Testimony of

Greg Garcia
Executive Director

of the

Healthcare and Public Health Sector Coordinating Council
Cybersecurity Working Group

on

"Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"

Before the

United States House of Representatives

Committee on Energy and Commerce

Health Subcommittee

April 16, 2024

HSCC Cybersecurity Working Group Summary of Recommendations

My statement today will offer what we believe the health sector and government need to do to get ahead of future similar incidents and reduce their likelihood and impact.

Our first recommendation, which in fact is now just getting underway, is the need to ***perform a health infrastructure mapping and risk assessment.*** This will provide visibility to those critical services and utilities – such as change healthcare - that support the many essential dependencies across the healthcare ecosystem.

Second, informed by risk mapping of those critical services, the results of such efforts should facilitate government's ability to ***assess consolidation proposals for mergers and acquisitions against their potential for increased cyber incident and impact risk.***

Third, related to critical function assessment is the imperative to ***hold third party product and service providers and business associates to a higher standard of "secure by design and secure by default"*** for technology services and capabilities used in critical healthcare infrastructure.

Fourth, invest in a government-industry rapid response capability.

Fifth, invest in a cyber safety net for the nation's underserved providers, built on accountability and incentives. The HHS FY 2025 budget request contemplates this approach modeled after the incentive structure in the promoting interoperability program. It calls for a $800 million commitment over two years to certain high-need hospitals to implement baseline "cyber performance goals." After that, penalties will apply to those that don't meet those minimum standards. *Incentives followed by accountability.*

Finally, over the next five years, the industry and government have an all-hands on deck responsibility to ***implement the HSCC 5-year Health Industry Cybersecurity Strategic Plan.*** The plan recommends 10 end-state cybersecurity goals, and 12 implementing objectives to achieve those goals by 2029.
If we make progress against the goals and objectives, we can achieve an overall industry target state that looks like:

- Healthcare cybersecurity, both practiced and regulated, is made easier for practitioners and patients;
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility;
- Leaders in the healthcare c-suite own cybersecurity as an element of enterprise risk;
- A cyber safety net is in place to promote cyber equity across the ecosystem;
- Workforce is trained and capable in good cybersecurity as a wellness continuum; and,
- A "911 cyber civil defense" capability to lead early warning, incident response and recovery is reflexive and always on.

Cyber Safety is Patient Safety

Introduction

Chairman Guthrie, Ranking Member Eshoo, and members of the Committee, my name is Greg Garcia. I am the Executive Director of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG), an industry-led advisory council of more than 430 healthcare organizations and government agencies working in partnership under the auspices of the DHS CISA's Critical Infrastructure Partnership Advisory Council (CIPAC) framework and Presidential Policy Directive 21. Our mission is to identify and mitigate cybersecurity threats and vulnerabilities to the delivery and support of healthcare. At the heart of this work is a recognition that patient safety must be a guiding principle of healthcare cybersecurity – that *cyber safety is patient safety.*

I appear before you today not with a doctor's bag or a cybersecurity practitioner's toolbox, but as one with 30 years of executive management in the cybersecurity and related professions. I have navigated and advised on the intersecting languages of policy, technology, and business operations and management across the Executive Branch, Congress, and the business community. This includes serving as the nation's first Assistant Secretary for Cybersecurity and Communications at the U.S. Department of Homeland Security from 2006 - 2009, as professional staff on the House Committee on Science where I shepherded the drafting and enactment of the Cybersecurity Research and Development Act of 2002, and as a policy and security executive with high technology and financial services companies and industry groups. In all of these capacities, I am proud of my public service.

We appreciate the Committee's holding this timely hearing to examine health sector cybersecurity in the wake of the ransomware attack against Change Healthcare. My testimony today will focus not on the technical or operational aspects of the Change Healthcare cyber attack – I will leave that to others on this panel – but on what the health sector and government have already done and more importantly need to do going forward to get ahead of future incidents and reduce their likelihood and impact.

