AMERICAN HEALTH LAW ASSOCIATION

The Legal Liabilities of Enterprise Cyber Risk Management

February 01, 2021

Bob Chaput, Clearwater | **Iliana Peters**, Polsinelli PC

The health care industry continues to be a prime target for cyber incidents. By any measure—number of attacks, frequency of attacks, scope and size of data breaches—cyber risks in health care have continued to escalate. As health care cyber risks have increased, the courts' perspective on organizational liability for cyber incidents has also evolved.

Two specific trends have emerged that merit the attention of health care leaders. The first trend is the emergence of a de facto "standard of care" related to cyber risk management. The second trend is the increasing possibility that the courts will hold executives and directors responsible for Enterprise

Cyber Risk Management (ECRM) failures.

It is important for health care executives and directors to pay attention to these developments as they consider the adequacy of their organization's ECRM program. A robust, proactive ECRM program—which ensures an organization is managing cyber risk appropriately—can help protect patients from injury or harm posed by cyber incidents. A comprehensive ECRM program will also help protect the organization from cyber incidents. Finally, if a cyber incident should occur, having a strong ECRM program in place can help mitigate the negative reputational, financial, and legal consequences that inevitably follow. In the case of legal consequences, an established ECRM program can help shield the organization and its executives and directors from claims of negligence or willful neglect.

Trend #1: Emerging Standards of Care for Cybersecurity and Enterprise Cyber Risk Management

Violation of the "standard of care" is a key characteristic of medical malpractice lawsuits. Most health care organizations understand "standard of care" in a clinical context. For example, if a patient presents with symptoms of a heart attack, the standard of care would likely involve a review of the patient's history and current symptoms, further testing as indicated, and timely treatment. If the treating physician deviates in any significant way from the standard of care, and the patient suffers harm as a result, the court may determine that the physician was negligent.

As health care organizations have become increasingly dependent on digital information, systems, and devices, a new consideration has emerged with respect to standard of care. That consideration is whether or not the health care provider or organization is adhering to a standard of care related to cyber risk management, in addition to clinical standards of care.

Today, most health care organizations rely heavily, if not exclusively, on digital information, systems, and devices. Every aspect of patient care—from appointment scheduling, to receiving lab test results, to diagnosis and treatment—requires access to accurate, electronic patient information. Any cyber incident that poses a threat to the confidentiality, integrity, and/or availability of electronic patient data has the potential to cause injury or harm.

Cyber-based Medical Malpractice?

Although we have not yet seen a medical malpractice lawsuit based on a violation of cyber risk management standards of care, it is likely inevitable that there will be such lawsuits in the future. Researchers in Israel have demonstrated how hackers could infiltrate a hospital network and modify a computerized tomography (CT) scan.[1] The researchers showed that experienced radiologists were unable to detect the modified images and that the radiologists subsequently made incorrect diagnoses

based on the changed images.[2] Given this scenario, and the fact that misdiagnoses and delayed diagnoses are among the top causes for medical malpractice lawsuits, the first medical malpractice lawsuit based on violation of cyber risk management standards of care may emerge sooner rather than later.

Understanding Standard of Care

How, then, can a health care organization protect itself against such a claim? The first step is to understand what "standard of care" means. Historically, the definition of standard of care was based on custom, with the understanding that "that which is typically done is what is considered standard."[3] Later on, however, the definition changed to emphasize what is *reasonable* over what is *customary*. This change, in part, was based on a 1903 court decision in which Justice Oliver Wendell Holmes, Jr., stated, "What usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."[4] In other words, what is *usually* done may provide some support for an assertion of having met the standard of care, but it is not necessarily sufficient, in and of itself.

This higher bar—doing what is *reasonable*, instead of relying on what is *usual*—is one reason that clinical practice guidelines (CPG) have become important in establishing the standard of care in medical malpractice lawsuits. Expertly vetted, evidence-based CPGs—such as those found in the repository maintained by the ECRI Guidelines Trust[5]—provide credible benchmarks against which the clinical standard of care can be measured.

