AMERICAN HEALTH LAW ASSOCIATION

HEALTH LAW WEEKLY
March 3, 2023

Why ALL Health Care Organizations Must Care About SEC Proposed Cybersecurity Rule Changes

Rachel V. Rose, Rachel V. Rose—Attorney at Law PLLC

Bob Chaput, Clearwater

According to the American Hospital Association (AHA), there are 6,093 hospitals in the United States.[1] Of this total number, 1,228 are investor-owned (for-profit) acute care hospitals and 2,960 are nongovernment not-for-profit acute care hospitals.[2] The remainder of the 6,093 hospitals is comprised of government acute care hospitals (federal, state, or local government), psychiatric hospitals, and other hospitals.[3] All of these hospitals, regardless of their designation as for-profit, not-for-profit, or government, can likely agree on the sentiment—"cybersecurity is patient safety."[4]

As of September 2022, the New York Stock Exchange (NYSE) had a combined total of 2,578 listed domestic and international companies, while the Nasdaq had 3,788 for a total of 6,366 publicly listed companies.[5] The population of companies subject to the U.S. Securities and Exchange Commission (SEC) disclosure requirements is small, especially when considering the approximately 32.6 million businesses in the United

States.[6] The point is that private companies dominate the U.S. economy and may not be directly subject to SEC registration, reporting, and disclosure requirements. They are, however, increasingly targeted by adversarial threat sources and subject to the same accidental, structural, and environmental threat sources that public companies face. Getting an organization's cyber risk management "ducks in a row" is not just for SEC-regulated companies.

For-profit hospitals that are part of publicly traded health systems, such as Tenet Healthcare Corp. (NYSE: THC), HCA Healthcare, Inc. (NYSE: HCA), and Community Health Systems, Inc. (NYSE: CYH), have additional requirements because they are registered with the SEC and have additional obligations imposed by the related securities laws, including the Exchange Act of 1934.[7]

On March 9, 2022, the SEC announced the release of proposed rules related to cybersecurity risk management, corporate governance, and incident disclosure by public companies.[8] Publicly traded for-profit companies (and arguably those that are registered through different avenues with the SEC) are mandated by law to comply with the proposed rules once they are finalized.[9] As Gary Gensler, SEC Chair stated, "[t]oday, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks."[10] These risks also apply to non-publicly traded, not-for-profit, and government hospitals, whose executives and board members have fiduciary duties that include cybersecurity risk management.[11]

The European Union's (EU) Directive 2022/2555—Security of Network and Information Systems (NIS2) has cybersecurity mandates similar to the SEC's proposed rules; however, NIS2 extends beyond publicly traded organizations.[12] NIS2 was published and became effective on January 16, 2023 and requires cybersecurity risk management for a broad range of segments within the health care industry: (1) laboratories; (2) organizations engaged in research and development of medical products; and (3) medical product manufacturers, which include but are not limited to pharmaceuticals and medical devices.[13]

Like the Sarbanes-Oxley Act of 2002 (SOX),[14] in which "[s]ome hospitals have adopted SOX policies as best practices even though they are not legally bound to comply with most of its regulations,"[15] not-for-profit hospitals and health systems should consider compliance with the SEC cybersecurity rules a best practice and potentially a way to mitigate risk and be in a good position to either be acquired by a publicly traded company or fund or to go public.

This article highlights how all types of health care organizations, as well as medical device and pharmaceutical companies and business associates,[16] should consider adopting the compliance and cybersecurity risk management requirements of the SEC

proposed rules, which are soon to be imposed on all publicly traded companies. The following "Questions and Answers" highlight key areas for organizations to consider.

Analysis—Key Questions and Proposed Considerations

Q1: What are the fundamental requirements of the SEC's proposed rule?
As articulated in the text of the proposed rule, the SEC is proposing

> to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents. We are also proposing to require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk.[17]

Disclosure of cybersecurity incidents are material in SEC filings and to the public. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule,[18] as well as the Federal Trade Commission's Health Breach Notification Rule,[19] there are additional disclosure requirements for HIPAA covered entities, business associates, and subcontractors, as well as persons who handle personal health records.[20]

Q2: Why are these changes being proposed?
Cybersecurity risks and incidents can impact the financial performance or position of a company. Consistent, comparable, and decision-useful disclosures regarding an organization's cybersecurity risk management, strategy, and governance practices, as well as a company's response to material cybersecurity incidents, would allow investors to understand such risks and incidents, evaluate a company's risk management and governance practices regarding those risks, and better inform their investment and voting decisions.[21]

In recent testimony before the United States Senate Committee on Banking, Housing, and Urban Affairs, as it relates to public company disclosures, SEC Chairman Gary Gensler, stated "For the last 90 years, our capital markets have relied on a basic bargain. Investors get to decide which risks to take as long as companies provide full, fair, and truthful disclosures. Congress tasked the SEC with overseeing this bargain. We do so through a disclosure-based regime, not a merit-based one."[22] The proposed cybersecurity disclosure rule changes are all about what the SEC believes are full, fair, and truthful disclosures. "The proposed amendments are intended to better inform

investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents."[23]

Q3: When could these proposed changes be implemented?

