February
Five
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
REGSQNA@health.ny.gov

RE: Hospital Cybersecurity Requirements; I.D. No. HLT-49-23-0001-P

Dear Ms. Ceroalo:

On behalf of the 170 voluntary and public hospitals and health systems in New York State that make up the acute care membership of Greater New York Hospital Association (GNYHA), I appreciate this opportunity to respond to the Department of Health's (DOH) proposed hospital cybersecurity regulations. I would also like to thank our DOH colleagues for their responsiveness to our outreach on this proposal, including meeting with us, our members, and leadership representatives from the Federal Health Care and Public Health Sector Coordinating Council's Cybersecurity Working Group (HSCC CWG).

There is no doubt that there has been a significant uptick in cybersecurity incidents directed at health care organizations in recent years.[1] These attacks are mostly led by sophisticated bad actors located in hostile nation states. These incidents are not only costly to hospitals, they also have the potential to disrupt patient care operations. As a result, GNYHA members have invested a significant amount of time, money, and staff resources into cybersecurity preparedness and response. We understand that more can be done to stay ahead of the ever-evolving threats. We therefore welcome New York State's attention to this issue, especially Governor Hochul's recent announcement of a cybersecurity roundtable to ensure hospitals have "the implementation and operational support they need to strengthen their cybersecurity posture."[2]

That said, it is imperative that the State act in concert with the US Department of Health and Human Services (HHS) to achieve the unified goal of strengthening hospitals against cyber-attacks. *New York State should not operate in a vacuum when it comes to developing cybersecurity regulations for hospitals*. Working closely with HHS, the HSCC CWG has become the leading organization working on health care

[1] *See generally*, Hospital Cyber Resiliency Landscape Analysis, https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf (last accessed January 28, 2024).
[2] *See* 2024 State of the State, pgs. 117-8, https://www.governor.ny.gov/sites/default/files/2024-01/2024-SOTS-Book-Online.pdf (last accessed January 28, 2024).

cybersecurity and has done extensive work in this area since its formation in 2017, the result of a series of Federal executive orders and legislation.

As DOH learned in its recent discussion with HSCC CWG leadership—a meeting that GNYHA arranged—HHS has developed cybersecurity performance goals for the health care industry.[3] Among other things, HHS plans to incorporate these goals into the Medicare and Medicaid program payment rules.[4] HHS also announced that it will amend the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security rule to incorporate these goals this year.[5]

The HIPAA security rule and standards promulgated by the National Institute of Standards and Technology (NIST) form the backbone of hospital cybersecurity policy across the country. The HSCC CWG is the body that develops procedures and guidance to assist hospitals in implementing those standards.

DOH's proposed regulations neither acknowledge these existing standards and structures nor anticipate the changes that HHS has announced—even though DOH indicates that its intent is to "supplement" HIPAA.[6] This misalignment will force hospitals to invest in resources they cannot afford to comply with differing mandates.

As Governor Hochul also noted in her State of the State address, "hospitals in New York are struggling financially more than in the rest of the U.S—42% of hospital facilities in New York had an operating deficit in 2021." Based on our internal analysis of hospital cost reports, that figure rose to 63% in 2022, a year in which New York hospitals experienced a median operating margin of -2.5%.

While we appreciate the State's recent capital allocation of $500 million for technological investments, it cannot be used for most cybersecurity implementation needs. That funding is for capital investments, but what hospitals need to improve cybersecurity resiliency is software and their workforce, neither of which is eligible for funding under the existing program. Rather than forcing hospitals to expend scarce resources on new State standards just before the Federal government releases its new standards, which will be tied to Medicare reimbursement, DOH should defer action.

We request that DOH delay finalizing this rule until after HHS finalizes its changes to payment programs and the HIPAA security rule. DOH should use this time to convene the hospital cybersecurity roundtable to hear directly from stakeholders on how they are complying with existing standards and what they may need from the State to enhance those efforts now and in the future. Alternatively, if DOH chooses to finalize the rule before HHS acts, we request that certain

[3] *See* Healthcare and Public Health Cybersecurity Performance Goals, https://hphcyber.hhs.gov/performance-goals.html (last accessed January 28, 2024).