References for Cyber Risk Management Standard of Care

The parallel to CPGs in the cyber risk management domain for most health care organizations and the vendors with whom they work is found in three different sources: (1) the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, (2) Office for Civil Rights (OCR) guidance and enforcement actions related to HIPAA, and (3) the National Institute of Standards and Technology (NIST) guidance related to cybersecurity. The cyber risk management guidelines contained in these documents provide a benchmark by which organizations may be judged when determining "reasonable" behavior with respect to cybersecurity.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). The first source of standards of care related to cyber risk management is found in HIPAA, which was enacted in 1996.[6] Sections 261 through 264 of the law required the Secretary of the Department of Health and Human Services (HHS) "to publicize standards for the electronic exchange, privacy and security of health information."[7] Key components of HIPAA include:

- The HIPAA Privacy Rule (45 C.F.R. Part 160 and Subparts A and E (500 series) of Part 164) was published as a revised Final Rule in 2002.[8] It established national standards for the use and disclosure of individuals' health information (i.e., protected health information or PHI). The Privacy Rule includes more than 50 standards (*what* organizations must do) and more than 50 supporting implementation specifications (*how* organizations must comply). Compliance has been mandatory since 2003.
- The HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C (300 series) of Part 164) was published as a final regulation in 2003.[9] It established "national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information."[10] The Security Rule includes more than 20 standards and more than 50 implementation specifications.
- The HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400-414) "requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information."[11]

A final, omnibus version of HIPAA was published in the *Federal Register* on January 25, 2013.[12] The extensive details of the HIPAA regulations are beyond the scope of this article, but the point is, HIPAA defines national standards that address the privacy and security of protected health information. These standards are grounded in the original HIPAA legislation that was enacted more than 20 years ago. While not every health care organization is covered by HIPAA, or currently compliant with the cyber risk management standards of care outlined in HIPAA legislation, it is certainly reasonable to expect health care organizations to be compliant with a law that has been on the books for more than 20 years.

Office for Civil Rights (OCR). The second source of standards of care with respect to cyber risk management is contained in guidance and enforcement actions published by OCR. OCR's role in the enforcement of the HIPAA Privacy and Security Rules was expanded and enhanced in the Health Information Technology for Economic and Clinical Health (HITECH Act), which was part of the American Recovery and Reinvestment Act of 2009.[13] As of November 30, 2020, OCR had received more than 250,367 HIPAA complaints, 98% of which have been resolved.[14]

HIPAA-aligned cyber risk management standards of care are found in OCR's published guidance documents, such as the *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*, which OCR published in 2010.[15] Additional insight on cyber risk management standards of care can be inferred from corrective actions imposed by OCR on non-compliant organizations. As of November 30, 2020, more than 28,481 OCR investigations have resulted in changes in privacy practices, via corrective actions or technical assistance.[16] These actions provide a wealth of information on OCR's expectations for cyber risk management practices.

National Institute of Standards and Technology (NIST). The third source of standards of care with respect to cyber risk management is found in NIST publications and resources. NIST used an open, collaborative process to develop an industry-agnostic, software-agnostic cybersecurity framework for critical industry sectors. The NIST Cybersecurity Framework was first released in 2014 but has

continued to evolve to meet new cybersecurity challenges. The NIST Cybersecurity Framework has been embraced by the health care industry. By 2018, a majority (57.9%) of health care organizations had already adopted the NIST Cybersecurity Framework.[17] In 2016, HHS released a document that provided a crosswalk between HIPAA Security Rule requirements and the NIST Cybersecurity Framework, further strengthening the NIST Cybersecurity Framework's position as a de facto standard of care for cyber risk management.[18]

These three sources—HIPAA, OCR guidance, and NIST—articulate the standards of care for cyber risk management. An organization that implements an ECRM program that is aligned with the guidance detailed in these sources will be able to:

- Conduct operations with the confidence that they have implemented policies and practices that provide far-reaching protections from critical cyber incidents that could harm patients and/or the organization.
- Document that the organization has "implemented a recognized industry standard in assessing, designing and improving its cybersecurity program."[19]
- Support a defense against claims of negligence in the event of a cybersecurity incident through a stronger affirmative defense.

Trend #2: Executive and Director Liability for Enterprise Cyber Risk Management Failures

A second notable trend is that liability for cyber incidents is not necessarily limited to the organization. C-suite executives and board members may also be held personally liable for ECRM failures, due to the responsibilities associated with their role in the organization.

