spg SACHS POLICY GROUP
60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

NYS Proposed Cybersecurity Regulations

OVERVIEW

On November 13th, Governor Hochul announced that the State is proposing new cybersecurity regulations for hospitals. The regulations would apply to all general hospitals licensed under Article 28 of the Public Health Law. Under the proposed regulations, hospitals would be required to establish a cybersecurity program to:

- Identify and assess internal and external cybersecurity risks;
- Use defensive techniques and infrastructure to protect information systems;
- Detect cybersecurity events;
- Respond to cybersecurity events to mitigate negative effects; and
- Recover from cybersecurity events and incidents and restore normal operations and services.

Hospitals will be eligible to apply to a pool of the upcoming round of the Statewide Health Care Facility Transformation Program (with up to $500 million in total funding, as allocated in this year's Enacted Budget) to support projects that will make improvements to technology systems to help hospitals comply with the proposed regulations.

The regulations will be sent to the Public Health and Health Planning Council (PHHPC) for approval. They will also be published in the State Register and are expected to be open to public comment through February 5, 2024. Once finalized, hospitals will have one year to come into compliance with the new regulations.

The Governor's press release is available here. The proposed regulations are available here and a brief summary is provided below.

CYBERSECURITY PROGRAM

The proposed regulations would require each hospital to establish a comprehensive cybersecurity program based on the hospital's annual risk assessment. The annual risk assessment would be conducted to determine potential risks and vulnerabilities related to confidentiality, integrity, and availability of nonpublic information (e.g., electronic protected health information, social security numbers, etc.). Risk assessments performed for other regulatory purposes, such as the Health Insurance Portability and Accountability Act (HIPAA), may be accepted for compliance with this requirement.

The cybersecurity program would supplement, and not replace, any existing patient protections mandated under HIPAA. Hospitals would be permitted to use an affiliate or qualified third-party service provider to support compliance with the new regulations.

The cybersecurity program would be created, implemented, and overseen by a designated Chief Information Security Officer (CISO). The CISO would be a senior or executive level staff member who may be an employee of the facility or who may be employed by a third party or contract vendor. The CISO would provide, on an annual basis, a report to the hospital's governing body on the effectiveness of the hospital's cybersecurity program and material cybersecurity risks.

60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

Each hospital's cybersecurity program would be required to:

- Limit user access privileges to information systems that provide access to nonpublic information;
- Ensure the use of secure development practices for in-house developed applications utilized by the hospital, and procedures for evaluating, assessing, and testing the security of externally developed applications utilized by the hospital;
- Ensure the secure disposal, on a periodic basis, of any nonpublic information that is no longer necessary for business operations, except where such information is otherwise required to be retained by law or regulation or where targeted disposal is not feasible due to the manner in which the information is maintained; and
- Implement security measures and controls, including encryption, to protect nonpublic information held or transmitted by the hospital, both in transit over external networks and at rest. If encryption is not feasible, the hospital must instead secure the nonpublic information using effective alternative "compensating controls," defined as alternative measures that satisfy the requirement for the security measure if implementation is otherwise not reasonable or appropriate.

POLICIES AND PROCEDURES

The policies and procedures would be developed by the CISO and hospital information security/information technology staff and approved by the hospital's governing body. The policies would be based on the hospital's risk assessment and address, at a minimum, the following:

- Information security;
- Data governance and classification;
- Asset inventory and device management;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Patient data privacy;
- Vendor and third-party service provider management;
- Risk assessment;
- Training and monitoring; and
- Overall incident response.

Monitoring, Training, and Records Maintenance

Hospitals would be required to provide regular cybersecurity awareness training for all personnel, which may include annual phishing exercises and training/remediation for employees. Hospitals would be required to use multi-factor authentication, risk-based authentication, or other compensating control to protect against unauthorized access to nonpublic information or information systems. Multi-factor

60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

authentication would be a requirement for any individual accessing the hospital's internal networks from an external network, unless the CISO has approved in writing the use of compensating controls.

Each cybersecurity program would include monitoring and testing requirements, including:

- Annual penetration testing of the hospital's information systems by a qualified internal or external party; and
- Automated scans or manual/automated reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the hospital's information systems based on the risk assessment.

Hospitals would be required to maintain records related to systems design, security, and maintenance that support normal operations for a minimum of six years. Records pertaining to audit trails designed to detect and respond to cybersecurity events and incidents must also be maintained for a minimum of six years.

Incident Response Plan

Hospitals would be required to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity incident materially affecting the confidentiality, integrity, or availability of the hospital's information systems or the continuing functionality of any aspect of the hospital's business or operations. The incident plan would address, at a minimum:

- The goals of the incident response plan;
- The definition of clear roles and responsibilities, a list of actual personnel and both business hour and off-business hour contact information with levels of decision-making authority;
- External and internal communications and information sharing about any incidents;
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- The internal processes for responding to a cybersecurity event including, at a minimum, mitigation, downtime procedures and contingency plan, and process for determining if a cybersecurity event (defined as an attempt to gain unauthorized access to information) becomes a cybersecurity incident (defined as a cybersecurity event that has a material adverse impact on the hospital), and processes for determining the material adverse impact;
- Documentation and reporting regarding cybersecurity events and related incident response activities; and
- The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

The CISO or their designee would be required to notify the State Department of Health (DOH) within two hours of a determination that a cybersecurity incident has occurred and has had a material adverse impact on the hospital.