Now & Next
Healthcare Alert

October 11, 2024

New York adopts cybersecurity regulations for general hospitals

By Mukta Chilakamarri, Laurie T. Cohen, and Justin D. Pfeiffer

The new regulations lay out requirements for risk assessments and a 72-hour reporting window.

What's the impact?

- Effective immediately, general hospitals in New York must report to the NYSDOH, within 72 hours, any discovery of a cybersecurity incident.
- General hospitals have until October 2, 2025, to implement a written cybersecurity program, designate a Chief Information Security Officer (CISO), perform risk assessments, and adopt multifactor authentication controls that align with industry standards.

On October 2, 2024, the New York State Department of Health (NYSDOH) adopted hospital cybersecurity regulations requiring general hospitals in the state to, among other requirements, establish a cybersecurity program based on the hospital's risk assessment. The regulations also require general hospitals to notify the NYSDOH within 72 hours of a cybersecurity incident. The newly adopted regulations contain revisions to the regulations proposed in November 2023 as part of Governor Hochul's New York State Cybersecurity Strategy.

New cybersecurity program requirements for general hospitals

The adopted regulations require New York general hospitals to: (1) establish within their policies and procedures a cybersecurity program based on the hospital's risk assessment, (2) maintain records of their cybersecurity systems including audit trails detecting and responding to cybersecurity events that have a reasonable likelihood of materially harming normal operations of the hospital, (3) designate a Chief Information Security Officer (CISO) to enforce the new policies, (4) notify the NYSDOH within 72 hours of any cybersecurity incident, and (5) use risk-based authentication or multi-factor authentication (MFA) controls to protect against unauthorized access to its nonpublic information or information systems.

Changes to cybersecurity incident reporting timeframe

Although the final regulations give general hospitals until October 2, 2025 to come into compliance with a majority of the new requirements, the mandate to notify the NYSDOH within 72 hours after the discovery of a cybersecurity incident is effective immediately. (Notably, the 72-hour reporting window is longer than the 2-hour window that the NYSDOH originally proposed.) Like the proposed regulations, a "cybersecurity incident" is defined as an event that: (i) has a material adverse impact on the normal operations of the hospital, (ii) has a reasonable likelihood of materially harming any part of the normal operation(s) of the hospital, or (iii) results in the deployment of ransomware within a material part of the hospital's information systems.

Additional guidance

Additionally, in its response to public comments, the NYSDOH clarified that the adopted regulations apply only to general hospitals and not to managed care organizations. The NYSDOH also revised the definition of "nonpublic information" to specify that a cybersecurity program must protect, in addition to certain sensitive "business-related information," protected health information (PHI) and personally identifying information (PII) as defined in the federal Health Insurance Portability and Accountability Act (HIPAA). As a result, a hospital's cybersecurity program must be designed to protect a broader range of information than HIPAA requires.

Lastly, with respect to the use of MFA controls, the adopted regulations revised the definition of "multi-factor authentication" to, according to the NYSDOH, more closely align with industry standards. The NYSDOH has indicated that it will be publishing guidance that will map the requirements in the regulations to standards published by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA).

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Mukta Chilakamarri
518.427.2665
mchilakamarri@nixonpeabody.com

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Justin D. Pfeiffer
518.427.2742
jpfeiffer@nixonpeabody.com