HANYS®
Always There for Healthcare

Marie B. Grause, RN, JD • President

Headquarters
One Empire Drive, Rensselaer, NY 12144
518.431.7600

Washington, DC Office
499 South Capitol Street SW, Suite 410
Washington, D.C. 20003
202.488.1272

February 4, 2024

Katherine E. Ceroalo
New York State Department of Health
Bureau of House Counsel, Regulatory Affairs Unit
Corning Tower Building, Rm. 2438
Empire State Plaza
Albany, New York 12237

Re: Hospital Cybersecurity Requirements: HLT-49-23-00001-P

Dear Ms. Ceroalo:

On behalf of the Healthcare Association of New York State's member nonprofit and public hospitals, nursing homes, home care agencies and other healthcare organizations, I write to provide comments on the above-referenced proposed regulations related to hospital cybersecurity.

HANYS appreciates DOH's willingness to meet with HANYS and our member organizations to help create effective and practical regulations. HANYS and our member hospitals work and invest on a continual basis to improve our cybersecurity posture amid ever-changing threats and attackers.

We look forward to continuing to work with DOH to improve cybersecurity and the business continuity and emergency management planning necessary to mitigate disruptions. We appreciate the proposal to create a state healthcare cyber roundtable.

HANYS agrees with the premise and principle of the proposed regulations; however, our members have serious concerns about their implementation.

Alignment with federal standards

It is critical that cybersecurity regulations across local, state and federal levels avoid creating duplicative or conflicting requirements for hospitals. We urge DOH to align these proposed regulations with existing and upcoming federal standards, such as Health Industry Cybersecurity Practices and the National Institute of Standards and Technology's cybersecurity framework, which many hospitals are already adopting.

Imposing additional New York-specific requirements that deviate from federal standards would further strain hospitals' limited resources. Instead the state should provide education and resources to assist hospitals in meeting national best practices such as the NIST standards.

The U.S. Department of Health and Human Services recently announced plans to propose federal cybersecurity regulations in 2024. HANYS strongly encourages DOH to work in alignment with HHS to avoid any duplication or mismatch of state and federal requirements.

The proposed state cybersecurity regulations as written do not match federal regulations or existing standards for management of "non-public" data, prescriptive third-party contract rules or two-hour notification.

Broad definition of "nonpublic information"

The definition of "nonpublic information" in the proposed regulations goes beyond protected health information. It would require hospitals to apply rigorous cybersecurity controls to a wide array of business data, which would be cost-prohibitive for many hospitals.

HANYS recommends narrowing the definition of nonpublic information to PHI and personally identifying information, aligning with existing state and federal regulations like the Health Insurance Portability and Accountability Act. The "Effect of Rule" section within the proposed regulations notes that the program is intended for safeguarding and securing PHI and PII. Adding extensive new categories of protected data would likely require new systems for access controls, encryption and auditing. Hospitals would be burdened with another project, with limited or uncertain benefit.

Third-party vendor management and controls

The proposed regulations would require each hospital to implement written policies and procedures to assess third-party providers for their security procedures and to ensure they meet existing standards. The regulations also include minimum requirements for third-party vendors for hospitals to contract with them.

In the current state healthcare technology marketplace there are few vendors available for specialized services and it is often burdensome to switch vendors for services. The proposed requirements would leave little leverage for even the largest of health systems to set terms or customize such contracts.

Due to the challenging healthcare technology industry and limited options available to hospitals, HANYS recommends removing language that prescribes specific contract elements and adjusting implementation timelines to maximize flexibility and implementation feasibility.

Two-hour notification and incident definition

The proposed regulations would require a two-hour turnaround to notify DOH of a "determination that a cybersecurity incident has occurred and has had a material adverse impact on the hospital."

HANYS has several concerns with the proposed reporting timeframe. Time spent reporting to DOH would take valuable time away from mitigating an ongoing attack. Additionally, the definition of a cybersecurity incident is vague. HANYS recommends a clearer definition that states the hospital will notify DOH within two hours of its site-wide emergency management or incident response team having met and determined that the current crisis will impact care and operations. Notification should not occur until the hospital has determined that the attack will have an adverse effect on hospital operations. Setting unrealistic reporting requirements would distract hospitals' incident response teams from priorities like restoring care.

HANYS recommends aligning the definition and reporting timelines with the federal HIPAA requirement of 72 hours. This also aligns with current New York state Department of Financial Services cyber incident reporting.

HANYS understands DOH's desire for an immediate assessment of existing network links to the site under attack. However, hospitals do not have direct, real-time, continual integrations with DOH. If the goal is to manage networks in real-time, healthcare systems, health information exchanges and the state should all be notified simultaneously once an incident is confirmed.

HANYS strongly encourages establishing this capability at the previously discussed proposed state healthcare cybersecurity roundtable.

Funding

While the proposed $500 million in assistance for hospital information technology infrastructure upgrades will be useful, many hospitals across the state have been planning to use these funds for foundational tools such as electronic health records. Most new technology investments are now following a cloud-based subscription model rather than capital improvements to on-premises data centers. Financial assistance needs to focus on supporting recurring software/platforms and employee costs rather than one-time infrastructure projects. New infrastructure and security systems do not bring value without ongoing staff and vendor support.

HANYS recommends allocating a significant portion of the proposed funding to offset the operating expenses associated with new cybersecurity platforms and services. This would provide more impactful assistance as hospitals adapt their technology to these new regulations.

Thank you for the opportunity to voice our concerns. Strengthening hospital cybersecurity is important, but regulations must strike the right balance between security, cost and patient impact. As always, we are ready to assist as needed. If you have questions, please contact me at 518.431.7719 or thallise@hanys.org.

Sincerely,

Thomas Hallisey

Thomas Hallisey
Director, Digital Health Strategy