Clearwater

Whitepaper

Driving Compliance Efficiency Through Enterprise Cyber Risk Management

By Bob Chaput, CISSP, HCISPP, CRISC, CIPP/US C/EH Founder & Executive Chairman

Table of Contents

Introduction 3

HIPAA: Where compliance and cyber risk management meet 4

The role of risk analysis 5

Compliant risk analysis methodology 5

Additional laws and regulations that require risk analysis 6

How ECRM can facilitate compliance efficiency 8

Getting started with ECRM to simplify compliance 9

Takeaways 10

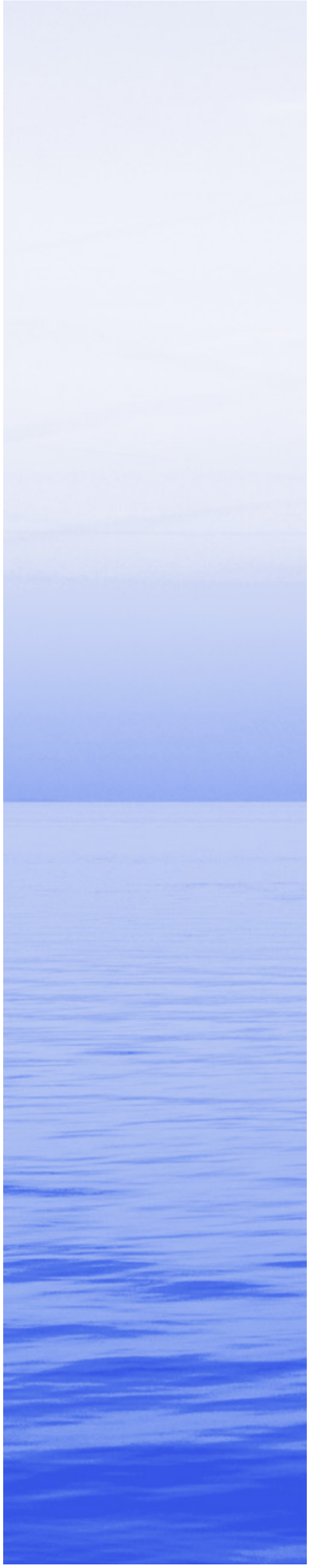
Introduction

The business case for cyber risk management is clear. A cyber incident can lead to consequences that threaten the care and safety of patients. Cyber incidents can also result in financial, reputational, compliance, and legal consequences that threaten the viability of an organization. Healthcare organizations have begun to understand that cyber risk management is a critical part of overall enterprise risk management. That is why many healthcare organizations are establishing enterprise cyber risk management (ECRM) programs.

ECRM is not defined by a specific product or service. Instead, ECRM describes an approach to cyber risk management that engages the entire organization instead of leaving this task solely in the hands of the information technology (IT) department. It addresses cyber risk management from the enterprise perspective and involves taking comprehensive steps to manage cyber risk and, in so doing, protecting data privacy and security across the entire organization.

A less obvious, but equally important, benefit of ECRM is that it can help healthcare organizations manage compliance efficiently. Healthcare is one of the most regulated industries in the US, making compliance a challenging task. A study by the American Hospital Association found that hospitals must comply with 341 distinct regulatory requirements, 23% of which are directly related to privacy and security.[1]When you add in health systems and post-acute care providers, the number of regulatory requirements increases to 629. Privacyand security-related regulatory requirements make up 13% of this broader scope of regulations.

It is likely that the American Hospital Association study, which was published in 2017, underrepresents the number of regulations related to data privacy and security in effect today. Additional regulations, such as the General Data Protection Regulation (GDPR), which became effective in May 2018, and the



[1] American Hospital Association, Regulatory Overload: Assessing the Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers, October 2017, https://bit.ly/3kBLPi0.

implementation of California Consumer Privacy Act in January 2020, have been adopted since the American Hospital Association study was completed. Research and advisory firm Gartner notes that since the GDPR went into effect, "More than 60 jurisdictions around the world have enacted or proposed postmodern privacy and data protection laws."[2]

Managing the numerous—and growing—number of mandates related to privacy and security can be overwhelming for healthcare organizations. One way to simplify cybersecurity management compliance is to address commonalities across regulations. This is where a comprehensive ECRM program can help.