[4] *See* Healthcare Sector Cybersecurity; Introduction to the Strategy of the US Department of Health and Human Services, https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf (last accessed January 28, 2024).

[5] *See* Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 0945-AA22, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22 (last accessed January 28, 2024).

[6] *See* Addition of Section 405.46 to Title 10 NYCRR (Hospital Cybersecurity Requirements), pg. 21, (stating "[t]he [HIPAA] Security Rule does provide broad requirements for safeguarding PHI, but the regulations contained herein are intended to supplement HIPAA.")

requirements—set forth in our comments—be better aligned with HIPAA and other relevant standards, including as they are updated over time.

Thank you again for this opportunity. Our detailed comments are attached.

Sincerely,

Kenneth E. Raske
President

Detailed Comments

DOH should defer finalizing cybersecurity regulations until HHS acts.

While DOH has an important interest in understanding and overseeing hospitals' efforts in this regard, there is no need for DOH to reinvent the wheel in defining practices and creating mandates. The HSCC CWG has created extensive resources and guidance documents for hospitals to use in buttressing their cybersecurity preparedness.

In 2018, the HSCC CWG developed the Healthcare Industry Cybersecurity Practices (HICP) document, utilizing the expertise of industry leaders, security experts, government officials (including a few state governments), and others.[7] HICP is organized by the top five cyber threats affecting the health care industry and the top 10 mitigating practices for these threats. The mitigating practices incorporate relevant parts of the NIST the cybersecurity framework.[8]

As previously mentioned, HHS recently announced cybersecurity performance goals (CPGs) for the health care industry.[9] For each goal, HHS cites specific HICP and NIST standards that can be used to meet the goal. Like the NIST framework, HICP is a living document that changes as threats and best practices evolve. For example, HICP was amended in 2023 to include "social engineering" as a top five threat. As HHS moves forward with its plan, including imposing mandates within the Medicare payment rules, our members will be aligning much of their cybersecurity activity to comply with these CPGs.

DOH should not supplant these efforts, which have been underway and evolving over many years. Instead, DOH should wait for HHS to complete its work before proceeding with its own regulations. DOH should use this time to convene the hospital cybersecurity roundtable to learn more about what hospitals are already doing in cyber preparedness, their challenges, and how those efforts and challenges will play out as the CPGs become required. DOH can develop future rulemaking, as necessary, to fill in any gaps.

DOH is in perfect position to determine, on behalf of the State, the additional support and resources hospitals need (and will need going forward). This more reasoned approach will result in a better-informed, more targeted set of regulations that truly will "supplement HIPAA."

[7] *See* Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, https://405d.hhs.gov/Documents/HICP-Main-508.pdf (last accessed January 28, 2024).
[8] *See* Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations, https://405d.hhs.gov/Documents/tech-vol1-508.pdf & Technical Volume 2: Cybersecurity Practices for Medium and Large Organizations, https://405d.hhs.gov/Documents/tech-vol2-508.pdf (last accessed January 28, 2024).
[9] *See* HHS Releases New Voluntary Performance Goals to Enhance Cybersecurity Across the Health Sector and Gateway for Cybersecurity Resources, https://aspr.hhs.gov/newsroom/Pages/HHS-Releases-CPGs-and-Gateway-Website-Jan2024.aspx (last accessed January 28, 2024).

In the alternative, DOH should finalize regulations that are better aligned with existing standards.

If DOH moves forward with finalizing cybersecurity regulations, we request the below revisions. We also request that DOH include language that states compliance with its regulations will create a presumption that a hospital has met the standard of care with respect to health data security. In addition, we urge DOH to extend the compliance period from one year from the effective date to two years, given the extensive work that will be necessary to achieve compliance.

Rescind definitions of nonpublic information and information systems and align with analogous HIPAA definitions.

The key, foundational difference between DOH's proposal and existing standards is the definition of the information to which the regulations apply. DOH's proposal requires that hospitals protect "nonpublic information," which is generally defined as 1) a hospital's "business-related information, the tampering with which, or authorized disclosure, access or use of which, would cause a material adverse impact to the business, operations, or security of the hospital"; 2) personally identifiable information (PII); and 3) protected health information (PHI). New York hospitals are already protecting PII and PHI by virtue of being subject to New York State's General Business Law (GBL) and HIPAA.[10] PHI and PII are similar in that they are defined as individually identifiable information (i.e., information about a natural person, which is a workable concept).

