GT GreenbergTraurig

Alert | Health Care & FDA Practice

October 2024

General Hospital Cybersecurity Requirements Take Effect in New York

Go-To Guide:

- New York adopts cybersecurity requirements for general hospitals, effective Oct. 2, 2024.
- Hospitals given one year to comply but must immediately report cybersecurity incidents.
- Regulation mandates comprehensive programs, policies, and appointment of chief information security officers.
- Requirements include regular testing, risk assessments, and incident response plans.

A new regulation related to cybersecurity program requirements for all New York general hospitals licensed under Article 28 of the Public Health Law (PHL) took effect Oct. 2, 2024. All general hospitals must comply with the new provisions within one year of the adoption date, except that general hospitals must immediately begin notifying the New York State Department of Health (Department) of any determined cybersecurity incident.

Background

In August 2023, Gov. Hochul released the New York State Cybersecurity Strategy to "better protect [the state's] critical infrastructure, personal information and digital assets from malicious actors." On Nov. 13, 2023, the governor announced the Department would adopt new cybersecurity regulations for the state's

general hospitals designed to protect against cyber threats to the hospitals' critical health care systems. In 2023, the Department responded to more than one cybersecurity incident per month, causing general hospitals to go on diversion, stopped billing procedures, and required facilities to operate on downtime procedures, which poised a significant health care risk to patients. The Department highlighted that in one breach alone, 225,000 patients had their data compromised.

Regulation Requirements

- Requires general hospitals to establish a comprehensive program covering risk assessment, response, recovery, and data protection.
- Mandates the creation of specific cybersecurity policies, including asset management, access, control, training, monitoring, and incident response.
- Requires the appointment of a chief information security officer in each general hospital responsible for program oversight and reporting.
- Requires general hospitals to conduct regular cybersecurity testing, including scans and penetration testing.
- Outlines cybersecurity risk assessment requirements that recognize HIPAA-compliant assessments.
- Defines qualifications and skills for cybersecurity staff.
- Sets policies for third-party cybersecurity providers.
- Mandates multi-factor authentication for external network access and risk-based authentication methods.
- Specifies requirements for ongoing training and monitoring.
- Defines incident response plan requirements, which would include roles, contact information, and incident determination.
- Requires general hospitals to report cybersecurity incidents affecting operations within 72 hours of the incident.
- Addresses confidentiality and the applicability of state and federal statutes.
- Allows for third-party or vendor contractors to complete compliance reporting and measures on behalf of the general hospital.

Applies to Article 28 General Hospitals Only

The newly adopted requirements apply only to "general hospitals" as defined under PHL §2801(10). Under New York law, a "general hospital" is narrowly and uniquely defined as a hospital engaged in "providing medical or medical and surgical services primarily to in-patients by or under the supervision of a physician on a twenty-four-hour basis with provisions for admission or treatment of persons in need of emergency care and with an organized medical staff and nursing service, including facilities providing services relating to particular diseases, injuries, conditions or deformities."

As such, the new regulation *does not apply* to PHL Article 28 licensed nursing homes or diagnostic and treatment centers (including ambulatory surgery centers). Nor does the new regulation apply to adult care facilities licensed under SSL Article 7. However, when presenting these requirements to the Public Health

and Health Planning Council, the Department indicated they would investigate applying some form of cybersecurity policy on other licensed facility types in the future.

HIPAA Security Requirements Remain

The new regulation intends to supplement, not supersede, any of the current federal Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements.

Final Regulation Extends Security Breach Notification

During the drafting process, the Department conducted several rounds of outreach with the hospital and health care sector to understand the current state of the industry. Stemming from the formal public comment process, the Department also amended the final regulation to require general hospitals to notify the Department as promptly as possible, but no later than 72 hours after determining a cybersecurity incident. The original draft required a two-hour reporting timeframe.

Implementation Costs Not Included

Costs to implement may range from $50,000-$2 million a year, depending on the size of the general hospital. Acknowledging this, the Department acted in January 2024 to mitigate the impact of the associated implementation costs and released Statewide Health Care Facility Transformation Program (SHCFTP) IV and SHCFTP V funds totaling $650 million to support facilities' technological needs, including cybersecurity purposes.

Conclusion

These requirements seek to safeguard the security of patients' protected health care information and personal identifying information. They aim to ensure all general hospitals develop, implement, and maintain minimum cybersecurity standards, including cybersecurity staffing, network monitoring and testing, policy and program development, and appropriate reporting protocols and record retention.

The new regulation is designed to supplement, not replace, existing security requirements currently required of general hospitals. Notably, the federal government is in the process of introducing enhanced cybersecurity measures for hospitals. New York general hospitals should be cautious about complying with any new cybersecurity rules and regulations that differ from the state's regulations.

Authors

This GT Alert was prepared by:

- Mark Furnish | +1 518.689.1400 | Mark.Furnish@gtlaw.com
- Jane M. Preston ˇ | +1 518.689.1447 | prestonj@gtlaw.com

ˇ *Not admitted to the practice of law.*