HIPAA: Where compliance and cyber risk management meet

The most well-known law that addresses cyber risk management within the healthcare industry is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA required the secretary of the Department of Health & Human Services (HHS) "to publicize standards for the electronic exchange, privacy and security of health information."[3] The final omnibus version of HIPAA, which was published in the Federal Register in 2013, includes detailed requirements that specify how any organization that "creates, receives, maintains, or transmits" protected health information must protect the "confidentiality, integrity, and availability" of that information.[4]

Key components of HIPAA include the HIPAA Privacy Rule (45 C.F.R. § 160 and Subparts A and E of 45 C.F.R. § 164); the HIPAA Security Rule (45 C.F.R. § 160 and Subparts A and C of 45 C.F.R. § 164); and the HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400–414). Between them, these three rules include more than 80 standards (what organizations must do) and more than 100 implementation specifications (how organizations must comply). These standards and specifications lay the groundwork for what HHS expects of organizations with respect to protecting patient data, including electronic patient data. These rules specify how HHS—and the Office for Civil Rights (OCR), which enforces HIPAA—expect healthcare organizations to address cyber risk.

[2] Susan Moore, "Gartner Predicts the Future of Privacy 2020," Smarter With Gartner, January 20, 2020, https://gtnr.it/3pBc4ZL.

[3] "Summary of the HIPAA Privacy Rule," Office for Civil Rights, U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://bit.ly/2Hdx2fH.

[4] 45 C.F.R. § 164.306(a)(1) .

The role of risk analysis

One of the required actions spelled out in the HIPAA Security Rule is that every organization subject to HIPAA regulations must conduct a risk analysis. The final rule states this requirement as follows: *"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" organization.[5]

Guidance published by the OCR states that the purpose of risk analysis is to "provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI [electronic protected health information]."[6] In addition, OCR guidance notes that "the Security Rule does not prescribe a specific risk analysis methodology….Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance."

Risk analysis is not just an essential task for HIPAA compliance; it is a foundational step for any ECRM program and most privacy- and security-related regulations. Every organization has a unique set of information assets to protect. Information assets include not only data, but also systems and devices. These assets are associated with unique vulnerabilities and unique threats. An organization cannot implement an effective ECRM program without conducting a risk analysis (i.e., identifying and documenting the organization's unique information assets and addressing the unique vulnerabilities and threats associated with those assets).

Compliant risk analysis methodology

With respect to methodology, OCR points to guidance established by the National Institute of Standards and Technology (NIST). NIST, a federal agency, has developed and published extensive resources on cyber risk management.[7] NIST's resources are in the public domain and therefore freely available. OCR guidance notes, "Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, nonfederal organizations may find their content valuable when developing and performing compliance activities."[8]

[5] 45 C.F.R. § 164.308(a)(1)(ii)(A) .

[6] U.S. Department of Health & Human Services, Office for Civil Rights, "Guidance on Risk Analysis Requirements under the HIPAA Security Rule," July 14, 2010, https://bit.ly/36HnsKQ.

[7] "Risk Management," Information Technology/Cybersecurity, National Institute of Standards and Technology, last accessed November 18, 2020, https://bit.ly/3kHrlik.

[8] U.S. Department of Health & Human Services, Office for Civil Rights, "Guidance on Risk Analysis Requirements under the HIPAA Security Rule."

OCR guidance specifically mentions NIST Special Publication 800-30, Guide for Conducting Risk Assessments.[9] (Note that NIST uses the term "risk assessment" synonymously with "risk analysis.") The guide provides comprehensive direction, including information about the purpose of conducting a risk assessment, definitions of terms and concepts important to understanding risk assessment, and detailed guidance regarding the risk assessment process.

OCR expectations regarding compliance with HIPAA rules, including the requirement to conduct a risk analysis, can also be determined by examining OCR enforcement action documents (e.g., resolution agreements, corrective action plans, notices of final determination). Resources and documents related to OCR's enforcement actions can be accessed through the HIPAA enforcement section of the HHS website.[10] It is interesting to note that our company's analysis of 60 OCR enforcement actions involving ePHI found that 88% of the cited organizations had not completed a comprehensive, enterprise-wide risk analysis acceptable to OCR. In addition, 80% of the organizations had adverse findings related to steps taken to address the risks documented in the risk analysis. Unfortunately, many organizations are caught off guard, believing they have conducted an adequate risk analysis or that they have an adequate ECRM program in place, only to find out that OCR does not agree.