Fiduciary Duty

Health care organization C-suite executives and board members, in fulfilling their responsibilities, operate as *fiduciaries*. The word "fiduciary" comes from the Latin word, *fiducia*, which means trust or confidence.[20] Fiduciaries have the "power and obligation to act for another . . . under circumstances which require total trust, good faith and honesty."[21] As fiduciaries, C-suite executives and board members have legal responsibilities (duties) both to the organization itself, and to the communities the organization serves (for example, patients).

One of those responsibilities is the *duty of care.* Duty of care means that the organization and/or individual (e.g., health care organization, executive leader, or board of directors' member) has a legal responsibility to act in a reasonable manner toward the people they are responsible for. In addition,

"duty of care requires that directors inform themselves 'prior to making a business decision, of all material information reasonably available to them.'"[22]

In negligence cases, the measure used to determine whether the defendant's actions were reasonable is the *standard of care*. In the event of a cybersecurity-related incident, the standard of care could reasonably be the HIPAA/OCR/NIST-based standards of care outlined above.

Regulatory Guidance

Changes in regulatory guidance have further emphasized the board's risk management responsibilities. The U.S. Securities and Exchange Commission (SEC) laid the groundwork for increased board responsibility in 2009, when it issued the following guidance:

disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company.[23]

In 2018, the SEC released additional guidance, the *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.[24] The SEC specifically addressed the importance of disclosures related to how boards meet their *cybersecurity* risk oversight responsibilities:

A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk. In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.[25]

Developments in Litigation

High-profile data breaches continue to plague organizations both within and outside of the health care industry. At the same time, multiple cybersecurity regulations, guidance, and resources (such as the NIST Cybersecurity Framework) have emerged. These two conditions—the emergence of known cyber risk, plus the development of protocols to manage the risk—have created a known duty to act with respect to corporate cybersecurity.

As a result, it has become increasingly common for the litigation that emerges after a cyber incident to include lawsuits targeting directors and officers for a breach of fiduciary duty. To date, many of these lawsuits have been dismissed. But as the repercussions of cyber incidents continue to be felt by an

increasing number of consumers, it is expected that more of these types of lawsuits will be filed, and that some of them will survive motions to dismiss.

Between the changes in regulatory guidance, and developments in litigation, it is likely that health care leaders, including board members, will see increased exposure to personal liability for ECRM failures. Research and advisory firm, Gartner, Inc., recently predicted that 75% of CEOs will be personally liable for "cyber-physical security incidents" by 2024.[26] Gartner defines cyber-physical systems (CPSs) as:

systems that are engineered to orchestrate sensing, computation, control, networking, and analytics to interact with the physical world (including humans). They underpin all connected IT, operational technology (OT) and Internet of Things (IoT) efforts where security considerations span both the cyber and physical worlds, such as asset-intensive, critical infrastructure and clinical healthcare environments [emphasis added].[27]

Conclusion

Health care organizations have developed expertise in managing the risk of medical malpractice lawsuits by paying close attention to clinical standards of care. As de facto standards of care emerge related to ECRM, it is becoming equally important for organizations to assess their cyber risk management practices in relation to these standards of care. Organizations that proactively address ECRM will be better able to manage cyber risks.

In addition, should a cyber incident occur, organizations that have proactively implemented appropriate ECRM policies and practices will be better positioned to assert that they have put practices in place that align with established cyber risk management standards of care. Implementing comprehensive ECRM policies and practices—which align with the requirements of HIPAA, OCR, and NIST—can reduce the risk of experiencing a significant cyber incident and may also serve to defend the organization's C-suite and board from allegations of negligence.

Endnotes

1 Yisroel Mirsky, Tom Mahler, Ilan Shelef, & Yuval Elovici, *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*, 28th USENIX Security Symposium (USENIX Security 19) 461-478 (Jan. 11, 2019), https://arxiv.org/abs/1901.03597. *See also Injecting and Removing Cancer from CT Scans*, YouTube.com (Apr. 3, 2019), https://www.youtube.com/watch?v=_mkRAArj-x0&feature=youtu.be.

2 Kim Zetter, *Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists*, Wash. Post, Apr. 3, 2019, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/.

