAA to heart and worked earnestly to be compliant, while others did not.

Once HIPAA was passed, the Department of Health and Human Services (HHS) worked to define the HIPAA Privacy and Security Rules. **The privacy rule became effective in April, 2003 and the security rule in April 2005**. These rules defined what Protected Health Information (PHI) was, and the administrative, physical and technical security safeguards to protect electronic health information (ePHI).

HHS.gov reports that from **late 2003 through 2008**, there were 11,629 complaints, however HHS did not impose any fines for violations. The approach taken to privacy complaints was to investigate and recommend improvements. The number of privacy complaints trended upward **from 2003 to 2013. In 2014, we saw the first sharp reduction (56%)** in complaints from the previous year, likely the result of enforcement efforts.

HIPAA enforcement

In March 2006, the HIPAA Enforcement Rule was passed to address the failure of covered entities to fully comply with the HIPAA Privacy and Security Rules. This rule provided a means by which HHS could investigate and fine covered entities who neglected to implement the legislated safeguards. Further, the Enforcement Rule provided HHS's OCR with the ability to convey criminal charges against recurrent offenders who do not implement corrective measures within 30 days. Individuals also have the right to pursue civil legal action against a covered entity if their personal healthcare information has been disclosed without their permission and it caused them to incur serious harm.

HITECH and the Omnibus Rule of 2013

Procedures to simplify the administration of health insurance became a catalyst to encourage the healthcare industry to computerize patient medical records. HIPAA planted the seeds for the development of the **Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009**, which in turn set in motion the Meaningful Use incentive program. HITECH had the goal of motivating healthcare organizations to implement and use Electronic Health Records (EHRs) in a meaningful way via stages of measures and Medicare and Medicaid incentive reimbursements.

Within the HITECH legislation, HIPAA requirements were extended to business associates and third-party suppliers in the healthcare industry, and the Breach Notification Rule was presented. Breach Notification stipulated that breaches of ePHI affecting more than 500 individuals must be reported to HHS – Office of Civil Rights. The criteria for reporting breaches of ePHI were defined in the **Final Omnibus Rule of March 2013**.

The Omnibus Rule clarified the definition of a workforce within covered entities, amended the length of time patient records could be held, covered administrative policies and procedures for the use of mobile devices, defined further penalties for noncompliance and reciprocal monitoring between covered entities and their business associates.

TODAY

bakertilly

now, for tomorrow.

Baker Tilly and AHIA

Baker Tilly author contact information:

Janice Ahlstrom, Director – Baker Tilly Virchow Krause, LLP
janice.ahlstrom@bakertilly.com • +1 (612) 876 4761

Kenneth Zoline, Manager – Baker Tilly Virchow Krause, LLP
kenneth.zoline@bakertilly.com • +1 (312) 729 8346

About Baker Tilly - bakertilly.com

Baker Tilly Virchow Krause, LLP (Baker Tilly) is a leading advisory, tax and assurance firm whose specialized professionals guide clients through an ever-changing business world, helping them win now and anticipate tomorrow. Headquartered in Chicago, Baker Tilly, and its affiliated entities, have operations in North America, South America, Europe, Asia and Australia. Baker Tilly is an independent member of Baker Tilly International, a worldwide network of independent accounting and business advisory firms in 147 territories, with 33,600 professionals. The combined worldwide revenue of independent member firms is $3.4 billion. Visit bakertilly.com or join the conversation on LinkedIn, Facebook and Twitter.

AHIA Whitepaper Subcommittee:

Alan Henton, White Paper Chair alan.p.henton@vumc.org
Mark Eddy mark.eddy@hcahealthcare.com
Linda McKee lsmckee@sentara.com
Debi Weatherford debi.weatherford@piedmont.org
Deborah Pazourek, AHIA Board Liaison Deborah.L.Pazourek@medstar.net

About Association of Healthcare Internal Auditors (AHIA) - ahia.org

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org.

AHIA whitepapers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare

Connect with us:

🌐 bakertilly.com/heathcare

in Baker Tilly Virchow Krause, LLP

🐦 @bakertillyUS

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Baker Tilly Virchow Krause, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2018 Baker Tilly Virchow Krause, LLP.