The Notice of Proposed Rule Making was published in the *Federal Register* on March 23, 2022, and comments were initially due by May 9, 2022. The comment period was extended, with a total of 156 comments submitted as of this writing.[24] Although there is always the possibility of delays in rulemaking, the SEC's timetable for these changes shows final action by April 2023.[25]

Q4: Why should private and not-for-profit organizations also adhere to the SEC's proposed rule?

1. **The SEC has the authority to investigate all companies that seek to raise capital from U.S. investors.** Among other avenues, investors in private companies often exit by way of an initial public offering and going public. SEC's oversight includes all public and private companies making any false or misleading statements as part of an offering process.[26]
2. **A strategic acquirer of a private company may already be public and currently subject to SEC disclosure requirements.** In this case, any potential acquirer would already be filing required cyber-related reports and disclosures and would place value on any private company efforts to not only easily make the disclosures but, more importantly, to have a mature enterprise cyber risk management program in place. According to a recent *Forescout* report, 48% of business leaders encountered a critical cyber issue or incident during an M&A transaction that jeopardized the deal.[27]
3. **Protect current stakeholders.** Private companies and nonprofit organizations have customers, perhaps patients, investors, bankers, insurers, employees, and regulators (think: HIPAA, Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, General Data Protection Regulation, etc.), all of whom expect the organization to have and benefit from a robust cyber risk management.
4. **The cost of capital is lower for all organizations that establish, implement, and mature an enterprise cyber risk management program.** Credit-rating agencies—including Standard and Poor's, Moody's, and Fitch Group—have all implemented consideration of the financial impact of a cyberattack on an organization's credit rating. Moody's downgraded the credit rating for Equifax from "stable" to "negative" based on the immense data breach the company experienced in 2017.[28]
5. **Most private companies are part of public company supply chains**. Heads up, even though you may serve on the board of a private company, your customers and vendors may be public companies. When the proposed SEC cyber disclosure requirements are finalized, expect to have your public company stakeholders raise the ante in terms of your incident response and reporting to them. We saw similar requirements tighten when the Omnibus Final Rule

codifying the Health Information Technology for Economic and Clinical Health Act was published in the *Federal Register* in 2013.[29]

6. **Manage talent risk in the new world.** COVID-19, the "Great Resignation," big tech layoffs, and "quiet quitting" have created a new set of dynamics for organizations striving to attract and retain talent for their organizations. Organizations with tainted reputations due to material cyber incidents will likely have a more difficult time with talent management, now a board issue. Specific to cybersecurity talent, how competitive will your company be in attracting cybersecurity professionals in the face of the current shortage of 3.4 million cybersecurity workers worldwide?[30]

Conclusion

Whether addressing HIPAA or the SEC's proposal, companies should already have committed to cultivating a culture of compliance by continually addressing technical, administrative, and physical safeguards, approaching cybersecurity from the vantage points of prevention, detection, and correction. It is imperative for public, private, and not-for-profit health care organizations alike to ensure that adequate documentation exists to substantiate ongoing compliance because the public market, insurance companies, and banks issuing lines of credit will all require cybersecurity risk management.

About the Authors

Rachel V. Rose, JD, MBA is an accomplished attorney who in 2012 established her own law firm, Rachel V. Rose – Attorney at Law, PLLC (Houston, Texas), and began teaching bioethics at Baylor College of Medicine (Houston, Texas). In addition to representing clients in transactional, compliance, select government investigations, and litigation matters related to health care, cybersecurity, securities law, the False Claims Act, and Dodd-Frank, she has served as both a consultative and a testifying expert in a variety of cases. Ms. Rose is often quoted as an expert in a variety of publications, as well as a sought-after presenter and author of articles and books. www.rvrose.com.

Bob Chaput, NACD.DC, CISSP, HCISPP, CRISC, CIPP/US, C|EH, NACD CERT Cyber Risk Oversight is the author of *"Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)."* He is the Founder and Executive Chairman of Clearwater, a leading provider of cybersecurity, risk management, and HIPAA compliance software, consulting, and managed services—exclusively for health care. He is an adjunct faculty member of Quinnipiac University's School of Computing and Engineering, developing enterprise cyber risk management courses, an Institute of Advanced Network Security (IANS) Faculty Member, and an advisory board member of Kennesaw State Uinversity's Institute of Cybersecurity Workforce Development.

[1] American Hospital Association, *Fast Facts on U.S. Hospitals, 2022*, https://www.aha.org/statistics/fast-facts-us-hospitals (last visited Feb. 11, 2023).

