

## **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 posed 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](mailto:Mark.Furnish@gtlaw.com)
- **Jane M. Preston** <sup>~</sup> | +1 518.689.1447 | [prestonj@gtlaw.com](mailto:prestonj@gtlaw.com)

<sup>~</sup> *Not admitted to the practice of law.*

Albany. Amsterdam. Atlanta. Austin. Berlin<sup>~</sup>. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia<sup>\*</sup>. Las Vegas. London<sup>\*</sup>. Long Island. Los Angeles. Mexico City<sup>+</sup>. Miami. Milan<sup>\*</sup>. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo<sup>></sup>. Seoul<sup>Ⓢ</sup>. Shanghai. Silicon Valley. Singapore<sup>Ⓢ</sup>. Tallahassee. Tampa. Tel Aviv<sup>^</sup>. Tokyo<sup>\*</sup>. United Arab Emirates<sup><</sup>. Warsaw<sup>~</sup>. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ↯Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. \*Operates as a separate UK registered legal entity. «Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ›Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ¯Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¨Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹Greenberg Traurig's United Arab Emirates office is operated by Greenberg Traurig Limited. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2024 Greenberg Traurig, LLP. All rights reserved.*