Now & Next
Healthcare Alert

November 27, 2023

New York proposes cybersecurity regulations for hospitals

By Laurie T. Cohen and Mukta

The proposed regulations are aimed at strengthening
The proposed regulatiagainst increasingly disruptive cyber threats.
against increasingly di

What's the impact?

- All hospitals operating in New York State would be required to establish a written cybersecurity program, designate a Chief Information Security Officer (CISO), perform risk assessments, and utilize multifactor authentication.
- Hospitals would also have new obligations to submit reports of cybersecurity incidents to the NYS Department of Health (NYSDOH).

On November 13, 2023, New York Governor Hochul announced proposed cybersecurity regulations applicable to all hospitals located within the state. The proposed regulations would amend the State Hospital Code and are aimed at strengthening hospital efforts at safeguarding hospital systems and nonpublic information from cyber threats.

According to the draft regulations, in 2023 the NYSDOH had responded to more than 1 cybersecurity incident per month. These incidents resulted in hospitals going on diversion, interrupted their billing procedures, and required facilities to operate on downtime procedures.

The proposed regulations would require hospitals to establish within its policies and procedures a cybersecurity program based on the hospital's risk assessment. The cybersecurity program would be expected to supplement existing HIPAA security and privacy requirements. Under the proposed regulations, a compliant cybersecurity program must:

- identify and assess internal and external cybersecurity risks;
- use defensive infrastructure and policies and procedures to protect the hospital's information systems and nonpublic information stored on those information systems from unauthorized access;
- detect, respond, and recover from identified or detected cybersecurity events;
- limit user access privileges to access information systems that include nonpublic information;
- periodically assess the strength of the cybersecurity infrastructure;
- securely dispose of any nonpublic information identified that is no longer necessary for business operations; and
- implement security measures and controls, including encryption, to protect nonpublic information held or transmitted by the hospital.

Additionally, the proposed regulations would require hospitals to maintain records of the cybersecurity systems including any audit trails detecting and responding to cybersecurity events that have a reasonable likelihood of materially harming normal operations of the hospital and assessments identifying areas of the cybersecurity system that require improvement, updates, or redesign. These records would be maintained for a minimum of 6 years.

Hospitals would also need to designate a Chief Information Security Officer or "CISO" to enforce the new policies and to annually review and update them as needed. The CISO could be a hospital employee or supplied by a third-party vendor. In addition to existing reporting/notification requirements, a hospital's CISO would be responsible for notifying the NYSDOH within 2 hours of a cybersecurity incident.

The proposed regulations define a "cybersecurity incident" as a cybersecurity event that:

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

Finally, the proposed regulations would require hospitals to use risk-based authentication or multi-factor authentication controls to protect against unauthorized access to its nonpublic information or information systems.

The proposed regulations are expected to be published in the State Registrar on December 6, 2023, and the public comment period would extend to February 5, 2024.

If the proposed regulations are adopted, New York hospitals will have one year to comply with the new requirements; however, the obligation to report cybersecurity incidents to NYSDOH would be effective immediately.

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

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Mukta Chilakamarri
518.427.2665
mchilakamarri@nixonpeabody.com