E-Briefings

VOLUME 20 • NO. 6 • NOVEMBER 2023

Avoiding Liability and Fulfilling Fiduciary Obligations in an Evolving Privacy and Security Landscape

By Carolyn V. Metnick, J.D., LL.M., Partner, *Sheppard Mullin*

While the U.S. healthcare regulatory landscape is constantly changing, an area that directly touches healthcare and has experienced significant change over the last year after being stagnant for almost a decade is that of privacy and security.[1]

The privacy regulatory landscape has been overhauled in the last year with the signing of at least 10 new state consumer privacy laws and other state health information privacy laws, such as Washington's My Health My Data Act and Nevada's Consumer Health Data Privacy Law.[2]

With the increased deployment of artificial intelligence, the rise in cybersecurity incidents, and important legal changes, hospital and health system boards should be aware of their organizations' privacy and security compliance obligations and their role in protecting their organizations, as well as their personal liability exposure in the event of failure to exercise oversight of these matters.

New SEC Rules on Cybersecurity

In July 2023, the U.S. Securities and Exchange Commission adopted new rules requiring public companies that are subject to the reporting requirements of the Security Exchange Act of 1934 to disclose material cybersecurity incidents and information regarding cybersecurity risk management, strategy, and governance.[3] The new rules also require disclosures about a company's process for assessing, identifying, and managing material risks and the effects of risks from threats and incidents, in addition to the board's role of oversight and management's role in assessment and management. Specifically, registrants must now:[4]

1 There have been few exciting developments in U.S. privacy law since the HIPAA Final Omnibus Rule with the exception of the rollout of the California Consumer Privacy Act and perhaps the New York Department of Financial Services Cybersecurity Regulation.

2 Connecticut recently amended its Data Privacy Act to adopt consumer health privacy protections.

3 The rules were published in the Federal Register on August 4, 2023, and are available at 88 FR 51896.

4 *Ibid*; see "Final Amendments."

- Describe the board's oversight of risks from cybersecurity threats.
- If applicable, identify any board committee or subcommittee responsible for oversight.
- Describe the process by which the board or such committee is informed about such risks.

For-profit publicly traded health systems, among other publicly traded healthcare organizations, became subject to these requirements when the amendments went into effect on September 5, 2023. As a result of these new rules, reporting companies must now disclose more information about their cybersecurity practices, including the role of the board in oversight, which may lead to increased personal exposure of directors for cybersecurity incidents.

Civil Liability for Poor Oversight

The disclosure of the names and roles of publicly traded directors who have cybersecurity oversight responsibility may make them easier targets in litigation for falling short in their duties, as is evidenced by years of shareholder derivative lawsuits alleging breach of fiduciary claims, among others, against officers and directors of companies in the wake of significant and highly public data breaches. These claims often involve allegations of breach of fiduciary duties and wasting of company assets. Plaintiffs also often assert securities fraud claims.

Shareholder derivative lawsuits brought against officers and directors relating to cybersecurity oversight failure are not a new trend.[5] However, we have now seen enough litigation and settlements in this area to know that the litigation is a serious headache for those named as defendants and that resolution can be expensive. For example:

- Following a 2017 data breach involving the data of 143 million consumers by a consumer reporting company, plaintiffs filed a securities class action against the company and its officers and directors.[6] Plaintiffs alleged, in part, that the company made misleading statements about the company's systems, failed to take basic precautions, and failed to adequately monitor. The case was ultimately settled for $149 million.
- In 2019, former directors and officers of a large technology company agreed to pay $29 million to settle a consolidated class action lawsuit claiming they breached their fiduciary duties following a data breach involving 3 billion data subjects.[7] In this case, the plaintiffs alleged, in part, that the directors and officers breached their duties by hiding the data breach from shareholders and the public.[8] The plaintiffs further claimed that the directors did not observe industry standards, respond to breaches, or train staff.[9]

5 See Carolyn Metnick, "Cybersecurity Responsibility and Accountability: What Directors and Officers Must Understand about Managing Data," *BoardRoom Press*, The Governance Institute, August 2016.

