LippesMathias LLP
ATTORNEYS AT LAW

Hospital Administrators – Is Your Hospital Cyber-Secure?

By Gregory T. Myers, Sarah E. Steinmann

November 6, 2024 | **ARTICLES**

On October 2, 2024, New York adopted new regulations requiring general hospitals to implement heightened cybersecurity safeguards. General hospitals, as defined in Article 28 of the NY Public Health Law, generally must begin complying with the regulation's cybersecurity program requirements by October 2, 2025. However, hospitals were obligated to begin complying with the regulation's incident reporting requirements on the regulatory adoption date – October 2, 2024.

The regulations, which create a new section 405.46 of Title 10 (Health) of the Official Compilation of Codes, Rules and Regulations of the State of New York, are intended to better protect patients' personally identifiable information (PII), protected health information (PHI), and other nonpublic information.

First Step: Risk Assessment

Hospitals should already have a cybersecurity program in place, so the first step for administrators will be to take a hard look at their current program to identify risks and vulnerabilities to the confidentiality of nonpublic information stored by the hospital and its third-party service providers. This process should include an evaluation of the continuity of the hospital’s business and operations to detect any gaps that might leave PII, PHI, and other patient information exposed during a cybersecurity event.

The risk assessment will serve as the foundation for building or enhancing a cybersecurity program that satisfies the regulations and should help the hospital identify the information systems they need to achieve that goal.

Designing Cybersecurity Programs & Policies

Based on current industry standards and practices, a hospital cybersecurity program should:

1. Identify and assess cybersecurity risks that leave nonpublic information vulnerable to attack;
2. Use defensive infrastructure, policies, and procedures to protect the hospital’s information systems, business and operations, and nonpublic information from unauthorized access, use, or malicious acts;
3. Detect cybersecurity events;
4. Recover from cybersecurity events leading to restoration of normal operations; and
5. Fulfill all reporting obligations.

The regulations outline the minimum standards for a hospital cybersecurity program. Issues that must be addressed include:

- Limits on user access privileges to systems that store nonpublic information;
- Evaluations of internally and externally developed applications used by the hospital;
- The secure disposal of nonpublic information;
- Encryption of nonpublic information held or transmitted by the hospital;
- Mitigation of risks from electronic mail-based threats; and
- Security policies for third party service providers.

The regulations outline fifteen (15) additional topics that must be covered by a hospital’s cybersecurity policies, including managing vendors and third-party service providers that may handle patient information. The prevalence of vendors and third-party service providers within healthcare business models places additional pressure on hospitals to ensure that patient information is managed correctly by vendors and third-party service providers. Hospitals should ensure that standard contract language used when engaging vendors and third-party service providers is updated to require compliance with the new regulations and for appropriate accountability in the event of data mishandling.

Designating A Chief Information Security Officer

Each hospital must designate a qualified Chief Information Security Officer (CISO) to oversee its cybersecurity program. Notably, the CISO does *not* need to be a hospital employee. Instead, hospitals may contract with a third-party provider or vendor to fill the role of CISO. This may help smaller hospitals lower the costs associated with their cybersecurity program. Hospitals engaging a third party to act as CISO must carefully craft the contract for CISO services to include the duties delineated in the new regulation.

The CISO is required, by the regulation, to provide the hospital’s governing body with an annual report on the cybersecurity program and material cybersecurity risks. The report must discuss the confidentiality of nonpublic information, cybersecurity policies and procedures, the overall effectiveness of the hospital's cybersecurity program, and cybersecurity incidents from the previous year.

The regulations also require the CISO to oversee on-going vulnerability testing and perform an annual risk assessment to drive the hospital's continued compliance with best practices in cybersecurity.

Hospital-Wide Employee Training

The regulations further require that Hospitals take special care to ensure that employees only have access to nonpublic information that is necessary to do their specific job. This includes limiting the number of privileged accounts and limiting the functionality of those accounts. User access privileges must be reevaluated annually and accounts that are no longer necessary must be promptly removed or disabled. Controls that monitor authorized users' activity to detect unauthorized access or unauthorized use of non-public information must be implemented.