"Business-related information," on the other hand, is a vague term disconnected from whether the data are individually identifiable, and thus much less workable. DOH does not give any examples to guide regulated entities. The vagueness and expansiveness of the term would create significantly more work and expense across the board, while the ambiguity of the definition will give rise to multiple interpretations among hospitals, perhaps increasing cyber risk in the field. By virtue of the expansiveness of nonpublic information and another key term, "information systems," the cybersecurity regulations could now apply to information from the entirety of hospital operations, including areas that are well outside the regulatory expertise of DOH, such as HVAC systems.

"Information systems" is similarly misaligned; HIPAA defines information systems as "an interconnected set of information resources, which are under the same direct management and control and share common functionality."[11] DOH's proposed regulations defines information systems as "a discrete set of electronic information resources organized for the collection, processing, storage, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." Unlike in HIPAA, there is no reference to management, control, and functionality. Furthermore, because the specialized systems listed by DOH do not typically contain

[10] This is despite DOH's statement that "[c]urrently in New York State there are no cybersecurity requirements for the safeguarding and security of patients' [PHI] and [PII]". *See* DOH's proposal, pg. 18.
[11] *See* 45 CFR §164.304.

individually identifiable information, the information in those systems is protected differently from systems that do. Hospitals protect these systems in other ways, such as against physical security threats.

It is unclear why DOH included these new and expansive definitions. We understand one consideration may be that non-PHI systems could be access points for cyber threats. It is reasonable for DOH to want hospitals to secure all possible access points. However, we encourage DOH not to manage this risk by vastly expanding the scope of its cyber regulations but to instead defer to the NIST cybersecurity framework and HICP practices for identifying and securing access points, depending, among other things, on data classification.[12] This is one of many topics that could be explored effectively in the hospital cybersecurity roundtable.

The expansiveness of these definitions renders other provisions in DOH's proposal unduly burdensome. First, an assessment of each system's data would need to be done (and redone regularly) to determine if it meets the definition of business-related information (i.e., whether its compromise would cause a "material adverse impact to the business, operation or security" of the hospital). Given the challenge of making such an assessment data set by data set and system by system, many hospitals would understandably want to opt for an all-inclusive approach for the sake of ease.

However, such an approach would be anything but easy longer-term: Multi-factor authentication would now apply to multiple systems, not just those containing PHI; security measures and controls, including encryption, would have to be deployed throughout a hospital's various systems; testing and vulnerability assessments would apply far more broadly than they do now; many more types of information would be subject to secure disposal; and implementation of policies, procedures, and controls to monitor the activity of authorized users and detect unauthorized access or use of, tampering with, nonpublic information by authorized users would become a much more onerous task.[13] Additionally, the requirements for risk assessments and third-party service providers, two areas that are challenging enough to manage under HIPAA, which applies only to PHI, would be magnified to an extreme, increasing the length of time it takes to do a risk assessment and greatly increasing the number of third-party vendors who must be vetted and overseen for security compliance. The provisions related to risk assessments and third-party service providers are problematic for other reasons as well, as noted below.

Once we catalogue all the additional work that these regulations would generate by virtue of their greatly increased scope, the financial implications become quite clear. Almost none of the above activities could be financed through last year's capital funding project. It is software and people, not hardware, that would be needed in most instances. For most hospitals, especially our distressed safety nets, the resources are simply not there.

This unworkable approach, borne out of a well-intentioned but not well-considered decision to go way beyond the scope of the HIPAA regulations, will result in unnecessary expenditures of time, resources, and

[12] *See e.g.*, HICP Cybersecurity Practice #4 on Data Protection and Loss Prevention.

[13] This last requirement could be read in such a manner that hospitals would be required to implement additional security measures on their community-based organization partners, who sometimes have access to scaled down instances of the hospital's electronic health record system. This would certainly have a chilling effect on the community work that our hospitals do with some of these organizations.

money, which take away from the goal of strengthening the industry's cybersecurity posture. It is also out of sync with NIST and HICP standards, which guide that not every type of data needs the same type of protection.

