Cybersecurity in Healthcare: Challenges, Risks and the Path Forward

Key Insights Report

eHI
eHEALTH INITIATIVE

PHILIPS

Introduction

Given the scope, intensity, and continuing focus on the COVID-19 public health emergency, there has been less attention paid to other healthcare crises, both current and imminent. The increasing frequency and impact of recent cyberattacks is one such menace, presenting an enormous challenge to our health infrastructure. Ransomware attacks, breaches of protected health information (PHI), and attacks on the operating systems of medical devices are top of mind for many healthcare executives. The interconnected nature of our healthcare system, combined with outdated infrastructure, means that cyberattacks can have dangerous and even deadly impacts[1] on our public health system as a whole.

A recent study showed a 55 percent jump in cyber incidents against the healthcare sector in 2020,[2] and as of August 2021 there were a total of 48 ransomware attacks of the same nature.[3] Threat actors are continuously adjusting and evolving their attacks to cause the greatest amount of harm to their victims, and the vulnerabilities of the healthcare system both caused and exposed by COVID-19 have now put our nation at colossal risk for catastrophic impacts. This climate has led to an increasing amount of public attention on cyberattacks, both in the press and on the part of government and policy leaders, and there is a growing awareness that the cybersecurity of critical healthcare infrastructure is crucial not only to ensure seamless and effective delivery of care, but to save lives.

It was in this environment that Philips and the eHealth Initiative (eHI) convened a Roundtable of industry and policy experts in Summer 2021, titled "Cybersecurity in Healthcare: Challenges, Risks and the Path Forward." Panelists included:

- Jonathan Bagnall, Global Cybersecurity Solutions Market Leader at Philips Healthcare;
- Josh Corman, Chief Strategist at Cybersecurity and Infrastructure Security Agency (CISA);
- Erik Decker, Assistant Vice President and Chief Information Security Officer at Intermountain Healthcare;
- Greg Garcia, Executive Director for Cybersecurity of the Healthcare and Public Sector Coordinating Council (HSCC);
- Gabrielle Hempel, Cloud Security Engineer at Cigna; and
- Mark Jarrett, Senior Vice President & Chief Quality Officer, Deputy Chief Medical Officer at Northwell Health.

The panelists led a weighty and nuanced discussion about the vulnerabilities of our healthcare system's cyber-defense systems, the dangerous impact of cyberattacks, and what is being done to prevent them, or reduce their harm, in the future.

Impact of Healthcare Cyberattacks

Infrastructure weakness can have disastrous effects across numerous different sectors, from the food supply chain to transportation to water supply. Healthcare comprises the single largest share of our nation's economy,[4] and its infrastructure is intertwined with those aforementioned sectors, as well as with broadband internet, telecommunications, and electricity.

"With great connectivity comes great responsibility. If we are overdependent on undependable IT, even the smallest event can have a profound impact."

- Joshua Corman
CISA

As noted by Intermountain's Erik Decker in his recent testimony before the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security, "cybersecurity incidents are not only a threat to national security, they are also a threat to patient safety, as attacks can cause denial of service, medical device corruption, and data manipulation that directly impact clinical operations, patient care, and public health."[5]

Given the myriad links between healthcare infrastructure and so much of society, a cyberattack on a healthcare entity can have a ripple effect, leading to wide-scale harm. Many of these have unfortunately already been experienced, whether causing an interruption in the delivery of care or increased patient mortality rates. CISA's Joshua Corman emphasized both the potential and reality of "excess mortality," noting that we already know that delayed patient care increases the patient mortality rate. Direct evidence of this comes in the wake of a ransomware attack on the University of Vermont Health Network in October of 2020, which, given resources already strained by the COVID pandemic, resulted in delayed chemotherapy and mammogram appointments. A team from CISA analyzed patient outcome data and found that patients fared more poorly in hospitals handling a cyberattack than in those hospitals that are not.[6]

Among other unfortunate realities the pandemic exposed were the effect of stress, burnout, and subsequent retirement of medical personnel; the limited nature of crucial medical supplies; and the inability of so many healthcare settings to cope with patient demand. The CDC estimates that once the United States hit 500,000 deaths from COVID-19, the country reached 150,000 excess deaths related to fear of seeking care or inability to receive treatment.[7]

Smaller, rural, and less-resourced hospitals or clinics can be particularly vulnerable to devastating cyberattack impacts, Jonathan Bagnall from Philips noted, as they often don't have a plan or budget for disaster recovery, nor do they have the ability to send patients to a nearby hospital in the event theirs becomes inoperable.