Today, I will cover four areas that will help inform both the diagnosis and prescription for healthcare cybersecurity:

First, a brief overview of the Health Sector Coordinating Council Cybersecurity Working Group and our partnership with HHS and other government agencies;

Second, a review of the cybersecurity challenges and their causes faced by the health sector; and

Third, what we learned about the Change Healthcare incident and what industry and government need to do to get ahead of future incidents.

About the Health Sector Coordinating Council Cybersecurity Working Group

The HSCC Cybersecurity Working Group serves as an advisory council to the sector, HHS, CISA, and other government agencies, with a formally-designated critical infrastructure protection mission. The HSCC, Health-ISAC, HHS, FDA, and CISA work jointly to identify and mitigate systemic cyber threats to the security and resiliency of critical healthcare infrastructure, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response.

The HSCC Cybersecurity Working Group (CWG) is a volunteer organization with a growing list of ~430 member organizations that operate under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to any organizations that are a) covered entities or business associates under HIPAA; b) health plans or payers; c) regulated by FDA as a medical device or pharmaceutical company; d) health IT companies subject to health data interoperability rules; e) public health organizations and f) any healthcare industry associations or professional societies. A small allotment of "Advisor" members – consulting, law, and security companies - is permitted to participate and support CWG initiatives pro bono.

The HSCC CWG is currently organized into numerous function-specific, outcome-oriented task groups composed of 40 to 140 organizations across the health industry and government that develop cybersecurity best-practices and resources for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity hygiene; supply chain cyber risk management; workforce development; incident response and operational continuity; and medical technology security, among many others.

With that cross-functional cybersecurity imperative in mind, since 2019 the CWG has published 28 best practices and guidance documents that address the many recommendations of a 2017 HHS healthcare cybersecurity task force of industry and government experts. Those resources, developed by the sector for the sector, are freely available on our website at https://healthsectorcouncil.org/hscc-publications/. Several of these publications are under joint seal by HSCC and HHS as a demonstration of our shared resolve and vision for sound

cybersecurity practices that all health organizations should implement. One of these – the *Health Industry Cybersecurity Practices (HICP)* - is recognized under P.L. 116-321 as a set of controls which, if implemented by an entity prior to a breach that becomes subject to HIPAA enforcement action, would be a mitigating factor in the consideration of punitive fines and audits by HHS.

Cyber Threats, Vulnerabilities and Incidents

The reference to "healthcare cybersecurity" was generally not heard ten years ago. But since 2017, when ransomware and other forms of cyberattack disabled the health system in the UK and many other U.S. providers and multinational companies, the epidemic of cyber threats against the health sector has only proliferated, with the Change Healthcare attack the most recent and indeed, the most catastrophic across the sector. In 2017, the HHS Healthcare Cybersecurity Task Force report diagnosed healthcare cybersecurity to be in "critical condition." It found that, because of the rise in digital healthcare, technological advances, and the expansion of connected devices and data, coupled with a widely distributed ecosystem, a shortage of skilled cyber workforce and resource constraints among the under-resourced healthcare entities, the cyber "attack surface" in healthcare – and the adversaries intent on exploiting it – have expanded.

Threat actors are motivated to leverage ransomware attacks to monetize stolen health data, and operational disruptions. The cybersecurity focus in healthcare has traditionally been on data and privacy, but if healthcare data are manipulated or destroyed, and if health delivery organizations (HDOs), their suppliers, service providers and payment systems are rendered

inoperable, as seen in the Change Healthcare attack and numerous ransomware incidents before it, patient lives can be at risk. This threat is particularly acute for small, rural, critical access and underserved, under-resourced health providers that are operating on razor thin or negative margins and haven't the capability to make the proper investments in cyber preparedness and response programs.

