May 5, 2022

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street, N.W.
Washington, D.C. 20549

RE: "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" Proposed Rule (File No. S7-09-22)

Dear Chair Gensler:

The Confidentiality Coalition appreciates the opportunity to provide comments on the proposed rule on, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective patient privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Cybersecurity incidents are a significant challenge to companies. From 2020 to 2021, publicly traded companies reported a 118% increase in unauthorized access incidents and a 44% increase in ransomware attacks.[1] These attacks can be harmful to companies in terms of financial cost[2] and the unauthorized release of sensitive information. Healthcare companies are particularly at risk of cybersecurity incidents. In 2021, over 45 million individuals were impacted

[1] Chris Gaetano, *Cybersecurity incidents soar at public companies*, Accounting Today (April 6, 2022), https://www.accountingtoday.com/news/cybersecurity-incidents-soar-at-public-companies-says-audit-analytics-report.
[2] Heather Landi, *Average cost of healthcare data breach rises to $7.1M, according to IBM report*, Fierce Healthcare (July 29, 2020), https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report.

by cyberattacks on healthcare entities, a record amount,[3] and of the 16 sectors categorized as "critical infrastructure," healthcare companies reported the most ransomware attacks.[4]

While the Confidentiality Coalition supports steps to increase awareness around cybersecurity incidents, we are concerned that the proposed disclosure framework would be overly burdensome to publicly traded companies without advancing the Security and Exchange Commission's (SEC) goal of transparency regarding cybersecurity incidents. Indeed, disclosing the impact of cyberattacks is appropriate to ensure public trust, but requiring all potential breaches to be reported within 96 hours of discovery would, among other things, increase the likelihood of misreporting, market volatility, civil liability, and risk to reputation.

The healthcare industry already has extensive health data breach reporting requirements as part of compliance with the Health Insurance Portability and Accountability Act's (HIPAA) Privacy and Security rules as well as the Federal Trade Commission's (FTC) Breach Reporting Rule. Further, the Cybersecurity and Infrastructure Security Agency (CISA) is expected to begin rulemaking on reporting of cyber breaches affecting critical infrastructure, which includes healthcare. We encourage the SEC to recognize the adequacy of these existing requirements and work with the healthcare industry to avoid duplicative reporting and instead focus on collaboration, education and support, rather than punitive action.

Notably, HIPAA's reporting requirements contain a clear definition of "breach" and a four-factor analysis to determine when an incident must be reported to the Health and Human Services (HHS) Office for Civil Rights (OCR). These requirements balance the need for timely notice while recognizing a thorough and accurate investigation takes time. Here, the proposed rule does not provide a comparable timeframe to complete an investigation before requiring public notification. Consequently, information disclosed in a report released to the SEC within 96 hours of discovery is more likely to be inaccurate or incomplete, which could lead to misreporting by the media and result in confusion among individuals, investors, customers, industry partners, law enforcement, and regulatory agencies.

Further, HIPAA allows for a reporting delay if a law enforcement official indicates that a notification, notice, or posting required under HIPAA would impede a criminal investigation or result in harm to national security. Here, the proposed rule fails to provide any reporting delay when there is an ongoing investigation of a cybersecurity incident. Failing to recognize a delay for notification by law enforcement will undermine HIPAA, and increase risk to the registrant, the overall healthcare industry, impacted individuals, state and/or federal investigations, and national security. As proposed, the rule will increase the likelihood of misreporting by the media, as a 96-hour disclosure requirement will require entities to publish incomplete or possibly inaccurate information. This will in turn increase market volatility, impede a full investigation, and increase the risk of civil liability. In addition to federal requirements, currently 21 states have a state cybersecurity breach law, the majority of which require reporting within three business days of discovery; however, this is limited to the information available at the time of reporting.

We recognize the need to provide greater transparency around cybersecurity incidents but are concerned that the proposal to disclose these events on Form 8-K would be unduly burdensome

---

[3] Heather Landi, *Healthcare data breaches hit all-time high in 2021, impacting 45M people*, Fierce Healthcare (February 1, 2022), https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people.

[4] *Internet Crime Report 2021*, Federal Bureau of Investigation Internet Crime Complaint Center (March 23, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

and provide little useful information for the SEC when examining these events. The Confidentiality Coalition encourages the SEC to recognize that cyber breaches require companies to quickly respond to a significant event and to work with impacted entities in ensuring that reporting is focused on assistance and education rather than punitive action. Additionally, the Cybersecurity and Information Security Agency (CISA) is preparing regulatory action to mandate cyber breach reporting. We encourage the SEC to work with CISA to ensure that the proposed rule is not unnecessarily duplicative.

The Confidentiality Coalition looks forward to working with the SEC on further steps to improve cybersecurity readiness. Included is a copy of the Confidentiality Coalition's principles on cyber incident reporting. Please contact me at tgrande@hlc.org or 202-449-3433 with any questions.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council