The threats to patient safety are not always obvious. For example, Decker noted in his NCVHS testimony and referenced again at the Roundtable that "we must consider the ability of a threat actor to hold the integrity of our data for ransom as well. For example, security research has demonstrated that malware can manipulate and inject realistic images of cancerous growth into MRI scans. When radiologists looked at these images, 99 percent of them believed the scan had detected cancer… A future attack could extort our ability to trust the very data that we use to treat and care for patients."[8]

As Northwell's Dr. Mark Jarrett explained in a recent piece in Modern Healthcare, "healthcare organizations are no longer siloed from each other or from other sectors of the national infrastructure on an increasingly integrated digital platform."[9] He reiterated at the Roundtable that "the next healthcare crisis could be due to attacks on other critical infrastructure that would then have effects on healthcare. An attack on any hospital system affects everything."

Outdated Healthcare Tech Models and Lack of Operational Understanding

Too many healthcare systems, hospitals, and clinics currently employ what are known as "legacy systems," or outdated information technology systems upon which providers are overly dependent. Decker noted that, given archaic or insufficient healthcare infrastructure available, "legacy systems stick around." Organizations are too often forced to make dangerous risk calculations, he explained: "do I put the money in therapeutics or diagnostics, or do we put money into infrastructure?" Due to the lack of any incentive to invest in cybersecurity, the money tends to flow to direct patient care, leaving the healthcare system vulnerable to attacks.

> *"As digitization continues to increase, rapid response speed will become increasingly a requirement," Jonathan Bagnall from Philips noted, emphasizing the need to align industry liability in the event of a breach or attack to performance and availability of systems.*

Underinvestment in infrastructure and security is often due in part to a lack of operational understanding when it comes to the "Cloud" – the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. There are obvious benefits to storing healthcare data in the Cloud, but unless the security implications of doing so are fully understood, or without conducting the necessary "due-diligence" before doing so, risks can increase, explained Cigna's Gabrielle Hempel. Much of her work focuses on educating users about the Cloud, making it more transparent, and increasing knowledge about Cloud environments so that users understand not just where information is stored but how to keep it safe.

The necessity to bolster not only system security but trust in cyber environments has been emphasized at the highest levels of government. Indeed, President Biden's May 2021 Executive Order on Improving the Nation's Cybersecurity held that "the private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."[10]

Public-Private Efforts to Mitigate Risk and Shore Up Security

The Cybersecurity and Infrastructure Security Agency (CISA) launched in August of 2021 the Joint Cyber Defense Collaborative (JCDC), a new agency effort designed to mitigate risks and shore up defenses in coordination with multi-sector partners. Its goals are to share insights to shape understanding of cyber defense challenges and opportunities; design whole-of-nation cyber defense plans to address risks; support joint exercises to improve cyber defense operations; and implement coordinated defensive cyber operations.[11]

> *"There's a Three Musketeers aspect to all of this: none of us individually are as smart as we are collectively,"*
>
> *- Greg Garcia*
> Public Health Sector Coordinating Council

The JCDC is only the latest in an on-going effort to create public-private partnerships to address cyber challenges, including those in healthcare. For more than a decade, the Healthcare and Public Health Sector Coordinating Council (HSCC) – a coalition of industry associations and their members – has been a platform for collaboration among healthcare industry leaders and the government to address the most pressing security and resiliency challenges facing the healthcare sector as a whole.

The work of the HSCC, and its success, is built on the notion that public-private partnerships based on critical infrastructure drive government policies recognizing these critical sectors. Collective efforts to identify threats and mitigate them are crucial, given the interdependence and interconnectedness of healthcare with other sectors.