6 Kevin M. LaCroix, *"Equifax Data Breach-Related Securities Suite Settled for $149 Million," The D&O Diary*, February 17, 2020.

7 In re Yahoo! Inc. Securities Litigation (Case No. 17-CV-00373-LHK).

8 Annette M. Bevans, "Directors Beware: Yahoo Derivative Breach Settlement—What It Means for Personal Exposure of Directors for Cybersecurity Breaches," American Health Law Association, October 4, 2019.

9 *Ibid.*

10 In re SolarWinds Corporation Securities Litigation.

- Investors filed a similar action in 2020 against SolarWinds Corporation and its officers, including its former CEO, Executive Vice-President, Chief Financial Officer and Treasurer, and VP of Security Architecture, following a data breach that resulted in the company's investigation by the SEC regarding its cybersecurity disclosures and statements.[10] Among the plaintiffs' claims were claims for misleading investors about the company's cybersecurity posture and failing to take action around cybersecurity.
- In 2021, shareholders filed a securities class action against board members of a telecommunications company as a result of a data breach that exposed the personal information of 54 million consumers.[11] The plaintiffs alleged, in part, that the board breached its fiduciary duty by failing to have effective internal controls and failing to respond to red flags showing inadequate controls. Plaintiffs further alleged that the board was aware of substantial security risks and misrepresented them in SEC filings.[12]

Criminal Liability for Concealment and Egregious Actions

Poor cybersecurity oversight can rise to potential criminal liability where officers and directors have knowledge of the breach and intentionally conceal it, where cybersecurity preparedness falls below industry standards, or where misleading statements are made about preparedness. The conviction of Uber's Chief Security Officer arising out of his response to the 2016 hack of Uber was a landmark event. While the actions of the former CSO were egregious, the conviction garnered the attention of cybersecurity officers nationwide.

Risk Mitigation

The fiduciary duties of officers and directors have not changed yet there appears to be appropriately higher expectations about cybersecurity oversight and a commitment to hold those in charge accountable for failure in oversight. Officers and directors should continue to remain informed about their organization's cybersecurity compliance program and ensure that vulnerabilities are addressed. Regular reporting from the Chief Security Officer or his/her designee can help board members stay abreast of issues and remain sensitive to their importance. Officers and directors must exercise a duty of care, which requires them to stay informed, be attentive, and act in the best interest of their organizations. Failure to respond to breaches, ignoring industry standards, and misrepresenting the strength of the cybersecurity program, among other things, are clearly not in an organization's best interests and fall beneath the standard of attentiveness of a reasonably prudent director.

Not only are cyber events expensive, the consequences can impede the delivery of healthcare in a community if a hospital or health system is unable to operate.

11 Kevin LaCroix, "Data Breach-Related Derivative Suit Filed Against T-Mobile USA Board," *The D&O Diary*, November 30, 2021.

12 *Ibid.*

13 Lisa Pino, "Improving the Cybersecurity Posture of Healthcare in 2022," HHS, February 28, 2022.

Key Board Takeaways

- Conduct board education around your organization's privacy and security compliance obligations, board members' fiduciary responsibility for managing cyber risk, and their personal liability exposure in the event of failure to exercise oversight of these matters.
- Ensure the board is regularly informed about your hospital or health system's cybersecurity compliance program and that vulnerabilities are promptly addressed.
- Keep the board updated on relevant legal developments that illustrate the significance (e.g., financial cost, reputational harm, and community impact) of cybersecurity oversight failure.

Not only are cyber events expensive, the consequences can impede the delivery of healthcare in a community if a hospital or health system is unable to operate as a result, which can have a potentially devastating impact. In 2022, the Office for Civil Rights called on providers to strengthen their cyber posture following cyberattacks in 2021.[13] Recent years are not different, and hospital and health system boards can make a difference by keeping cybersecurity top of mind.

The Governance Institute thanks Carolyn V. Metnick, J.D., LL.M., Partner, Sheppard Mullin, for contributing this article. She can be reached at cmetnick@sheppardmullin.com. The author would also like to thank her colleague Esperance Becton for her research assistance.