[2] *Id*.

[3] *Id*.

[4] R.V. Rose, *Cybersecurity is Patient Safety* (Nov. 10, 2022), https://www.physicianspractice.com/view/cybersecurity-is-patient-safety (quoting Sen. Warner's November 2022 policy paper entitled "Cybersecurity is Patient Safety").

[5] Statisca, Comparison of the number of listed companies on the New York Stock Exchange (NYSE) and Nasdaq from 2018 to 3rd quarter 2022, by Domicile (Nov. 1, 2022), https://www.statista.com/statistics/1277216/nyse-nasdaq-comparison-number-listed-companies/.

[6] Small Business and Entrepreneurship Council, *Facts & Data on Small Business and Entrepreneurship*, https://sbecouncil.org/about-us/facts-and-data/ (last visited Feb. 11, 2023).

[7] *Id*.

[8] 87 Fed. Reg. 16590 (Mar. 23, 2003); SEC, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022), https://www.sec.gov/news/press-release/2022-39 (hereinafter, SEC Press Release).

[9] SEC, *Fact Sheet: Public Company Cybersecurity Proposed Rules*, https://www.sec.gov/files/33-11038-fact-sheet.pdf (last visited Feb. 11, 2023).

[10] *See supra* note 8, SEC Press Release.

[11] J. Halper, et al., *The Ramifications of The Delaware Court of Chancery's McDonald's Decision—Beyond Holding That Caremark Oversight Obligations Apply to Corporate Officers* (Feb. 9, 2023), https://www.natlawreview.com/article/ramifications-delaware-court-chancery-s-mcdonald-s-decision-beyond-holding-caremark.

[12] *See* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Jan. 16, 2023).

[13] J. Giantsidis, *New EU Directive Marks Cybersecurity Regulatory Paradigm Shift For Bio/Pharma & Medical Devices* (Feb. 15, 2023), https://www.meddeviceonline.com/doc/new-eu-directive-marks-cybersecurity-regulatory-paradigm-shift-for-bio-pharma-medical-devices-0001.

[14] SOX, Pub. L. No. 107-204 (Jul. 30, 2002).

[15] P. Loubeau, A. Griffith, *Some Empirical Evidence of Sarbanes-Oxley Implementation in the Hospital Sector*, The Coastal Business Journal, Vol. 11, No. 1 (Spring 2012), https://digitalcommons.coastal.edu/cgi/viewcontent.cgi?article=1069&context=cbj .

[16] U.S. Department of Health and Human Services, *Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited Feb. 11, 2023).

[17] 87 Fed. Reg. 16590.

[18] 45 C.F.R. §§ 164.400-414.

[19] R.V. Rose, *Cybersecurity risk considerations after the FTC's first breach notification settlement* (Feb. 9, 2023), https://www.physicianspractice.com/view/cybersecurity-risk-considerations-after-the-ftc-s-first-breach-notification-settlement.

[20] *Id*.

[21] B. Chaput, *Overview of the SEC "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" Proposed Rule Changes*, https://clearwatercompliance.com/blog/overview-of-the-sec-cybersecurity-risk-management-strategy-governance-and-incident-disclosure-proposed-rule-changes/ (last visited Jan. 11, 2023).

[22] Gensler, Gary, *Testimony Before the United States Senate Committee on Banking, Housing, and Urban Affairs (*Sept. 15, 2022), https://www.sec.gov/news/testimony/gensler-testimony-housing-urban-affairs-091522

[23] 87 Fed. Reg. 16590.

[24] SEC, *Comments on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, https://www.sec.gov/comments/s7-09-22/s70922.htm (last visited Feb. 11, 2023).

[25] SEC, *Cyber Risk Governance* (Spring 2022), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=3235-AM89.

[26] WTW, *SEC enforcement is not just a public company concern: What private companies need to know* (Nov. 18, 2019), https://www.wtwco.com/en-US/Insights/2019/11/sec-enforcement-is-not-just-a-public-company-concern-what-private-companies-need-to-know.

[27] Forescout, *The role of Cybersecurity in M&A Diligence* (2019), https://www.forescout.com/merger-and-acquisition-cybersecurity-report/.

[28] N.Lindsey, *Equifax downgrade shows the lasting financial impact of a massive data breach*, (Jun. 3, 2019), https://www.cpomagazine.com/cyber-security/equifax-downgrade-shows-the-lasting-financial-impact-of-a-massive-data-breach/.

[29] U.S. Department of Health and Human Services, *Business Associate Contracts*, https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last visited Feb. 15, 2023); *see also* 78 Fed. Reg. 5566 (Jan. 25, 2013).

[30] ISC2, (*ISC)2 CYBERSECURITY WORKFORCE STUDY 2022,* (Oct. 17, 2022), https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.