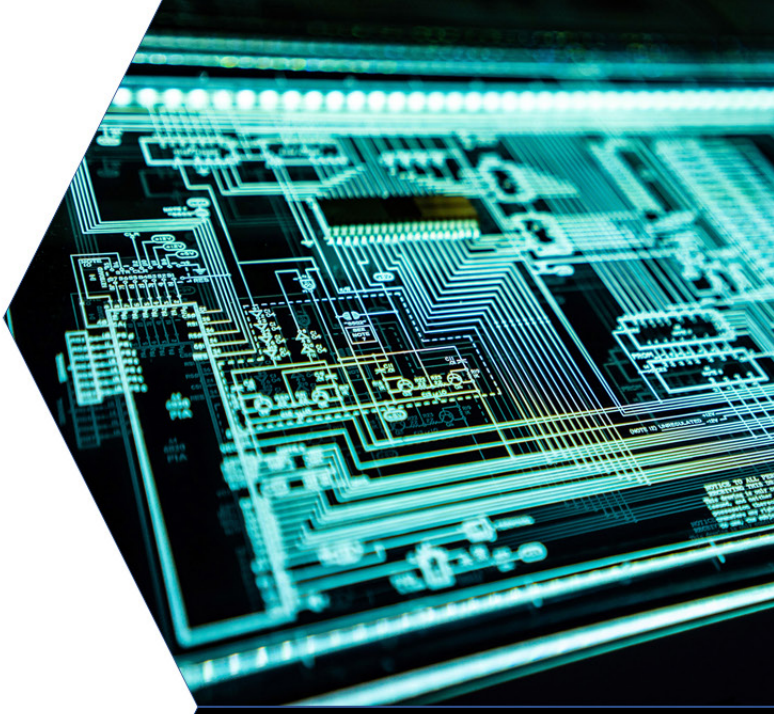
Key to the work of the HSCC is the 2017 Healthcare Industry Cybersecurity (HCIC) Task Force, the imperatives of which include defining and streamlining leadership, governance, and expectations; increasing the security and resilience of medical devices and health IT; developing the capacity necessary to prioritize and ensure awareness and tech capabilities; and increasing healthcare industry readiness through improved awareness and education.

When CISA was stood up, the agency shifted focus to the national critical functions. Even though critical healthcare infrastructure is privately owned and operated, CISA and its work are evidence of the employment – and importance – of a shared responsibility model.

The federal government, too, has been taking important action to support cybersecurity infrastructure and contribute to the efforts of the HSSCC. In January of 2021, Congress signed into law H.R. 7898 (now P.L. 116-321), recognizing the proliferation of cyber threats against the healthcare system and directing the Department of Health and Human Services (HHS), when making penalty determinations against HIPAA-covered entities and their business associates victimized by a cyberattack, to take into account the covered entity's use of recognized security best practices over the course of the past year.

Importantly, this provision "serves as a positive incentive for health providers to increase investment in cybersecurity for the benefit of regulatory compliance and, ultimately, patient safety," said Decker. This law is an important way to help even the smallest healthcare organizations make the investments necessary to help them protect themselves.

The law explicitly recognizes a set of cybersecurity best practices established under Section 405(d) of the Cybersecurity Act of 2015 and implemented as a joint standing task group of the HSCC Cybersecurity Working Group and HHS, composed of more than 250 volunteers from across the HSCC membership and HHS. The resulting report, "Healthcare Industry Cybersecurity Practices (HICP)," provides scalable and voluntary cybersecurity principles and practices for use by providers of any size and ability. This publication is designed to be used across the sector as well as tailored to small, medium, and large organizations. Panelists touted this work as key to bringing industry along toward more robust and responsible cybersecurity.



Industry Efforts to Improve Cyber-Defense

Industry has also taken important strides to shore up cybersecurity for healthcare entities and systems of all sizes. At Philips, Bagnall's workstream has focused on development of model language for healthcare contracts, which will help shorten and streamline security negotiations as part of the procurement process. The three concepts on which the model language focuses are performance, product design maturity, and system maturity. Philips has developed some 52 security clauses that fit within these three concepts, negotiating throughout the development process on what the contract terms should cover, both from minimum-requirement perspective and on a baseline of acceptability.

The healthcare industry is increasingly using the Federal Risk and Authorization Management Program (FedRAMP) as a model for its own cybersecurity efforts, and in particular cloud security. FedRAMP was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government and encourages agencies to use modern cloud technologies, with an emphasis on security and protection of federal information. FedRAMP provides a good set of controls and framework for how the cloud levies responsibility.

Positive steps are being taken to both improve and invest more in cybersecurity, panelists noted, but upending the model and improving healthcare budgets for cyber-defense is still imperative. Otherwise, the near-impossible choice between spending money on patient care or on improving the security of the operating infrastructure will persist.

The cyber-maturity of a particular organization should dictate its cybersecurity budget; if its cyber infrastructure is low-maturity, an organization should have a very high cybersecurity budget and then reduce cost over time. Panelists agreed that conducting a cyber-maturity evaluation is critical, in part because it provides justification to an organization's board of directors.

A Path Forward

Despite the current cyber threat environment, all panelists expressed optimism in the work being done to improve cybersecurity across the sector, with government and industry partnerships leading the way. This work cannot happen soon or quickly enough, as there was unanimous agreement that if we don't significantly enhance our preparations for the acute risk to healthcare systems and patients now, we will almost certainly repeat the disorganized – and deadly – COVID-19 response evident during early 2020.

