ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
JANUARY 9, 2025

Understanding cybersecurity trends and the new NYSDOH hospital regulations | Viewpoint

ANNA MERCADO CLARK, DOROTHY SHULDMAN, JULIA MARKOV, LISA SMITH

As technology advances, hospitals and other health care organizations face increasing cybersecurity vulnerabilities. Hospitals and health care organizations have been the subject of cybersecurity threats, such as ransomware attacks, that have impacted millions of people across the U.S. By staying informed of cybersecurity trends impacting health care and other sectors, stakeholders can effectively put plans in place to safeguard and improve their organization's cybersecurity. In addition to understanding the risks, health care organizations must also stay abreast of new cybersecurity regulations that impose new requirements on organizations' information technology infrastructure. In this article, we review emerging cybersecurity trends and discuss New York State's new cybersecurity regulations for hospitals.

CYBERSECURITY TRENDS

Two key reports, IBM's 2024 Cost of a Data Breach Report (the IBM Report)[i] and the U.S. Department of Health and Human Services' (HHS) 2023 Hospital Cyber Resiliency Initiative Landscape Analysis[ii], provide important overviews of current cybersecurity threat and mitigation strategy trends.

The IBM Report ranked health care as the industry with the highest average cost of a data breach for the 14th consecutive year at $9.77 million. Health care organization breaches also took the longest to identify and contain, at nearly 300 days.

According to the IBM Report, the top five factors that increased average breach costs for industries were security systems complexity, security skills shortage, third-party breach, noncompliance with regulations and migration to the cloud. The top five factors that decreased average breach cost included employee training, artificial intelligence (AI) and machine-learning driven insights, security information and event management (SIEM), incident response (IR) planning and encryption.

Meanwhile, HHS' Hospital Cyber Resiliency Initiative Landscape Analysis found that 89% of hospitals surveyed performed regular vulnerability scanning. In addition, 50% or less of hospitals evaluated risk to patient safety from third-party suppliers and 96% of hospitals used "antiquated" hardware, systems or software with known vulnerabilities. Notably, 99% of hospitals used basic spam and phishing protection, but these are not always effective against increasingly sophisticated social engineering and phishing attacks.

The trends identified in the two reports highlight the urgent need for organizations to evaluate and strengthen their cybersecurity practices in order to safeguard against potentially devastating consequences, including compromised data privacy, disrupted care, patient safety risks, regulatory implications, reputational damage and potential lawsuits.

NEW YORK STATE DEPARTMENT OF HEALTH'S NEW CYBERSECURITY REGULATIONS

In November 2023, Governor Hochul proposed cybersecurity regulations for hospitals with the intention of complementing the HHS' Health Insurance Portability and Accountability Act (HIPAA) Security Rule by requiring the implementation and maintenance of specific, minimum cybersecurity standards, including staffing, network monitoring and testing, policy and program development, employee training and remediation,

incident response, and reporting protocols and records retention. (Press Release, Governor Hochul Announces Proposed Cybersecurity Regulations for Hospitals Throughout New York State (Nov. 13, 2023)). While the costs of implementing the regulations will depend on the cybersecurity programs currently in place, it is estimated that it may cost between $250,000 and $10 million to initially develop and implement, and about $50,000 to $2 million (or more) to maintain annually, depending on the facility size.

On October 2, 2024, the New York State Department of Health (NYSDOH) adopted cybersecurity regulations (the Regulations), which contain revisions to the regulations proposed in November 2023. (10 NYCRR § 405.46 (2024)).

At this time, the Regulations apply to all general hospitals licensed pursuant to Article 28 of New York Public Health Law but do not extend to nursing homes or residential health care facilities, public health centers, diagnostic and treatment centers (including ambulatory surgery centers), outpatient lodges for cancer treatment, dispensary and laboratory or central service facilities serving more than one institution.

The Regulations include requirements for the protection of nonpublic information, which is broader than HIPAA's definition of protected health information.

Although the requirement on reporting cybersecurity incidents within 72 hours is currently in effect, hospitals will have until October 2, 2025, to come into compliance with much of the Regulations. The Regulations require, among other things: designation of a Chief Information Security Officer (CISO), who is responsible for developing, overseeing and enforcing the cybersecurity program and has certain reporting and attestation requirements; maintaining and implementing certain policies and procedures (including third-party risk management), as well as a written cybersecurity program upon recommendation by the CISO; security training and remediation for employees; and incident response preparedness.

The Regulations mark New York's response to threat actors' sustained attacks on this sector in an attempt to minimize data loss and delay of care. These changes align with broader cybersecurity trends in health care, including the adoption of zero-trust frameworks by health care organizations, the use of AI for cybersecurity threat detection and the growing emphasis on regulatory compliance in the health care information technology sector.

As cyber incidents become more costly, frequent and sophisticated, regulators are motivated to implement regulations for safeguarding sensitive data in hospitals' possessions. In fact, on December 27, 2024, HHS issued a proposed rule that would modify the HIPAA Security Rule with requirements for health plans, health care clearinghouses and most health care providers regarding strengthening the protection and security of electronically protected health information. (Press Release, U.S. Dep't of Health & Human Servs., HHS Office for Civil Rights Proposes Measures to Strengthen Cybersecurity in Health Care Under HIPAA (Dec. 27, 2024)). Accordingly, New York hospitals will need to develop a strategy for implementing the Regulations while being mindful of proposed new rules at the federal level as well.

It is important that hospitals review their compliance programs and seek assistance from experienced professionals in light of the Regulations.

Anna Mercado Clark, Partner and Chief Information Security Officer at Phillips Lytle, is the Co-Leader of the firm's Technology Industry Team. She can be reached at aclark@phillipslytle.com or (212) 508-0466.

Lisa L. Smith is a Partner and Co-Leader of the Health Care and Life Sciences Team at Phillips Lytle LLP. She can be reached at lsmith@phillipslytle.com or (716) 847-8336.

Dorothy E. Shuldman is an Attorney at Phillips Lytle LLP and a member of the firm's Corporate and Business Law Practice and Health Care and Life Sciences Team. She can be reached at dshuldman@phillipslytle.com or (716) 504-5778.

Julia M. Markov is a Science Specialist at the firm and a member of the Health Care and Life Sciences Team. She can be reached at jmarkov@phillipslytle.com or (716) 847-5442.

[i] IBM, *Cost of a Data Breach Report* 2024, https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700067972513691&p5=p&p9=587000075467407 65&gclid=EAIaIQobChMIqtqZ3MrZiQMVmkf_AR1BTyT6EAAYASABEgKTZfD_BwE&gclsrc=aw.ds (last visited Jan. 2, 2025).

[ii] Dep't of Health & Human Servs., Healthcare & Public Health Sector Coordinating Council, Ctrs. for Medicare & Medicaid Servs., HHS 405(d), *Hospital Cyber Resiliency Initiative Landscape Analysis* (Apr. 17, 2023), https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf.