Charles N. Kahn III
President and CEO

May 9, 2022

**Via electronic submission at** *https://www.sec.gov/rules/submitcomments.htm*

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

**Re: S7-09-22 SEC: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure**

Dear Secretary Countryman:

The Federation of American Hospitals (FAH) is the national representative of more than 1,000 leading tax-paying public and privately held hospitals and health systems throughout the United States. FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across 46 states, plus Washington, DC and Puerto Rico. Our members include teaching, acute, inpatient rehabilitation, behavioral health, and long-term care hospitals and provide a wide range of inpatient, ambulatory, post-acute, emergency, children's and cancer services.

We appreciate the opportunity to provide the Securities and Exchange Commission (Commission) with our views in response to the *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* proposed rule, 87 Fed. Reg. 16,590 (March 23, 2022) (Proposed Rule). The FAH agrees broadly with the comments to the Proposed Rule submitted by the U.S. Chamber of Commerce (Chamber). The FAH comments emphasize certain of the Chamber's comments and are based on our members' experience serving patients and maintaining critical health care infrastructure. Hospitals and health systems have significant experience in navigating the cybersecurity of such information systems, requiring both expedient and thoughtful assessment and response to cyber threats, as well as allocation of limited resources. Thus, discretion and consistency with existing regulatory frameworks are key elements to be considered within the Proposed Rule. Our registrant members greatly value transparency to guide investors' practical decision-making; however, a perceived enhancement of such transparency via the Proposed Rule cannot come at the cost of safety and security to

patients and vital health care infrastructure, as well as national security. For the reasons set forth below, the FAH believes the Commission's 2018 interpretive guidance provides adequate cybersecurity reporting obligations for our registrant members, including the appropriate provision of information to investors, and urges the Commission to further collaborate with cybersecurity industry participants and other federal agencies with regard to the continued rulemaking process.

## Reporting Material Cybersecurity Incidents

The Proposed Rule proposes an amendment to Form 8-K to add Item 1.05 to require a public company to disclose information about a cybersecurity incident within four business days after the company determines that it has experienced a "material" cybersecurity incident, including information describing (i) when the incident was discovered and whether it is ongoing, (ii) the nature and scope of the incident, (iii) whether any data was stolen, altered, accessed, or used for any other unauthorized purpose, (iv) the effect of the incident on the company's operations, and (v) whether the company has remediated or is currently remediating the incident. The Commission has set forth a belief that the disclosure of such information within four business days of a materiality determination "would significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures."[1] The FAH has strong concerns with both the timing and required content of such disclosures, including what the Commission deems standardized and comparable information in the cybersecurity context with regard to the determination of materiality, an organization's ability to monitor third parties, unintended effects on patient safety, and coordination with existing state and federal law.

### *Triggering Determination*

Cybersecurity disclosures are of a conceptually different nature than many other types of disclosures required by the Commission. In considering whether disclosure should be triggered upon discovery or upon a determination of a material incident, the FAH appreciates the Commission's recognition that disclosure based on a materiality determination is the more practical trigger; however, materiality in the cybersecurity context can be more subjective than the principle of materiality to a shareholder's "total mix" of information otherwise prevalent throughout federal securities law. When considering the impact of a cybersecurity incident, a company may, in some instances, be able to quickly determine that an incident may have a material effect from a regulatory perspective, but unlike other more bright-line material disclosures affecting an investor's total mix of information (e.g., the resignation of company executives or disclosure of litigation), the determination of whether a cybersecurity incident may be material could take an extended period of time as the assessment of overall impact usually takes place during and sometimes well after the incident is remediated. As a result, in complying with the Proposed Rule, registrants could have to decide whether to disclose a cybersecurity event without the benefit of having any available information with which investors may use to make informed decisions.

[1] 87 Fed. Reg 16,595 (Mar. 23, 2022).

It is unlikely that a company, despite potential ability to identify an incident as material, would simultaneously have adequate material information to disclose to investors, such as the nature and magnitude of the incident, financial impact, or anticipated vulnerabilities or regulatory consequences. For this reason, it also will be impractical for a company to retrospectively consider any immaterial incidents to determine if they are material in the aggregate on an ongoing basis. Likewise, it is impractical for a company to continually reassess its prior determination that an incident was immaterial. The proposed requirement to continually reassess prior incidents or disclose incidents that become material in the aggregate imposes an undue burden on companies that have appropriately handled incidents as they arise to continually reconsider their prior determinations regarding any individual incident – resources with which FAH registrant members may better serve their investors and patients through efficient and quality patient care.

Our registrant members appreciate and work to follow the Commission's 2011 and 2018 interpretive guidance concerning reporting of cyber incidents under existing regulation. Compared to this existing guidance, the Commission now contends that the Proposed Rule will allow more comparable disclosures for consideration by investors than current disclosure practices. To the extent the Commission or investors perceive a disparity of disclosure, they observe the disparity inherent in cybersecurity incidents. Incidents may vary greatly in nature, scope, and magnitude of individuals impacted – imposing a four-day reporting window will not actualize information for companies they are not yet in a position to have, particularly if an incident is ongoing. The inclusion of requested line items for investor comparison will not cause companies to possess information to disclose for such items even with a company's diligent efforts. Therefore, although the FAH agrees with the spirit of desiring easier comparison for investors, premature disclosures in the cybersecurity space may actually detract from the effectiveness of the disclosure requirement by providing an excess of inconsequential information. In addition, such premature disclosures are likely to cause more confusing and disparate information, not less, due to the lack of visibility companies themselves may have within the short reporting window.

***Relationship with Vendors***

In reference to a company's disclosure obligations, the Commission proposes to define the term "cybersecurity incident" as an "unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."[2] It further defines "information systems" as "information resources, owned *or used* by the registrant..." (emphasis added).[3] Our members utilize third-party vendors, such as electronic medical record and similar service providers, relevant to their daily operations. These registrant members generally have less visibility into the security status of these third parties than their internal systems, further confusing any potential materiality determination under the Proposed Rule. Our registrant members cannot always discern when an incident may have occurred or is still in process on information systems used, but not owned, by the respective organization. Any ability to make a

[2] 87 Fed. Reg. 16,601 (Mar. 23, 2022).

[3] Id.

materiality determination regarding a cybersecurity incident on information systems owned by a third party will depend on what the system owner is contractually required to disclose and the required timeframes associated with that disclosure. Although, depending on the nature of the services provided, FAH members may have agreements with third-party system owners requiring upstream reporting of cybersecurity incidents, the timing and nature of such reporting is designed to comply with existing regulatory requirements and may not align with the disclosure timing imposed by the Proposed Rule. Even if there were such alignment, third-party vendors may have varying views of what constitutes a material reportable incident.

Further, the vast majority of our registrant members' vendors are not registrants themselves who would be subject to the Proposed Rule; consequently, under the Proposed Rule, our members may experience insufficient vendor reporting under existing agreements, as vendors would likely be reluctant to disclose information to our registrant members who would then be obligated to publicly disclose details of incidents such vendors may or may not otherwise be obligated to disclose to state or federal authorities, or the public at large. A registrant may find it particularly difficult to obtain this information from a privately held information systems provider, whose resources may be stretched thin as it responds to an incident, potentially resulting in misinformation to the registrant and ultimately to the investors. This potential lack of transparency between hospitals and health systems and their vendors may result in inadequate information on which our members otherwise rely to provide patient care.

***Effect on Patient Care***

Of particular concern to our members is the Commission's proposed four-business-day reporting window, requiring disclosure of details of an organization's cybersecurity incident regardless of whether such incidents remain ongoing or have yet to be remediated. As written, an organization would be required to disclose a potentially active cybersecurity incident, which may be unduly burdensome to an organization's limited resources while it works to address the active incident and may adversely impact the outcome of the remediation effort. In addition to the lack of visibility inherent in disclosures under the proposed reporting window, disclosure of ongoing incidents that have not yet been remediated discloses an organization's active vulnerability that may be further taken advantage of by bad actors. Such actors will be told, in real time, that their actions are having a material effect, emboldening them to continue their attack or deploy the same techniques on a secondary target. This risk is too great and significantly undermines the intended goals of such disclosure.

The proposed disclosure of a health system's active vulnerability may adversely impact its ability to fully focus on quickly restoring critical systems that have a direct impact on providing care to patients. A cybersecurity incident in the hospital or health system context may involve sensitive patient health information. In the event of an incident, our members need the ability to preserve flexibility and resources to protect and mitigate risk to such sensitive information and cannot provide the level of detail required by the Proposed Rule regarding incidents that have not yet been remediated at the risk of placing their patients' information in greater vulnerability.

### *Alignment with Existing State and Federal Law*

While the FAH appreciates the Commission's desire to provide greater transparency to investors, we urge the Commission to consider that its Proposed Rule does not exist in a vacuum. Cybersecurity incidents, including breach notification requirements, are already the focus of both federal regulatory oversight and state law. Although the Commission has recognized in the Proposed Rule that organizations are subject to other reporting requirements and exceptions, it asserts that "there is a possibility a registrant would be required to disclose [an] incident on Form 8-K even though it could delay incident reporting under a particular state law" under the belief that "[i]t is critical to investor protection and well-functioning, orderly, and efficient markets that investors promptly receive information regarding material cybersecurity incidents."[4]

This presumption diminishes the value of critical infrastructure both at the federal and state levels and ignores the interagency cooperation that exists in the evolving cyber environment. In addition to other federal laws, HIPAA has its own incident reporting requirements and definitions, including materiality thresholds for disclosures to government authorities, individuals, and media agencies. Other federal agencies, as well as state law enforcement have certain authority to investigate cybersecurity incidents and pursue the bad actors involved. As such, HIPAA and certain other state and federal laws allow a covered entity to delay reporting an incident if the entity is working with law enforcement to investigate the cybersecurity incident. Requiring registrants to report a cybersecurity incident under the Proposed Rule while an active law enforcement investigation is underway would conflict with the intent of HIPAA's reporting delay and may adversely affect law enforcement's investigation of a cybersecurity incident and apprehension of the responsible bad actors. Although the FAH believes in the value of informed investors to an efficient market, we question whether the proposed reporting requirements should be preeminent to the rights of individuals whose information is actually affected by an incident or the pursuit of protecting organizations and individuals locally and nationwide via investigation of the perpetrators of an incident. Any rulemaking by the Commission should allow registrants to delay reporting a cybersecurity incident in line with HIPAA and other applicable state and federal law, or where requested by the Attorney General, in order to balance the need for timely disclosure with the pursuit and prosecution of malicious actors.

## **Management, Strategy, and Governance Information to be Disclosed**

### *Value of the Information Disclosed*

Under the Proposed Rule, the Commission would amend Form 10-K to require disclosure of (i) a registrant's policies and procedures, if any, for identifying and managing cybersecurity risks, (ii) a registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks, and (iii) management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies, as well as propose Items 106(b) and (c) and 407 of Regulation S-K, requiring disclosure of whether an organization has certain types of policies, procedures, and governance concerning cybersecurity risks. The Proposed Rule asserts the Commission's view that a

[4] 87 Fed. Reg. 16,597 (Mar. 23, 2022).

company's disclosures concerning its cybersecurity risk management, strategy and governance practices "would allow investors to...evaluate a registrant's risk management and governance practices regarding those risks, and better inform their investment and voting decisions" and that such disclosures can "improve an investor's understanding of the registrant's cybersecurity risk profile."[5]

