Health Sector Coordinating Council
Cybersecurity Working Group

Statement on Healthcare Cybersecurity Policy

March 2025

The Health Sector Coordinating Council Cybersecurity Working Group offers recommendations for how our industry and the Trump Administration should collaborate toward an updated healthcare cybersecurity policy structure that combines regulation and voluntary commitments for the healthcare industry to protect itself from cyber threats that jeopardize patient care and operational continuity. Specifically, we propose that the Trump Administration and the healthcare industry ***initiate a structured series of consultations and workshops to forge consensus on a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability.***

Institutional and Policy Background

The *Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG)* is a government-recognized critical infrastructure industry council of more than 470 healthcare providers; lab, blood, pharmaceutical and medical technology companies; payers; health IT entities; public health and government agencies partnering to identify and mitigate cyber threats to patient care, health data and research, systems, and manufacturing. The CWG membership collaboratively develops and publishes free healthcare *cybersecurity leading practices* and policy recommendations, and produces outreach and communications programs emphasizing the imperative that ***cyber safety is patient safety***.

The public-private partnership model that engages all critical infrastructure sector coordinating councils has progressed over 25 years, built on a foundation of presidential executive orders and statutes, notably Executive Order 13800 - *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* - signed by President Trump in 2017, and his Executive Order signed March 19, 2025 on *Achieving Efficiency Through State and Local Preparedness.* These policies institutionalize joint industry and government identification and mitigation of systemic threats to the nation's critical infrastructure, with sustained policy and practices that support the sector's security and resiliency.

As one of the standing working groups under the Healthcare and Public Health Sector Coordinating Council, the Cybersecurity Working Group has grown from 50 organizations in 2017 after it was established to more than 470 across all subsectors in 2025, and has produced *almost 30 leading practices and guidance documents*, by the sector for the sector, with more on the way.

The CWG has been a long-standing and respected partner to the government, leading the development of initiatives and recommendations that measurably improve our cyber defenses and resiliency to protect patient safety. Prominent among our joint accomplishments was a comprehensive set of cybersecurity controls published in 2019 (and updated in 2023) after two years of work. Called the *Health Industry Cybersecurity Practices (HICP)*, the framework was designed specifically for the healthcare industry under the auspices of Section 405(d) of the Cybersecurity Act of 2015, which directed HHS to work with the healthcare industry on a set of voluntary, consensus best practices for healthcare cybersecurity. This resource, along with the many other cybersecurity best practices we have produced for medical device security, supply chain cybersecurity, incident response, workforce development and others have attracted several hundred thousand downloads from the HHS and HSCC websites and are increasingly referenced as the principal NIST-mapped cybersecurity frameworks for the health sector.

Indeed, President Trump formally recognized HICP by signing Public Law 116-321 on January 5, 2021 as a set of "recognized security practices", along with the NIST Cybersecurity Framework, which if implemented by health provider entities would serve to reduce regulatory exposure in the event of a breach.

The HSCC-405(d) partnership also jointly developed the *Hospital Cybersecurity Landscape Analysis* (currently being updated), which identified those threats and vulnerabilities resulting in the most common sources of cyber attack against health systems, and pointed to prioritized controls that would most effectively address them. The result was 10 *Essential* and 10 *Enhanced HPH Cybersecurity Performance Goals* and the HSCC *Prioritized Recognized Cybersecurity Practices*.

Together, these resources developed jointly by HHS and health sector owners and operators represent a roadmap for advanced cybersecurity protections which, when implemented systemically throughout the health industry, will result in measurable improvements to the security and resiliency of the sector. While we cannot say that these recommended controls are yet as widely adopted as we know they will be with government amplification, leaders in the health sector have forged these recommendations with the recognition that they are affordable, scalable, implementable and *effective* as a negotiated foundation for a modernized and consensus-based healthcare cybersecurity framework for accountability.

HIPAA Security Rule Proposed Update Not Practicable or Effective

The HIPAA Security Rule Notice of Proposed Rule Making (NPRM) released in December 2024 either dismisses these important developments or mischaracterizes their potential for measurable improvement. A considerable number of the 52 CWG member industry associations that submitted comments representing their constituent members have made their concerns clear in their submissions to HHS about the cost and complexity of implementing the rule and the dubious effectiveness that compliance could achieve at improving security.

