



December 1, 2022

The Honorable Mark Warner  
U.S. Senate  
Washington, D.C. 20510

**RE: Cybersecurity is Patient Safety Policy Paper Comments**

Dear Senator Warner:

The Confidentiality Coalition appreciates the opportunity to provide comments on your policy paper on, "Cybersecurity is Patient Safety: Policy Options in the Health Care Sector."

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 health information 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 for healthcare stakeholders. In 2021, over 45 million individuals were impacted by cyberattacks on healthcare entities, a record number.<sup>1</sup> Of the 16 sectors categorized as "critical infrastructure," healthcare companies reported the greatest number of ransomware attacks in 2021.<sup>2</sup> These attacks are not only harmful to organizations in terms of financial cost<sup>3</sup> and the unauthorized release of sensitive information but can disrupt operations and put the health and safety of patients in jeopardy. As Congress considers further steps to improve cybersecurity readiness, we encourage you to consider the following proposals:

---

<sup>1</sup> 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>.

<sup>2</sup> 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](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

<sup>3</sup> John Hewitt Jones, Treasury seeks industry input on cyber insurance market support measures, FedScoop (October 11, 2022), <https://www.fedscoop.com/treasury-seeks-input-on-cyber-insurance-market-support-measures/>.

## **Improving Federal Leadership and Our National Risk Posture**

Improving cyber protections is a priority for all public and private stakeholders. As Congress considers further legislation, we emphasize the need to streamline cooperation across federal agencies to reduce unnecessary or duplicative reporting requirements. The Cybersecurity and Infrastructure Security Agency (CISA) is currently beginning steps to implement provisions of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to require critical infrastructure to report breach incidents. We recognize the need to provide greater transparency around suspected cyber incidents but emphasize the need for CISA to work with other federal agencies that are currently engaging in reporting rulemaking or already have reporting requirements in place such as the Department of Health and Human Services (HHS).

The healthcare sector currently operates under a robust privacy and security framework created from the Health Insurance Portability and Accountability Act (HIPAA) and the subsequent Privacy and Security Rules. For over 20 years, these regulations have provided protections for certain healthcare information. However, as technology has advanced, significant amounts of healthcare data are now collected but not protected by the HIPAA framework. The Coalition encourages Congress to advance comprehensive privacy legislation that provides a framework to safeguard health information not covered by the HIPAA framework. We emphasize that any legislation recognizes how HIPAA functions and does not duplicate existing requirements. This would provide further safeguards preventing sensitive health data from being misused or accessed without authorization.

We thank the HHS Office of Inspector General (OIG) and the Centers for Medicare and Medicaid Services (CMS) for finalizing changes to the Anti-Kickback Statute and the Physician-Self Referral (Stark) Law to establish a safe harbor for donations of cybersecurity technology. This provision will allow smaller entities unable to afford sophisticated cybersecurity software the ability to properly safeguard patient data. In order to better leverage this exception, Congress should work with OIG and CMS to identify entities unable to take advantage of these arrangements and work to further support donations of these tools.

Additionally, the Coalition supports efforts to reexamine the HHS Breach Portal. In revisiting this provision, Congress should maintain consumer notifications of breaches, but should differentiate organizations that use appropriate security practices and were simply unfortunate victims of cyberattacks. The presence of a company on the public-facing breach reporting website undermines consumer confidence in specific healthcare organizations and the healthcare system as a whole. This penalty should be reserved for organizations that have not adequately protected their healthcare information – not those that took appropriate precautions but were overcome by major attacks that virtually no organization would have been able to stop. Similarly, HHS should develop a mechanism for healthcare organizations to remove their name from this list by demonstrating that they have resolved security issues and have implemented appropriate information security tools and protocols.

## **Improving Health Care Providers' Cybersecurity Capabilities Through Incentives and Requirements**

The Confidentiality Coalition thanks Congress and federal agencies for their continued support to strengthen cybersecurity protections for healthcare stakeholders. In particular, we appreciate the work to implement Public Law 116-321 that directs the Secretary of Health and Human Services to take recognized security practices into consideration when levying fines for violation of the HIPAA Security Rule. This past May, the HHS Office for Civil Rights (OCR) issued a

request for information on how to implement provisions of this law. We encourage Congress to work with OCR on how to provide clarity to stakeholders about what constitutes recognized security practices and provide further educational support for entities to improve their own security frameworks.

### **Recovery from Cyber Attacks**

We appreciate the report's findings that recognize cybersecurity incidents constitute an emergency event and should be treated with similar focus. In particular, the Coalition supports the recent proposal by the Federal Insurance Office (FIO) to categorize cyber incidents as catastrophic for the purposes of supporting a federal backstop for cybersecurity coverage. In 2021, a record 26,000 claims for cyber-related incidents were filed with insurers<sup>4</sup> and this number is expected to rise in coming years. We encourage Congress to work with federal agencies to provide clarity to impacted entities about the extent of insurance coverage and work to build trust in this process.

The Confidentiality Coalition looks forward to working with you on steps to improve cybersecurity for healthcare stakeholders. Please contact me at [tgrande@hlc.org](mailto:tgrande@hlc.org) or 202-449-3433 with any questions.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive, flowing style.

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

---

<sup>4</sup> John Hewitt Jones, Treasury seeks industry input on cyber insurance market support measures, FedScoop (October 11, 2022), <https://www.fedscoop.com/treasury-seeks-input-on-cyber-insurance-market-support-measures/>.