If DOH finalizes the proposed regulations, we request that DOH narrow the definitions of nonpublic information and information systems to align with HIPAA and the GBL, which focus on individually identifiable information. If DOH wants to address cyberattacks on other systems that contain information that is not individually identified, we urge DOH to defer to existing standards under NIST for classifying data and identifying and securing access points.

Align the risk assessment and third-party service provider requirements with existing standards.

While the definitions of nonpublic information and information systems render the several provisions outlined above unworkable, two provisions—the proposed risk assessment and third-party service provider requirements—are problematic in their own right.

It is instructive to note that HIPAA foregoes a hard timeframe for risk assessments and instead requires them to be done "on a periodic basis." [14] Doing a thorough risk assessment takes significant time and resources. GNYHA's health system members report that it takes several months to conduct a risk assessment in accordance with the HIPAA security rule. It then requires time and commitment to act on the findings, including addressing and remediating issues to manage risk. In addition to the difficulty of applying the risk assessment to all "nonpublic information" as opposed to just PHI, having to do so annually will result in hospitals checking compliance boxes rather than engaging in meaningful assessment, analysis, and follow-up. **The risk assessment requirement should therefore be aligned with the analogous provisions under HIPAA and be required on a periodic, rather than annual, basis.**

The proposed rule also requires hospitals to ensure the security of information systems and nonpublic information that are accessible to, or held by, a third-party service provider. DOH seeks to impose requirements for how hospitals conduct due diligence of such third parties, dictating review of various policies and procedures and mandating representations and warranties. The specificity of these requirements goes beyond HIPAA's current dictates and deny hospitals the flexibility they need in interacting with service providers.

Furthermore, this proposal is impractical. All GNYHA members report having difficulty getting some third-party vendors to agree to security assessments and certain other requirements. Larger systems and hospitals may have somewhat more leverage with certain third parties, but even they struggle to persuade the large vendors they do business with to cooperate with certain requests (e.g., Zoom and Google reportedly refuse to sign business associate agreements in many instances) And for our growing number of distressed safety net hospitals and systems, sourcing and maintaining relationships with vendors that are willing to do

[14] See HHS' Guidance on Risk Analysis, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html) (explaining "The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities.")

business with them is hard enough without imposing additional compliance burdens. They have no choice but to work with certain vendors, and there is no negotiating ability. The HIPAA requirements for business associates and the NIST/HICP practices for managing third-party risk, while difficult to implement, are somewhat more workable than the DOH proposal.[15] **We urge DOH to align these requirements with these existing standards. We also request that DOH allow a hospital's "good faith effort" to impose and oversee certain security controls with third-party service providers to satisfy the requirement.**

Revert to notification requirements agreed on with industry stakeholders.

In 2019, DOH worked with GNYHA and other associations to develop a cyber incident reporting standard that was workable for our members and met DOH's mission to protect, improve, and promote the health of New Yorkers. The consensus was for a 24-hour notification requirement of a cybersecurity incident, which was generally defined as any cybersecurity event that affects patient care or represents a serious threat to patient safety.[16]

DOH now proposes to change this to a two-hour notification of "any cybersecurity event that has a material adverse impact, has a reasonable likelihood of materially harming normal operations; or results in the deployment of ransomware within a material part of the hospital's information systems"[17] It is unclear why DOH feels the need to change the 24-hour standard or the substance of the standard. If there is a concern about individual incidents not being reported in a timely fashion, DOH certainly has the authority to address that on an individual level. As far as we are aware, the 24-hour standard has worked well, with hospitals and DOH maintaining timely lines of communication as needed in managing cyber incidents. We understand that DOH, in its desire to receive notification in time to act, has concerns about the extent to which hospitals connect with DOH networks. It is not clear from our conversations with DOH, however, that there has been a thorough analysis of this theoretical risk.

According to our members, a two-hour standard would be wholly unworkable.

During the first hours of a cybersecurity incident, hospital personnel must work hard to characterize the incident. Various members of interdisciplinary teams carry out tasks to investigate and determine the potential impact on operations. There would be no way to know, in two hours, whether the DOH standard was met, even if the term "material" was defined.

