Published on *The National Law Review* https://natlawreview.com

New York Adopts Comprehensive Hospital Cybersecurity Requirements

Article By:

Sara Helene Shanti

Michael D. Sutton

Cyberattacks on healthcare organizations are on the rise, with the number of affected individuals nearly tripling between 2022 and 2024, according to data compiled by the Department of Health and Human Services Office for Civil Rights ("OCR").[1] OCR data also reveals a 239% and 278% increase in hacking incidents and ransomware attacks, respectively, between January 2018 and September 2023.

Responding to this alarming trend, the New York State Department of Health ("DOH") finalized a regulation on October 2, 2024, introducing new cybersecurity requirements for in-state general hospitals.[2] The action signals an intensifying state interest in data privacy and maintenance.

Immediately Effective Obligations

The following requirements are effective as of October 2, 2024:

- Hospitals must notify the DOH as soon as possible, but no later than 72 hours after determining a "cybersecurity incident" has occurred, which generally includes a cybersecurity event[3] that: (1) has a materially adverse impact on the hospital's operations; (2) has a reasonable likelihood of materially harming any part of the hospital's operations; or (3) causes deployment of ransomware within a material part of the hospital's information systems.[4]
- Hospitals must maintain any and all documentation required by the new regulations for at least six years, including records, schedules, reports, and data. If the hospital identifies any "areas, systems or processes that require material improvement, updating or redesign," the hospitals must additionally document the identification and remedial efforts undertaken. In addition, hospitals must provide any documentation that the DOH requests.

Requirements Effective October 2, 2025

Effective a year from adoption of the regulation, hospitals must implement a cybersecurity program designed to perform the following key functions:

- Identify and assess internal and external cybersecurity risks that may threaten the security of "nonpublic information"[5] and the continuity of hospital operations.
- Implement defensive infrastructure, policies, and vulnerability assessments to protect information systems and nonpublic information from unauthorized access and malicious acts.
- Establish mechanisms to detect cybersecurity events promptly.
- Develop protocols to respond to and mitigate negative effects of cybersecurity events and to restore normal hospital operations and services.
- Designate a Chief Information Security Officer who will be responsible for submitting an annual report to the hospital's governing body on the cybersecurity program.
- Conduct testing and vulnerability assessments, including automated vulnerability scans and penetration testing, of the hospital's information systems.

Considerations for Hospitals

Even though the new regulation does not specifically enumerate available penalties, the regulation is not without teeth. In fact, DOH is authorized to impose civil penalties on parties who violate applicable laws and regulations[6] as well to require completion of costly corrective action plans. In addition, the requirements of the new regulation are a component of the minimum standards for hospitals, which are prerequisites to initial and ongoing licensure and certification. Failure to adhere to these requirements could risk licensure or certification.

We will continue to monitor for developments and will publish updates when available. Regarding the other requirements noted above, hospitals should also begin preparing for the compliance deadline next October.

FOOTNOTES

[1] Healthcare Data Breach Statistics, HIPAA Journal (Jul. 30, 2024), H1, 2024 Healthcare Data Breach Report.

[2] The revisions are specific to N.Y. Codes R. & Regs. tit. 10, § 405.46.

[3] N.Y. Codes R. & Regs. tit. 10, § 405.46(b)(5).

[4] A "cybersecurity event" means "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse the hospital's information system or information stored on such information system, including but not limited to health records." N.Y. Codes R. & Regs. tit. 10, § 405.46(b)(4).

[5] "Nonpublic information" covered by the regulation includes not only personally identifiable information and protected health information under HIPAA, but also certain of the hospitals' business-related information, if a compromise of that information would cause a material adverse impact to hospitals' business or operations. N.Y. Codes R. & Regs. tit. 10, § 405.46(b)(8).

[6] N.Y. Pub. Health Law § 12.

Listen to this post

Tina Watson contributed to this article

National Law Review, Volume XV, Number 6