Ransomware and other disruptive cyber attacks

Widely reported incidents experienced over the past few years involved some combination of disruptions affecting patient safety, business operations and clinical workflow, such as:

- Stroke, trauma, cardiac, imaging and other services, closed to admissions;
- Radiation and other treatments for cancer patients, including surgery, delayed;
- Medical records about prescriptions, diagnoses, and therapies become inaccessible and some, permanently lost;
- Clinical trial data in a research lab, lost;
- Payment systems, down;
- Inability to order or receive supplies;
- Emergency transition to a paper system causing time lags, inefficiencies, and errors;
- Staff furloughed; and
- Medical devices stop working, or their settings are corrupted, risking danger to the patient.

Business Risks

In addition to the obvious impact on direct patient care, a cyberattack can inflict health providers and companies with business risks, such as:

- Disruptions to reimbursement and other financial flows
- Damaged reputation
- Lost patient trust
- Lawsuits
- Regulatory penalties
- Strained employee morale and burnout, and
- Reduced stock value.

Current and Future Dynamics in the Healthcare System

The health sector is highly interconnected:

- Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and payment for those services;
- Many healthcare facilities, such as hospitals, operate in environments that are accessible to the public, which adds to the vulnerability;
- The average patient bed has 15 supporting medical devices, and a 500-bed hospital could have 7,500 devices, many of which are over 8-10 years old and connect to a network that may not be protected or segmented from other systems or databases;

- Thousands of hospital-deployed medical devices are supplied by many different manufacturers with various levels of security and patching protocols. Devices often have unencrypted hard drives or common passwords set by the manufacturer that cannot be changed. Implementing compensating controls, or taking them offline for patches, updates or replacements is complicated. Further complicating HDO replacement programs are budget constraints and small operating margins;
- When supply chains are tightened or non-existent for various reasons, or pandemics or natural or man-made regional disasters occur, stretched supplies and staff become additional factors; and
- Coupled with a diverse base within the sector, complex siloed departments, a lack of skilled cyber staff, cyber security situational awareness, knowledge and training for the medical staff and CEO and Board levels, and lack of cyber security strategy including a risk management approach, the health, and public health sector face an enormous challenge.

Change Healthcare Attack and the Way Forward

The Change Healthcare attack that occurred on February 21 imposed a stark reminder to the health sector – and indeed to every critical industry sector – that there are essential utilities undergirding our critical infrastructure that, if severely disrupted or disabled, would cause cascading and crippling impact on our national economic security and public health and safety. These utilities such as software programs, processing applications and specialty

communications platforms are often unknown and taken for granted, but without which the very delivery and financing of healthcare would not be accomplished.

HSCC Cybersecurity Recommendations

1) Our first recommendation, which is now underway, is the need to ***Perform a national health infrastructure mapping and risk assessment*** to provide visibility to those critical services and utilities – such as Change Healthcare - that support the many interconnected interdependencies across the healthcare ecosystem. There is in fact a policy framework in place – Section 9 of Executive Order 13636 of 2013 - which directs DHS and sector agencies to identify those "critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

   This involves HHS convening industry leaders from across the healthcare subsectors – health providers and health IT, insurers and plans, pharmaceutical and medical technology companies, and public health agencies -- to identify those critical functions and assets, their connect points and dependencies, and the relative risk to the provision of healthcare – both immediate impact and duration - that those functions would pose if disrupted. It is about working with the DHS Cybersecurity and Infrastructure Security Agency to understand concentration risk, levels of redundancy of similar services, and the adequacy of both physical and cyber protective measures to support the security and resiliency of those critical utilities. This process will take time to get it right, even as it will never be fully accurate given the constantly shifting architecture of our complex healthcare system.

To my knowledge such an assessment has not yet been done comprehensively for healthcare, and now is the time to do so, with haste. We indeed are in the early stages of working with HHS to begin this process. It needs to be done comprehensively, yet carefully, to ensure that we do not inadvertently reveal critical and potentially vulnerable elements of our critical infrastructure operations to our adversaries.