Recommendation

Given extensively critical feedback submitted by sector stakeholders about the NPRM, the Health Sector Coordinating Council Cybersecurity Working Group advises ***that the Administration suspend any further consideration of the NPRM as written and initiate a structured series of consultations and workshops with the HSCC CWG and other owners and operators of our national critical healthcare infrastructure to forge consensus on a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability.*** Such an approach would operationalize the aforementioned executive orders on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* and *Achieving Efficiency Through State and Local Preparedness.*

Precedent for this innovative approach to cybersecurity policy is in the development of the NIST Cybersecurity Framework as directed in Executive Order 13636 of 2013, "*Improving Critical Infrastructure Cybersecurity.*" This E.O. directed the National Institute of Standards and Technology (NIST) to serve as a convening authority for the private sector to drive development of the Cybersecurity Framework (CSF) for critical infrastructure protection, guided by NIST workshop processes over the prescribed course of one year. *The result was good policy operationalized*: The CSF has grown organically over the past 10 years as the guiding reference for essential cybersecurity practices. It establishes "*the What"* - expected objectives and measurable outcomes, leaving the owners and operators of critical infrastructure to implement "*the How"* – specific technical, operational and managerial controls tailored for accountability to those promulgated objectives. This approach replaces static one-size-fits-all regulations with guidance that is relevant and scalable to unique sector imperatives, flexible to meet ever-evolving threats and disruptive technology, cost-efficient, and effective at measurably improving cybersecurity outcomes.

The HICP can serve as a starting point for identifying priority practices that can be mandated as baseline controls, and the attached *Recommendations for Government Policy and Programs* presents principles and programmatic ideas which can supplement discussions toward joint commitments for a higher level of community security and accountability.

When applied specifically to healthcare and its supporting infrastructure this approach would represent a *contract* between the healthcare industry and government for *accountable* and *effective* healthcare cybersecurity policy.

As HICP, the HPH Cyber Performance Goals and other leading practices developed by the CWG were designed to map in various degrees to the NIST CSF, ***we propose that the HSCC Cybersecurity Working Group and other leaders in the industry convene with government to design a healthcare-specific policy, programmatic and regulatory framework that maps to CSF for all interconnected owners/operators and their supporting infrastructure in the healthcare ecosystem***. The framework would be informed in part by the methodologies and findings of the *Hospital Landscape Analysis* and the *HSCC Prioritized Recognized Cybersecurity Practices*.

This framework must also be applied to the currently unregulated technology and service providers that interact with healthcare; it should not be the sole responsibility of covered entities to independently confirm their third-party alignment with cybersecurity controls. HSCC proposed in congressional *testimony* to the House Energy and Commerce Committee April 1, 2025 that any technology and service providers supporting critical healthcare infrastructure should be held to higher standards of cybersecurity. Healthcare is considered critical infrastructure for a reason - because lives are at stake – and the protection of lives through the hardening of our digital healthcare infrastructure and its inputs should not be optional.

The results of this consultative process would enable us to prioritize those most critical cybersecurity controls that should be made mandatory - staggered over a phased period - and which should be allowed to evolve through incentives and support for needs-based, resource-constrained health providers, practices and clinics in rural, urban and other hard-working communities across America.

Conclusion

There is little disagreement in the healthcare industry that our cyber health and patient care would be better served with higher levels of accountability and enforcement on the principle that *Cyber Safety is Patient Safety*. A firm floor of cybersecurity expectations, even if they come at increased cost when calculated with risk-prioritized justification, can establish consistency and stability across a sector that is otherwise under constant attack. But any enhanced regulatory requirements must also be promulgated with thoughtful assessment of their operational feasibility and security effectiveness, and with appropriate backstops for those on the razor's edge of clinical resiliency and financial solvency. If we can negotiate a rational regime for accountability, as a rising tide lifts all boats rather than a breaking wave capsizing them, we will jointly succeed.

##

Contact:
Greg Garcia
Executive Director
greg.garcia@healthsectorcouncil.org
https://HealthSectorCouncil.org