GNYHA members also share information, outside of legal and regulatory requirements, where it aids in response and recovery. For example, if it appears there may be criminal aspects to the incident, our members may call the US Federal Bureau of Investigation (FBI), which has an established cyber command center. In some cases, the FBI can provide encryption keys for ransomware incidents, which could be critical in recovering quickly. Our members may also share information with intelligence sharing and analysis centers (ISAC), which will then share the threat information–-in a deidentified format—with other ISAC members. Finally, our members make notifications to their vendors and other partners if it appears the cyber incident

[15] *See e.g.*, supply chain and third-party risk management practices in NIST 800-53.
[16] DOH announced this requirement on October 18, 2019 via DAL #19-01.
[17] We also note that DOH uses the term "covered entity" in defining cyber incident, which is not defined in the proposed regulation.

may affect their systems. All of this happens simultaneously with moving staff to “downtime” procedures, caring for patients, and maintaining continuity of operations.

We request that DOH keep the current 24-hour notification requirement for cyber incidents affecting patient care and safety. If DOH is determined to tighten this requirement, it could require notification sooner—but no later than 24 hours—if a hospital or health system knows there are patient care or safety issues, or that any DOH information systems may be affected.

Remove the cybersecurity-specific incident response plan requirement.

GNYHA members are already required to perform a hazard vulnerability assessment (HVA) on a biennial basis as a condition of participation in Medicare. [18] This involves evaluating hazards that threaten the hospital’s ability to continue operations and deliver patient care, including cyber disruptions. A hospital’s HVA drives their priorities for emergency preparedness and directly influences their emergency operations plans (EOP), which is an “all hazards” playbook for hospitals to continue operations during any disaster. The Centers for Medicare & Medicaid Services (CMS) and The Joint Commission (TJC) require that EOPs contain plans for maintaining communication mechanisms and operations in general, in addition to maintaining continuity of operations plans that include procedures for maintaining medical documentation. Hospitals are required to evaluate and test EOPs on a regular basis.

Our members go above and beyond these requirements. They have taken additional steps, including providing staff-level education on downtime procedures, conducting exercises with operational leaders, and testing plans with executive leadership. GNYHA is a regular convener and participant in such exercises, some of which have included several hospitals within a region since a cyber-attack on one can affect others.

DOH’s proposal here is similar but not identical to CMS regulation and TJC standards. As written, the DOH requirement would mandate the development of a separate and distinct plan for cyber disruptions. This runs contrary to how incident response plans should be developed and implemented, which is in a unified all hazards manner regardless of the type of incident. Maintaining a separate and distinct incident response plan for cyber disruptions will lead to confusion among the staff about which plan to follow during the actual response. This will only hinder the continuity of operations, perhaps including patient care. **We request that DOH remove the requirement for a cyber-specific incident response plan. If DOH wants to address incident response in some way, we request that it align with the CMS and TJC requirements, using an all hazards approach.**

Clarify there is no requirement to maintain all log data.

Under HIPAA, hospitals are required to retain records pertaining to systems design, security, and maintenance for six years. DOH reiterates this requirement but also requires hospitals to maintain, for six years, the records of systems that include “audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the

[18] *See* 42 CFR 482.15(a)(1), (2), & (3), (c)(3)(i); see also The Joint Commission Emergency Management Standard EM 12.01.01 & 13.01.01

hospital and of cybersecurity incidents defined herein." This requirement could be read as requiring hospitals to maintain log data of all security incidents.

If that is DOH's intent, this is a significant deviation from HIPAA and an incredibly costly demand that only increases with hospital size. One GNYHA member estimated that this requirement, assuming it applies to log data, would cost them almost $600,000 a year. Another large health system member estimated that this requirement would cost them between $24-48 million a year. The variation in this estimate is partly due to the fact that their vendor, like most vendors in this space, does not offer the log data retention service for more than a few months, and therefore could not provide an estimate for what retention for several years would cost. DOH is well aware that hospital resources are limited. Requiring hospitals to spend large sums on record retention undercuts, not enhances, cybersecurity preparedness. **We request that DOH clarify that this requirement does not apply to log data but to the same matters as the HIPAA provision: systems design, security, and maintenance.**

Incorporate by reference existing standards.