FAH registrant members are concerned about, and committed to, protecting their information systems and digital assets from cybersecurity threats, as well as providing investors a clear understanding of that commitment from a risk management and governance perspective. However, the required risk management and strategy disclosures should balance improving an investor's understanding of an organization's risk profile with the risk of a bad actor's understanding of the same risk profile. The proposed requirements for an organization to disclose specific policy types and describe its programs for risk assessment and incident detection may provide a road map for bad actors to easily accessible information on potential targets and the general means by which its malicious actions may go undetected or otherwise cause the most damage. Even where an organization is not required to disclose specific security controls, the existence or absence of certain risk management procedures or governance may allow bad actors a basis on which to target a particular organization. Such misinformed assumptions by malicious actors could make a specific organization more vulnerable to attacks. Therefore, the Commission should alternatively consider requiring that such disclosures provide the registrant company's overall framework for cybersecurity risk management and governance, without providing unnecessary detail of specific policies and procedures or composition of the company's cybersecurity risk management team.

The Commission contends that research has not suggested evidence that detailed cybersecurity risk disclosures lead to more attacks, recognizing, however, that the Proposed Rule would require more detailed disclosures than the current rules such that the referenced research is not generally applicable to the proposed reporting requirements. Although the Commission may be comfortable that it has no reason to believe more disclosure may lead to more risk, the FAH is concerned with the absence of evidence under the current rules as a basis on which to assume the safety of more detailed disclosures under the Proposed Rule.

***Disproportionate Representation of Public Health Systems***

In addition to the potential harm for all organizations required to disclose sensitive information regarding their risk management procedures and governance, our registrant members in particular may face disproportionate attention in the health care industry. Our registrant members as compared to their privately held counterparts, will be required to disclose particulars of their cybersecurity policies and procedures, providing additional emphasis on such registrants as targets for a bad actor looking to infiltrate a health system. This disparity may discourage privately held health systems considering registration, thereby reducing optionality for investors seeking to direct resources within the healthcare industry.

[5] 87 Fed. Reg. 16,594, 16,599 (Mar. 23, 2022).

**Request for Alternative Structure for Hospitals and Health Systems**

Although the FAH believes the Commission's 2018 interpretive guidance provides adequate cybersecurity reporting to investors via disclosure obligations for our registrant members, in light of the points above, the FAH respectfully requests the Commission to consider the following in any further rulemaking activity related to cybersecurity:

- Engage in interagency coordination and ensure alignment with those federal agencies that are better suited to online defense, law enforcement, and national security;
- Carve out entities subject to compliance with HIPAA or other laws imposing similar reporting of cybersecurity incidents, or, in the alternative, provide greater particularity for determinations of "materiality," such as alignment with existing regulatory frameworks, including an entity's obligation to disclose certain incidents pursuant to HIPAA;
- Limit an organization's obligation to report a cybersecurity incident to one affecting systems owned by such organization, given the inability to control reporting of privately held vendors, as well as provide safe harbor protection for reporting cybersecurity events affecting resources that are used but not owned by the registrant;
- Tie the incident disclosure trigger to a reasonable number of days following remediation of a material event rather than only a determination of materiality in order to allow the organization to focus its resources on remediation and recovery efforts, protect the organization from further vulnerability, and allow appropriate time for all facts and circumstances impacting materiality to be identified;
- Align the ability to delay disclosure of incidents in circumstances allowed under existing state and federal law, so as not to impede investigation by appropriate supervisory authorities and law enforcement; and
- Reduce an organization's obligation to disclose particulars of its cybersecurity risk management strategy and governance in favor of a general description of risks and mitigation contemplated under the current rules, so as not to aid bad actors in targeting and attacking registrants on the basis of such disclosures.

**********

The FAH appreciates the Commission's dedication toward protecting investors and your consideration of our comments. We look forward to continued collaboration with the Commission to implement effective policies that assist the health care industry in meeting the challenges of the evolving cyber landscape. If you have any questions, please contact me at [redacted], or any member of my staff at [redacted].

Sincerely,