3 Peter Moffett & Gregory Moore, *The standard of care: legal history and definitions: the bad and good news*, 12 Western J. of Emergency Med. 109–112 (Feb. 2011), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3088386/#.

4 *Texas & P. Ry. v. Behymer*, 189 U.S. 468, 470 (1903).

5 ECRI Guidelines Trust, https://guidelines.ecri.org/.

6 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

7 U.S. Dep't of Health & Human Servs., OCR Privacy Brief, *Summary of the HIPAA Privacy Rule* (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

8 67 Fed. Reg. 53181 (Aug. 14, 2002).

9 68 Fed. Reg. 8334 (Feb. 20, 2003).

10 U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Security Rule* (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

11 U.S. Dep't of Health & Human Servs., *Breach Notification Rule* (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

12 78 Fed. Reg. 5566 (Jan. 25, 2013).

13 American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, 123 Stat. 115 (2009).

14 U.S. Dep't of Health & Human Servs., *Enforcement Results as of November 30, 2020* (Dec. 15, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

15 U.S. Dep't of Health & Human Servs., OCR, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (July 14, 2010), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf

16 U.S. Dep't of Health & Human Servs., OCR, *Enforcement Highlights November 2020* (Dec. 15, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

17 Healthcare Information and Management Systems Society, *2018 HIMSS Cybersecurity Survey,* https://www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pd

18 U.S. Dep't of Health & Human Servs., OCR, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework* (Feb. 22, 2016), https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

19 Richard Raysman & John Rogers, with Practical Law Data Privacy Advisor, *The NIST Cybersecurity Framework*, Thomson Reuters Practical Law (2020).

20 Merriam-Webster Dictionary, *Fiduciary*, https://www.merriam-webster.com/dictionary/fiduciary.

21 Gerald Hill & Kathleen Hill, *Fiduciary*, The People's Law Dictionary, https://dictionary.law.com/default.aspx?selected=744.

22 *Smith v. Van Gorkem*, 488 A.2d 858 (1985); Cornell Law School, Legal Information Institute (LII), *Fiduciary Duty*, https://www.law.cornell.edu/wex/fiduciary_duty.

23 74 Fed. Reg. 68334 (Dec. 23, 2009).

24 Commission Statement and Guidance on Public Cybersecurity Disclosures, Release No. 33-10459; 34-82746 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

25 *Id.*

26 Gartner, Inc., *Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024*, (Sept. 1, 2020), https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl#:~:text=Liability%20for%20cyber%2Dphysical%20security,of%20property%20or%20environmental%

27 *Id.*

Bob Chaput is the Founder and Executive Chairman of the Board of Clearwater, a provider of health care cyber risk management solutions. 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). He has 35+ years of experience in the field, and has earned many risk management, privacy, and security professional certifications, including: Certified Information Systems Security Professional (CISSP), Health Care Information Security and Privacy Practitioner (HCISPP), Certified in Risk Information Security Controls (CRISC), Certified Information Privacy Professional/US (CIPP/US), Certified Ethical Hacker (C|EH), and NACD CERT Certificate in Cybersecurity Oversight. Bob can be reached at bob.chaput@clearwatercompliance.com.

Iliana Peters is a shareholder at Polsinelli PC. Iliana is recognized by the health care industry as a preeminent thinker and speaker on data privacy and security, particularly with regard to HIPAA, the HITECH Act, the 21st Century Cures Act, the Genetic Information Nondiscrimination Act (GINA), the Privacy Act, and emerging cyber threats to health data. For over a decade, she both developed health information privacy and security policy, including on emerging technologies and cyber threats, for the Department of Health and Human Services, and enforced HIPAA regulations through spearheading multi-million dollar settlement agreements and civil money penalties pursuant to HIPAA. Iliana is one of the very few attorneys to have a Juris Doctor (JD), a Master of Laws (LLM) in health care, and a data security certification, as a Certified Information Systems Security Professional (CISSP). Iliana can be reached at ipeters@polsinelli.com.

1099 14th Street NW, Suite 925, Washington, DC 20005 | P. 202-833-1100

For payments, please mail to P.O. Box 79340, Baltimore, MD 21279-0340