February 5, 2024

New York State Department of Health
Bureau of Program Counsel, Regulatory Affairs Unit
Corning Tower, Empire State Plaza, Rm. 2438
Albany, New York 12237-0031

Submitted electronically via regsqna@health.ny.gov

Subject: Addition of Section 405.46 to Title 10 NYCRR (Hospital Cybersecurity Requirements)

DirectTrust appreciates the opportunity to comment on the New York State proposed rules to create cybersecurity requirements for all hospital facilities. We commend the State for providing guidance to hospitals as well as financial resources for this effort, which is congeneric with recent federal activity on cybersecurity in health and public health sectors [1234]

Relevant Background

DirectTrust™ is a non-profit, vendor-neutral alliance dedicated to instilling trust in the exchange of health data. The organization serves as a forum for a consensus-driven community focused on health communication, an American National Standards Institute (ANSI) standards development organization, an accreditation and certification body through EHNAC (the Electronic Healthcare Network Accreditation Commission), and a developer of trust frameworks and supportive services for secure information exchange like Direct Secure Messaging and trusted, compliant document submission.

The goal of DirectTrust is to develop, promote, and, as necessary, help enforce the rules and best practices necessary to maintain privacy, security, and trust for stakeholders across and beyond healthcare. In addition, DirectTrust is committed to fostering widespread public confidence in the interoperable exchange of health information while promoting quality service, innovation, cooperation, and open competition in healthcare.

Comments

DirectTrust has the following specific comments for consideration:

---

[1] Healthcare and Public Health (HPH) Cybersecurity Performance Goals https://hphcyber.hhs.gov/performance-goals.html

[2] Federal Cybersecurity Strategic Research & Development Plan https://www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

[3] Hospital Cyber Resiliency Initiative Landscape Analysis Hospital Cyber Resiliency Initiative Landscape Analysis https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

[4] Healthcare Sector Cyber Security https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

- Section 405.46 (c) states "(1) Each hospital shall establish within its policies and procedures a cybersecurity program based on the hospital's risk assessment. (2) The cybersecurity program shall be designed to supplement HIPAA and shall not replace any provisions of the HIPAA Security Rule (45 CFR part 160 and subparts A and C of part 164), or any existing patient protections afforded and mandated under HIPAA. Hospitals are expected to comply with this section and HIPAA",

  We find this statement to be somewhat redundant, given that HIPAA already requires a risk assessment and a proportional cybersecurity program based on a risk assessment. Perhaps the language could be revised to say "Hospitals are expected to follow the HIPAA requirements for a risk assessment and cybersecurity plan based on that assessment, with reasonable and necessary actions"

- Section 405.46 (c) 3 also states that "The cybersecurity program shall be designed to perform the following core functions", Another requirement at (5) "Each hospital's cybersecurity program shall include written procedures, guidelines and standards designed to 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. All such procedures, guidelines and standards shall be annually reviewed, assessed, updated and attested as such by the chief information security officer (CISO) (or a qualified designee) of the hospital"

  We suggest that the rule include that an accreditation program could be used to review and assess the requirements, or even require it. DirectTrust's privacy and security accreditation programs or HITRUST assessments can be used to measure the adequacy and quality of an organization's privacy and security programs, and include criteria based on the recognized security practices as outlined in the NIST (National Institute of Standards and Technology) Cyber Security Framework[5]. Such independent assessments would assure NY State that a hospital's cybersecurity program is adequately protecting the organization and meeting industry accepted standards. By accepting industry-accepted accreditations it may thereby reduce burden on state resources who may be performing oversight and/or audit functions of entities required to abide by the rule. Additionally the state may consider a "safe harbor" allowance for hospitals that experience a breach yet have demonstrated full compliance via an approved independent assessment.

- Section 405.46(f) sets up requirements for testing and vulnerability assessments. *We note that this is a function that might best be handled by external , independent organizations that have experience in penetration testing and vulnerability. These types of organizations have experience as outside testers and would better serve the hospital than inside*

[5] NIST Cyber Security Framework https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

staff. We suggest the rule recommend or require that it be accomplished by such outside organizations. Guidance could be provided by the state to hospitals regarding best practice in vendor selection and minimum requirements of services to consider for support.

- In the section titled security personnel, the rule states "(2) Each hospital may utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this section."

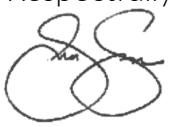
  Some of the biggest risks to cybersecurity in hospitals are from third party service providers and other connected platforms. Therefore, we suggest that the rule should require that a Third-Party Risk Management (TPRM) program be in place for all third-party vendors, not just those that assist in complying with these requirements. We also recommend that the hospitals implement their own Third-Party Risk Management (TPRM) to assure compliance with their own security risk management for those entities providing services for or on behalf of the hospital.

NY State should continue to be aware of the Federal (White House and HHS) push for cybersecurity and pursue state alignment to anything accomplished federally by any federal body, agency, or legislation. See referenced footnotes on page 1 as examples that may be considered to add as references within the rule.

As an additional comment, it appears that the $500 million in funding for hospitals is part of another grant program which encompasses other types of providers and other types of activities with applications due by Mar 6. This is before a final rule is published. We suggest that NY State look at the applications to determine the adequacy of the total funding and determine if additional funding may be necessary.

We appreciate the opportunity to comment on the proposed rule and stand ready to assist NY State in implementing the requirements.

Respectfully submitted,



Scott Stuewe
President and CEO, DirectTrust

