COSMOS
Navigate the Compliance Universe

Compliance Today - January 2021
Driving compliance efficiency through enterprise cyber risk management

By Bob Chaput, CISSP, HCISPP, CRISC, CIPP/US, C|EH

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

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. Privacy- and 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 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.