Hospitals are also required to provide regular cybersecurity awareness training for all personnel. The trainings should be updated annually to include any risks identified in the hospital's annual risk assessment. Such trainings could include phishing exercises, training on multi-factor authentication, or remediation for employees.

Reporting Requirements – Effective Now!

The incident reporting requirements became effective as of October 2, 2024. Under the regulations, hospitals must notify the New York State Department of Health within 72 hours of determining a cybersecurity incident has occurred. Notice to the Department is *in addition to* any other reporting requirements under State or Federal law. Records, schedules, reports, and data regarding any cybersecurity incident must be maintained for at least six (6) years.

If a cybersecurity incident exposes areas, systems, or processes in need of material improvement, the hospital must document those efforts and maintain records of those efforts for inspection by the Department.

New York Supplements HIPAA Security Rule Framework

The New York cybersecurity regulations for general hospitals mandate specific protective actions not explicitly required by HIPAA's Security Rule. The Security Rule, as administered by the Department of Health and Human Services (HHS), requires that covered entities (including general hospitals and their business associates) ensure the confidentiality, integrity, and availability of patients' electronic PHI (ePHI), identify and protect against threats, and train a compliant workforce. Despite the Security Rule's overarching cybersecurity protections and requirements, HHS's resources for the granular and specific implementation of those protections and requirements are more appropriately characterized as guidelines. New York's cybersecurity regulations take further steps into the implementation process by explicitly requiring the incorporation of additional safeguards for the protection of patients in New York's general hospitals. Therefore, general hospitals should view the regulations as additional layers of protection on top of federal requirements.

Investment in Cybersecurity Compliance Reduces Risks of Costly Investigations, Litigation, and Enforcement

Due to reporting requirements under other state and federal laws and regulations, regulators like the New York State Department of Health, the NYS Attorney General, and the HHS Office of Civil Rights (OCR), cybersecurity failures and breaches often lead to costly investigation and oversight. If investigations reveal deficiencies in a provider's cybersecurity apparatus, costly compliance and enforcement actions follow. Therefore, investing in cybersecurity as an integral part of the data management process can save providers from costly regulatory remedies and can save patients and their health information from needless exposure.

On October 31, 2024, OCR issued a press release as part of a settlement with a South Dakota healthcare provider due to the provider's failure to protect against ransomware infection. As part of the settlement, the provider agreed to pay $500,000 in penalties to OCR and to implement an enhanced cybersecurity program that is compliant with applicable laws and regulations. OCR will monitor this implementation for a period of two years. Although the cost of the implementation is not noted, settlements can require a minimum dollar investment in cybersecurity while additional penalties are held in abeyance. This drives up the total cost of non-compliance.

Cyber-threats, and protecting data from them, are a reality with which providers must now live. Since 2018, "large breaches" reported to OCR have increased by a staggering 264%. As part of the press release, OCR identified ransomware and hacking as "the primary cyber-threats in health care." General hospitals, and healthcare providers in general, must be mindful that their patients' data is constantly at risk of exposure from cyber-threats.

General hospitals and healthcare providers should view cybersecurity compliance as an investment for their business and as insurance for the patients' data and privacy. For more information regarding compliance with state and federal cybersecurity requirements, contact Lippes Mathias attorneys Gregory T. Myers by phone at 518-462-0110 ext.1410 or by email at gmyers@lippes.com and Sarah E. Steinmann by phone at 315-477-6232 or by email at ssteinmann@lippes.com.

Resources

General hospital administrators enjoy a wealth of State and Federal resources to help them manage their data privacy and cybersecurity requirements. A sample of these resources are provided below:

- Notice of Adoption
- Text of Regulation
- HHS Security Rule
- HIPAA Security Rule Toolkit from the National Institute of Standards and Technology
- Cybersecurity & Infrastructure Security Agency Toolkit for Healthcare and Public Health

Attorey advertising. Prior results do not guarantee a similar outcome.