akerman

Blog Post

New York Focuses on Healthcare Cybersecurity: Recent Regulatory and Enforcement Activities

November 12, 2024

By Jordan T. Cohen, Elizabeth F. Hodge, and Ameer Al-Khudari

The healthcare sector has seen an alarming uptick in cybersecurity incidents, including ransomware attacks, in recent years. In response to these cybersecurity threats, New York State is ramping-up efforts to protect patient data by issuing new cybersecurity regulations governing "general hospitals" and by requiring that a healthcare provider spend $2.25 million to improve its internal cybersecurity program as part of its settlement of cybersecurity breach claims.

The Regulatory Angle: What Hospitals in New York State Need to Know

The New York State Department of Health (Department) published the new cybersecurity regulations (Regulations) on October 2, 2024 to "ensure continued functioning of patient care and hospital operations." The Regulations only apply to "general hospitals" in New York; they are not applicable to other health care facilities like nursing homes, diagnostic centers, and treatment centers.

A copy of the full text of the Regulations is available on the Department's website. Notably, the Regulations' scope extends beyond protected health information under HIPAA to a hospital's nonpublic

Related People

Ameer Al-Khudari
Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Digital Health
Healthcare
Hospitals and Health Systems

Related Offices

Chicago
New York
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

business-related information and any information that can be used to identify a natural person.

Effective immediately, general hospital facilities in New York must report cybersecurity incidents to the Department "as promptly as possible, but no later than 72 hours after" determining a cybersecurity incident has occurred. This state regulation has a much shorter reporting window than HIPAA's Breach Notification Rule, which requires covered entities to report breaches that affect 500 or more individuals to relevant parties, including the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR), "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach."

A "cybersecurity incident" is defined as a cybersecurity event that:

1. has a material adverse impact on the normal operations of the hospital, or
2. has a reasonable likelihood of materially harming any part of the normal operation(s) of the hospital; or
3. results in the deployment of ransomware within a material part of the hospital's information systems.

The incident response report must be made "in the manner prescribed by the Department." Hospitals are also required to retain "any and all documentation related to cybersecurity incidents, such as records, schedules, reports" for a minimum of six years and be prepared to furnish such information to the Department upon request.

The new reporting requirement must be made in addition to other notifications required by state and federal law, such as HIPAA.

Beginning in October 2025, the Regulations will require that New York hospitals:

- establish a cybersecurity program within the hospital's policies and procedures;
- implement cybersecurity policies that are based on the facility's risk assessment and that address a minimum set of topics set forth in the Regulations;
- designate a Chief Information Security Officer;
- conduct an annual risk assessment;
- utilize qualified cybersecurity personnel;
- implement security policies for third-party service providers;
- implement identity and access management systems, including multi-factor authentication or other controls to protect against unauthorized access to nonpublic information;
- provide training and monitoring for personnel, including regular cybersecurity awareness training; and
- establish an incident response plan.

Hospitals subject to the Regulations must ensure proper planning to comply with these requirements before they become effective on October 2, 2025.

Non-Hospital Provider Settlement

A healthcare provider that operates specialized ENT and allergy facilities in upstate New York agreed to pay $2.75 million in penalties and towards data security enhancements to resolve cybersecurity claims that the New York Attorney General brought against it. In a rare development, state officials specified the dollar amount the provider must spend to improve its information security procedures.

The Attorney General alleged that the provider failed to protect medical data exposed in two ransomware cyberattacks that occurred within a two-week period in 2023. In total, the breach affected the medical records of more than 200,000 of the provider's patients.

The exposed data included patients' names, dates of birth, driver's license numbers, Social Security numbers, diagnoses, and medications, among other data. The cybercriminal group responsible for the attack claims that it has published two (2) terabytes of data from the provider's systems onto the dark web. While the provider initially disclosed the exposure of patients' Social Security numbers, it failed to report the disclosure of over 80,000 driver's license numbers.

The Attorney General's investigation found a string of cybersecurity failures. As is common with smaller providers, the practice lacked any employees with cybersecurity experience. Although the provider contracted with two third-party cybersecurity vendors, it allegedly failed to adequately monitor the vendors, who failed to install critical security software updates, to properly encrypt private consumer information, and to utilize proper authentication processes. Also, the provider "... was unable to confirm the attack vector in part because it did not retain server logs for a reasonable period of time and ... did not have security programs in place to monitor and analyze server traffic," the state said.

The October 29, 2024, settlement agreement provides for the following penalties and corrective action:

- pay $1 million of penalties in the form of two installments of $250,000, with the remaining $500,000 to be suspended if the provider satisfies its information security investment obligations described below;
- spend at least $450,000 a year for five years ($2.25 million total) to improve and maintain its information security program;
- maintain a comprehensive information security program that is reasonably designed to protect the security, integrity, and confidentiality of personal information; and

- appoint a “qualified individual” to be responsible for implementing, maintaining, and monitoring the information security program.

In addition to the high-level goals of the information security program described above, the $2.25 million the company must spend on security enhancements over a 5-year period will include conducting an inventory of private information on its systems, encrypting that information, implementing multifactor authentication on remote access devices, monitoring and logging all security activity, establishing a process to ensure critical security updates are timely made, and maintaining an incident response plan for future security issues.

* * * * *

Based on the new cybersecurity Regulations and New York State officials’continued attention to the uptick in cybersecurity concerns in the healthcare sector, hospitals and providers in the state should remain prepared for robust enforcement. Akerman’s healthcare attorneys continue to monitor these regulatory developments and enforcement activities and are available to assist hospital facilities and providers in determining how the New York State cybersecurity regulations may apply to them, and how to plan accordingly.