The bulk of our above comments are concerned with DOH's choice not to align the proposed regulatory text with applicable HIPAA or NIST standards. However, in some places DOH has copied text from the HIPAA security rule and NIST standards, but without attribution and as those standards are currently written. One example of this is the proposed definition of multi-factor authentication (MFA.) While the definition currently aligns with NIST, it ignores the fact that NIST is working on version 2.0 of its framework and the definition may change. Not only does DOH's static structure raise security issues, but DOH will have to go through additional rulemaking to update the definition or leave a disconnect in place. Indeed, there is no way for *any* of DOH's mandates to change as threats or best practices evolve by operation of their own regulatory text. **To make New York's cybersecurity regulations align with its Federal counterparts and more responsive and flexible, we request that DOH incorporate by reference general citations to existing standards, in particular the HHS CPGs, NIST, and HICP, throughout these regulations.**

Allow health systems to meet regulatory requirements on behalf of their affiliated hospitals.

DOH's proposed rule applies to all Article 28-licensed general hospitals. The proposal uses the term "hospital" throughout. However, our health system members often share information technology infrastructure and services across their systems. These health systems take certain centralized steps and use unified controls to achieve compliance with existing rules, leveraging the economies of scale that are a feature of their operations. Most health systems have one chief information security officer (CISO) who functionally serves as the CISO for each hospital. It would be repetitive and expensive for each hospital facility in a health system to meet each requirement on their own, nor should we want hospitals to conduct cybersecurity activities in a vacuum when health system facilities are interconnected. **We request that DOH clarify that health systems may meet the regulatory requirements at the system level on behalf of each of their affiliated hospitals**.

Recognize that not all mandated activity falls under a cybersecurity program overseen by a CISO; provide flexibility in governing body reporting requirements.

DOH's proposed rule would require hospitals to establish a cybersecurity program in which, among other things, the CISO is tasked with reviewing, assessing, and updating the hospital's cybersecurity procedures, guidelines, and standards. In some cases, the CISO has an oversight role, such as approving whether a compensating control can be used in lieu of MFA. In some hospitals, however, the CISO serves in a "risk advisor" role, where their job is not to approve security practices, which are approved through other mechanisms.

Also, hospitals are fulfilling many of the proposed requirements to the extent required by existing standards. But some of this activity is not traditionally thought of as "cybersecurity" and thus does not fall under the leadership of the CISO, such as the secure disposal of information and determining how data is used and accessed. Hospitals have leaders in physical security, privacy, data analytics, software engineering, and other areas who are responsible for many of the activities required by this proposal, but those roles do not report to the CISO. Each of our members is organized differently. There should be some flexibility in allowing them to implement the requirements in the most effective and efficient manner based on their structure. **We request that DOH recognize that hospitals can meet the proposed requirements outside of a prescribed cybersecurity program overseen by a CISO.**

DOH's governing body requirements are likewise too prescriptive. The proposed rule requires the governing body to approve the hospital's cybersecurity policy. Governing bodies, however, are responsible for overseeing and advising on high-level issues, such as key risks and investment decisions. While some key risks may be cybersecurity related, the governing body is certainly not responsible for operational activities such as approving policies. A better approach, more consistent with governance best practices, would be for the governing body to receive a report on the hospital's cybersecurity program on a regular basis.

While DOH's proposed rule does contain such a requirement, it is once again too prescriptive and risks chilling innovation and flexibility. DOH tasks the CISO with making an annual written report to the board on the cybersecurity program, but the reporting requirements include certain elements, such as reporting on any cybersecurity incidents and steps taken to mitigate future incidents. Also, it is not always the CISO who makes reports to the board on cybersecurity activity; it can sometimes be the chief technology officer, data privacy officer, or other leadership roles. Especially given the breadth of the proposed rules, hospitals should be permitted to satisfy their governance obligations through reports by whomever is in the best position to advise the board and respond to the board's questions. **We request that DOH revise the proposed regulations to require hospitals to make regular reports to their governing body on cybersecurity issues that the governing body and hospital leadership together determine are appropriate for such reporting, and to leave the question of who provides such reports to hospital discretion.**

Conclusion

It is crucial that DOH work in lockstep with HHS on this important issue. Any misalignment will result in unintended consequences—including potentially increasing our collective cyber risk—and significant costs to the health care system, which we cannot afford. We strongly urge DOH to wait for HHS to complete their work before acting on State regulations.