Additional laws and regulations that require risk analysis

HIPAA is not the only law that addresses data privacy and security within the healthcare industry. There are many other laws and regulations that apply to specific types of data and/or specific kinds of data transactions that are applicable to the healthcare industry. Many of these laws and regulations include language, requirements, and standards related to risk assessment. Some of them are listed below.

GDPR. The GDPR, a data privacy law designed to protect individuals in the European Union, went into effect in 2018.[11] US healthcare organizations that offer goods or services to individuals in the European Union may be subject to the provisions of the GDPR.[12] GDPR requires organizations to conduct a data protection impact

[9] U.S. Department of Commerce, National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1, September 2012, https://bit.ly/38W2lY2.

[10] "HIPAA Enforcement," Office for Civil Rights, U.S. Department of Health & Human Services, last reviewed July 25, 2017, https://bit.ly/3f9rGPh.

[11] Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119.

[12] Amy Joseph and Krietta Bowens Jones, "GDPR compliance: Considerations for U.S. healthcare organizations," Compliance Today, October 2018, https://bit.ly/38P62i6.

assessment. This provision requires “an assessment of the risks” and “the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation.”[13]

Gramm–Leach–Bliley Act (GLB Act).[14] The GLB Act requires organizations that offer consumers financial products or services (e.g., loans) to “explain their information-sharing practices…and to safeguard sensitive data.”[15] The GLB Act specifically addresses the safeguarding of “‘nonpublic personal information,’” which includes “any ‘personally identifiable financial information’ that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise ‘publicly available.’”[16]

The Federal Trade Commission issued a Safeguards Rule (16 C.F.R. § 314) as part of its implementation of the GLB Act.[17] Among the requirements of the rule are that each company must “identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks.”

Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS articulates global standards that apply to any organization that stores, processes, or transmits credit card information. Guidance from the PCI Security Standards Council identifies assessment as the first step in adhering to PCI DSS standards.[18] PCI Security Standards Council guidance describes assessment as “identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.” Additional guidance from the PCI Security Standards Council defines risk analysis/risk assessment as the “process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.”[19]

Family Educational Rights and Privacy Act (FERPA). The FERPA statute and accompanying regulations give parents access, and some control, over the

[13] Council Regulation 2016/679, General Data Protection Regulation § 3, art. 35(7)(c),(d).

[14] Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[15] “Gramm-Leach-Bliley Act,” Federal Trade Commission, last accessed November 18, 2020, https://bit.ly/2Kk4IcS.

[16] “How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act,” Federal Trade Commission, July 2002, https://bit.ly/2HbAtn4.

[17] “Financial Institutions and Customer Information: Complying with the Safeguards Rule,” Federal Trade Commission, April 2006, https://bit.ly/35J43Kd.

[18] PCI Security Standards Council, PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1, July 2018, https://bit.ly/3kHDucw.

[19] PCI Security Standards Council, “Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms, Version 3.2.” April 2016, https://bit.ly/3pHnQli.

disclosure of personally identifiable information found in education records.[20] When a student enters postsecondary education or turns 18 years old, FERPA rights transfer to the student.

The FERPA statute and regulations do not directly address the need to conduct a risk analysis. However, the National Center for Education Statistics, within the Department of Education, published specific guidance on managing personally identifiable information in electronic student education records, in which it effectively outlined all the steps for conducting a risk analysis.[21] Conducting a risk analysis is important to complying with FERPA requirements.[22]

Genetic Information Nondiscrimination Act (GINA) of 2008. GINA protects individuals from discrimination based on their genetic information. The specific areas of discrimination GINA addresses are employment and health coverage.[23] When the HIPAA Omnibus Final Rule was published in 2013, the Privacy Rule was modified to encompass the protections specified in GINA.[24] Genetic information, as part of a patient's health record, is protected by both HIPAA and the more specific protections spelled out in GINA.