The recently enacted American Rescue Plan and the funds it directs to cybersecurity are a promising start. With enhanced investment and strategic planning among the Biden Administration, public-private partnerships, and HHS, Roundtable panelists are confident that not only the security and resiliency of the healthcare system but patient safety can measurably improve.

Resource Hub

- Testimony by Erik Decker, CIO, Intermountain Healthcare to the National Committee on Vital & Health Statistics, Subcommittee on Privacy, Confidentiality, and Security, July 2021, *Addressing Healthcare Security Challenges*
- Modern Healthcare, Drs. Mark Jarrett and Reuven Pasternak, *Why All Cybersecurity Breaches Could Post a Threat to Healthcare*
- Department of Health and Human Resources, Office of Information Security's August 2021 report *Ransomware Trends in 2021*
- Healthcare & Public Health Sector Coordinating Council, Healthcare Cybersecurity Overview, *Recent Cybersecurity Policy Development Affecting the Healthcare Sector, 2021*
- Healthcare & Public Health Sector Coordinating Council, *Recent Cybersecurity Policy*
- CPO Magazine, February 2021, Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the US Impacted
- May 12, 2021, *Executive Order on Improving the Nation's Cybersecurity*
- Cybersecurity and Infrastructure Security Agency's August 2019 report *Strategic Intent: Defend Today, Secure Tomorrow*
- Department of Health and Human Services, Office of the Assistant Secretary of Preparedness & Response, February 2021 report, *Healthcare System Cybersecurity: Readiness & Response Considerations*
- Department of Health and Human Services, Office of Inspector General, June 2021 report, *Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals*

Endnotes

1. Addressing Healthcare Security Challenges: Testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality and Security, 117th Cong. (2021) (hereinafter "NCVHS testimony").
2. Ikeda, S. (2021, February 26). Healthcare cyber attacks rise by 55%, over 26 million in the U.S. Impacted. CPO Magazine. https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/.
3. HHS Cybersecurity Program. Office of Information Security. (2021.) Randsome Trends 2021. Department of Health and Human Services.
4. See, e.g., Nunn, Ryan, et al. "A Dozen Facts about the Economics of the US Health-Care System." Brookings, The Brookings Institute, 6 Apr. 2020, www.brookings.edu/research/a-dozen-facts-about-the-economics-of-the-u-s-health-care-system/.
5. NCVHS testimony.
6. See, e.g., Westman, Nicole. "The Pandemic Revealed the Health Risks of Hospital Ransomware Attacks." The Verge, 19 April 2021, https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks.
7. See generally Czeisler MÉ, Marynak K, Clarke KE, et al. Delay or Avoidance of Medical Care Because of COVID-19–Related Concerns — United States, June 2020. MMWR Morb Mortal Wkly Rep 2020;69:1250–1257. DOI: http://dx.doi.org/10.15585/mmwr.mm6936a4external icon.
8. NCVHS testimony.
9. Jarrett, M. P., &; Pasternak, R. (2021, July 19). Why all cybersecurity breaches could pose a threat to healthcare. Modern Healthcare. https://www.modernhealthcare.com/opinion-editorial/why-all-cybersecurity-breaches-could-pose-threat-healthcare.
10. "Executive Order on Improving the Nation's Cybersecurity." The White House, The United States Government, 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
11. United States, Department of Homeland Security, Cybersecurity & Infrastructure Security Agency. CISA Strategic Intent - Defend Today, Secure Tomorrow, Office of the Director of CISA, Aug. 2019. https://www.cisa.gov/publication/strategic-intent

About eHealth Initiative & Foundation

eHealth Initiative Foundation (eHI) convenes executives from every stakeholder group in healthcare to discuss, identify and share best practices to transform the delivery of healthcare using technology and innovation. eHI, along with its coalition of members, focuses on education, research, and advocacy to promote the use and sharing of data to improve health care. Our vision is to harmonize new technology and care models in a way that improves population health and consumer experiences. eHI has become a go-to resource for the industry through its eHealth Resource Center. For more information, visit ehidc.org.

About Philips Healthcare

Philips is a leading health technology company focused on improving people's health and enabling better outcomes across the health continuum – from healthy living and prevention, to diagnosis, treatment and home care. To learn more, visit https://www.usa.philips.com/healthcare/resources/landing/interoperability-and-cybersecurity.