2) Informed by mapping and risk measurement of critical services in healthcare infrastructure, the results of such efforts should facilitate government's ability to ***assess consolidation proposals for mergers and acquisitions against their potential for increased cyber incident and impact risk.*** We expect that the healthcare industry will continue to consolidate over the coming years, both vertically and horizontally. This can present market concentration risk as considered under traditional antitrust rules, but also the potential for creating single points of failure as vulnerable targets for cyber threats. If there is no – or low – redundancy or fall-back options for critical services in the healthcare value chain that are disrupted by cyber attack such as what happened to Change Healthcare and its thousands of customers, the resulting cascading impact to patient care and financial flows should serve as a reference for evaluating cybersecurity and resilience factors among other market factors in the consideration of mergers and acquisitions.

3) Related to critical function assessment is the imperative to ***hold third party product and service providers and business associates to a higher standard of "secure by design and secure by default"*** for technology services and capabilities used in critical healthcare infrastructure. More than half of all data breaches on health systems are through business

associates; many ransomware attacks similarly find their way into enterprise networks through third parties. Many medical devices continue to be delivered to the customer with security vulnerabilities, with uneven attention to the security imperative among device manufacturers.

The 2021 Executive Order on Improving the Nation's Cybersecurity, while focused on government procurement of software and technology, can serve as a reference for how the private sector and the government can work together to require workable third party cybersecurity assurances. The third party/supply chain security issue is a seemingly intractable one, complicated by constant innovation and the unsustainable costs of assessment, testing, audit, and compliance. But making progress requires a collective resolve – our reach must exceed our grasp.

4) ***Invest in a government-industry rapid response capability.*** Emergency response, recovery and business continuity remain ongoing challenges for private sector and government stakeholders alike. The Change Healthcare attack exposed significant challenges for health systems to maintain business continuity and for government and payers to provide time sensitive operational and financial backup for providers in dire straits. Whether we call it a "Healthcare Cyber FEMA" or a "911 Cyber Defense", so much of our health system and patient care depend on minutes, hours and days, not on months. Investing in a rapid response force against systemic attacks, using government authority to declare "national cyber emergency", activate catastrophic national cyber insurance to supplement private insurance, provide fast financial support, permit temporary suspension of certain regulatory

chokepoints and provide mobile healthcare capability to assist those in dire need, would be a next-generation end-state we call for in our Health Industry Cybersecurity Strategic Plan, discussed below. This need is particularly important for the "target rich, cyber poor" small, rural, critical access, Federally Qualified Health Centers and other underserved, under-resourced health providers across the nation.

5) ***Invest in a cyber safety net for the nation's underserved providers, built on accountability and incentives.*** As discussed, the nation's under-resourced health systems are the most vulnerable to cyber threats, lacking the resources and expertise to invest in basic cyber hygiene requirements. The HSCC, through its Health Industry Cybersecurity Practices and many other published healthcare-focused cybersecurity resources - https://healthsectorcouncil.org/hscc-publications/ - has worked to close that gap between cyber threats and preparedness. However, the issue of resources and awareness remain as impediments to adoption and implementation. Many of the smaller, underserved providers in our membership have expressed the same observation that they will invest in strengthened cyber defenses if they are told to do so, but that if given the choice between hiring a nurse to care for patients or hiring a cybersecurity professional, the Hippocratic Oath of "first do no harm" usually wins. But under the principle that "cyber safety is patient safety" many providers would acquiesce to minimum mandatory cyber controls as long as they are financially supplemented. The HHS FY 2025 budget request contemplates this approach modeled after the incentive structure in the "Promoting Interoperability Program", involving an $800 million commitment over two years to certain high-need

hospitals to implement baseline "Cyber Performance Goals", after which penalties apply to those that don't meet those minimum standards. Many of the 10 "essential" or baseline goals, and the 10 "enhanced" or more mature controls, are based on the voluntary industry best practices promulgated in the Health Industry Cybersecurity Practices, so we are aligned with this approach. We emphasize, in addition, that whatever resources are directed to the underserved, funding should as much as possible take the most direct route to providers through grants, subsidies and technical assistance, according to the choice of those that need it.