How ECRM can facilitate compliance efficiency

As these examples illustrate, laws and standards that address the privacy and security of data are embedded in many different regulations that affect healthcare organizations. The examples cited above focus specifically on language related to risk analysis/risk assessment. But the fact is, conducting a risk analysis is but one aspect of a comprehensive ECRM program. An effective ECRM program includes, but is not limited to, the following activities:

- Evaluating whether or not the organization has adopted a cybersecurity framework, such as the NIST
- Cybersecurity Framework, and evaluating the maturity of the organization's implementation of the framework;

[20] 20 U.S.C. § 1232g .

[21] National Center for Education Statistics, Institute of Education Sciences, "Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records," SLDS Technical Brief, November 2010, https://bit.ly/3kK0oQH.

[22] U.S. Department of Health & Human Services and U.S. Department of Education, Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records, updated December 2019, https://bit.ly/2UGJuaR.

[23] "Genetic Information," Office for Civil Rights, U.S. Department of Health & Human Services, last reviewed June 16, 2017, https://bit.ly/2IEgbDH.

[24] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,565 (January 25, 2013) .

- Conducting an enterprise-wide risk analysis that identifies all of an organization's information assets (data, systems, and devices), documents the threats and vulnerabilities associated with each of those assets, and documents the organization's approach to addressing each of those risks;
- Assessing the organization's compliance with the requirements of the HIPAA Security Rule;
- Assessing the organization's compliance with the requirements of the HIPAA Privacy and Breach Notification rules;
- Establishing ongoing processes for identifying and treating risks as the organization evolves and the risk landscape continues to change; and
- Assuring ongoing maturity of the ECRM program through continuous process improvement.

An effective ECRM program will execute these tasks in a way that complies with HIPAA requirements and meets OCR expectations. A comprehensive ECRM program, which meets these goals, can provide the foundation for meeting the data privacy and security requirements of many different mandates and regulations. In other words, a comprehensive ECRM program not only serves to protect the organization from cyber risk, but it also helps simplify compliance with myriad regulations related to data privacy and security.

Getting started with ECRM to simplify compliance

ECRM is a journey, not a destination. It takes time to establish and implement a comprehensive ECRM program. However, once such a program is in place, it can help make compliance activities more efficient and more effective. By implementing a single, comprehensive ECRM program, organizations can not only have confidence that they will meet HIPAA's requirements, but also have confidence that they have a program in place that will meet the data and privacy requirements of many other statutes and regulations.

The following three action steps can help compliance professionals move toward leveraging the power of ECRM to manage privacy and security mandates efficiently and effectively:

1. Identify the information security and privacy regulations that affect your organization. HIPAA's Privacy, Security, and Breach Notification rules are likely at the top of the list. But what about the other regulations mentioned in this article?

Do any of them apply to your organization? Are there other regulations (e.g., state-specific regulations) that control the way your organization manages cyber risk?

2. Analyze the specific requirements of the data security and privacy regulations that affect your organization. For example, how many of the regulations require a risk analysis or risk assessment, as described in this article? What other common requirements related to cyber risk management can you find across the breadth of data privacy and security regulations your organization is subject to?
3. Find out whether your organization has implemented an ECRM program. Share the information you have gathered about how cyber risk management affects your organization with respect to compliance. Make sure compliance has a seat at the table as the organization establishes, or matures, its ECRM program.

Takeaways

- Cyber risk is a business risk issue and a compliance issue for healthcare organizations.
- An enterprise cyber risk management (ECRM) approach to cyber risk can protect patients and the organization.
- The most effective way to achieve compliance with the Health Insurance Portability and Accountability Act's Privacy, Security, and Breach Notification rules is by establishing and maturing a comprehensive ECRM program.
- Many statutes and regulations (e.g., General Data Protection Regulation, the Gramm–Leach–Bliley Act, Payment Card Industry Data Security Standard, Family Educational Rights and Privacy Act, Genetic Information Nondiscrimination Act) include cyber risk analysis/risk assessment requirements that align with the ECRM approach.
- A mature ECRM program can help organizations efficiently and effectively manage multiple, diverse mandates related to data privacy and security.

Bob Chaput (bob.chaput@clearwatercompliance.com) is Founder and Executive Chairman of Clearwater Compliance in Nashville, TN. He is also the author of the book, Stop The Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM).

linkedin.com/in/bobchaput

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

■ ClearwaterSecurity.com/Contact