6) Finally, over the next five years, the industry and government have an all-hands on deck responsibility to ***contribute to achievement of the 5-Year Health Industry Cybersecurity Strategic Plan*** - ***https://healthsectorcouncil.org/cyber-strategic-plan/*** published by the HSCC Cybersecurity Working Group coincidentally one week after the Change Healthcare attack.

The Strategic Plan projects 7 major industry trends in the health sector over the next 5 years and present a sector-level call to action for healthcare organizations to address those trends and increase their individual and collective cyber resiliencefor an interconnected industry. The intent of this document is to guide C-suite executives, information technology and security leaders, government and other relevant stakeholders toward investment and implementation of strategic cybersecurity principles which, if adopted, will measurably reduce risks to patient safety, data privacy, and care operations which can cause significant financial, legal, regulatory, and reputational impact.

The strategic plan is meant for all HPH sub-sector participants, including medical device manufacturers (MDMs), pharmaceuticals, healthcare delivery organizations (HDOs), health insurance payors, regulators, and other industry and government participants whose products and services are used in healthcare environments.

The plan presents 10 end-state cybersecurity goals, with 12 implementing objectives to achieve those goals by 2029.

If we make progress against the goals and objectives, we can achieve an overall industry target state that looks like:

- Healthcare cybersecurity, both practiced and regulated, is reflexive, evolving, accessible, documented, and implemented for practitioners and patients;
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility;
- Leaders in the healthcare C-Suite embrace accountability for cybersecurity as an enterprise risk and a technology imperative;
- A cyber safety net is in place to promote cyber equity across the ecosystem;
- Workforce cybersecurity learning and application is an infrastructure wellness continuum; and,
- A “911 Cyber Civil Defense” capability to uphold early warning, incident response and recovery is reflexive and always on.

Five-Year Cybersecurity Goals to Address Industry Trends

G1	Healthcare and wellness delivery services are user -friendly, accessible, safe, secure, and compliant	G6	Healthcare technology used inside and outside of the organizational boundaries is secure -by-design and secure -by-default while reducing the burden and cost on technology users to maintain an effective security posture
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	G7	A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non -traditional health and life science entities
G3	Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors	G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing
G4	Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	G9	The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	G10	Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization

Five-year Cybersecurity Objectives to Implement the Goals

O1	Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure -by-design and secure -by-default	O7	Increase incentives, development and promotion of health care cybersecurity -focused education and certification programs
O2	Simplify access to resources and implementation approaches related to the adoption of controls aligned with regulatory and sector standards for securing devices, services, and data	O8	Increase utilization of automation and emerging technologies like A.I. to drive efficiencies in cybersecurity processes
O3	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco -system	O9	Develop health sub -sector specific integrated cybersecurity profile aligned with regulatory requirements
O4	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	O10	Develop meaningful cross -sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third -party provider cybersecurity risks
O5	Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations	O11	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness
O6	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health	O12	Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurityincidents

The Cybersecurity Strategic Plan is the result of extensive and multiple collaborative sessions among almost 200 industry and government organizations across the HPH sector represented by senior cybersecurity and clinical executives and subject matter experts over a period of over 18 months.

Conclusion

Mr. Chairman, Members of the Committee, as a critical infrastructure industry the health sector and its dedicated workforce are mobilizing against the ongoing and existential threat of cyber disruption. We also recognize we need to move faster to keep up with the evolving threats. But through continued and expanded engagement in our collective purpose, broader awareness promotion, and forward-leaning government programs and support, we can move the needle and five years from now upgrade the healthcare cybersecurity diagnosis from "critical" to "stable condition."

Thank you.

Submitted for the record:

- Health Industry Cybersecurity Strategic Plan - https://healthsectorcouncil.org/the-plan/
- HSCC cybersecurity policy, programmatic and regulatory recommendations for government consideration - https://healthsectorcouncil.org/health-industry-cybersecurity-recommendations-for-government-policy-and-programs/