CSC 2.0

June 2024

Healthcare Cybersecurity Needs a Check Up

By Michael Sugden and Annie Fixler

Table of Contents

Executive Summary 4

Overview of Healthcare Cyber Challenges 5

Case Study: Change Healthcare Attack 7

Unique Challenges Facing Rural Hospitals 7

Current U.S. Government Efforts 8

Industry-Led Collaboration 10

Recommendations 10

Conclusion 13

Executive Summary

In May 2021, San Diego-based hospital system Scripps Health suffered a massive ransomware attack lasting almost four weeks. The attack compromised the personal data of roughly 150,000 patients, and all five hospitals operated by Scripps Health faced significant limitations on their ability to provide care. With their data-sharing systems offline, hospital staff had to use paper records. Patients requiring emergency care had to be diverted to other hospitals. Not only did the attack cost Scripps Health a record $112 million in remediation costs and lost revenue,[1] but the diversion of patients to other facilities resulted in overcrowding and degraded care. A case study of the incident found that nearby emergency departments saw patient volumes spike along with “significant increases in … waiting room times, patients left without being seen, [and] total patient length of stay.” In short, the attack caused a “regional disaster.”[2]

The safe and efficient provision of health services is a matter of both personal safety and national security, yet the healthcare and public health sector has suffered more ransomware attacks than any other critical infrastructure sector (*Getty Images/ 123RF*).

Local healthcare providers are not the only ones threatened by cyberattacks. In February 2024, a ransomware attack on healthcare payment processor Change Healthcare disrupted payments to providers across the country for weeks.[3] The disruption affected patient care at almost three-quarters of all hospitals, and more than half reported a significant or serious financial impact.[4] An impact of this magnitude can threaten national security.

The frequency of cyberattacks against the healthcare and public health sector has increased rapidly since the onset of the COVID-19 pandemic. Ransomware in particular has become the biggest threat.[5] Ransomware attacks can block access to electronic patient records, databases, and equipment, creating a higher incidence of patient mortality and morbidity in otherwise treatable circumstances.[6] Rural hospitals face a particularly high risk.[7] Such facilities face more financial constraints, leaving them with insufficient funding to invest in cybersecurity.[8] Patients relying on these hospitals are at greater risk of complication if a cyberattack occurs, as alternative hospitals tend to be farther away than their urban or suburban counterparts.

The safe and efficient provision of health services is a matter of both personal safety and national security. This is why the federal government designated the healthcare and public health sector as a critical infrastructure sector. The U.S. government must collaborate with stakeholders in this sector to increase providers’ resiliency against cyberattacks.

This report provides 13 recommendations directed at the executive branch, Congress, and the healthcare sector to guide the sector into a safer, more resilient future. Industry must invest more in cybersecurity, including by properly resourcing security teams, implementing organization-wide cyber hygiene training, and developing contingency response plans for destructive cyberattacks. The executive branch must update its strategy for the sector, provide roadmaps to secure key lifesaving services, incorporate stakeholder feedback on cybersecurity goals, and address the rural cybersecurity workforce gap. Finally, Congress should fund relevant executive agencies and programs so they can better support the sector. These recommendations are not exhaustive but serve as a starting point to address the pervasive cybersecurity issues facing the sector. The health and welfare of the American people depend on it.

Overview of Healthcare Cyber Challenges

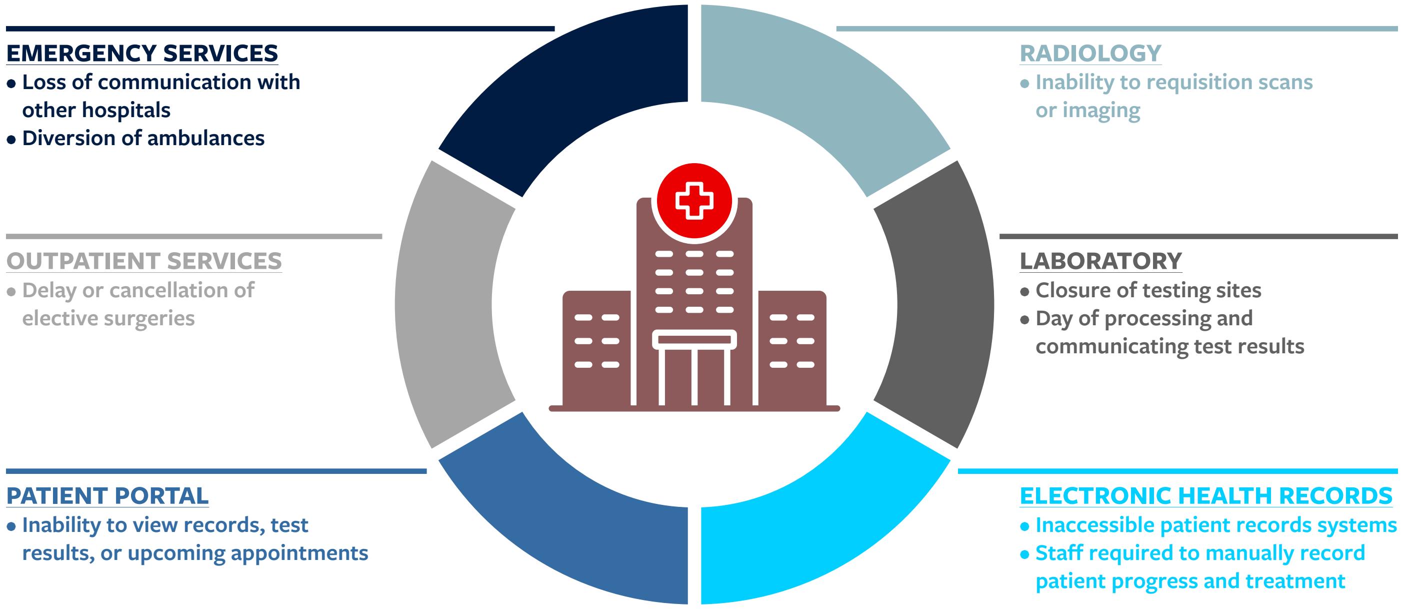
Healthcare providers across the country have long suffered from financial difficulties, resource constraints, staffing shortages, and capacity limitations. The proliferation of cyberattacks has exacerbated these issues while jeopardizing patient privacy and access to care.

The healthcare and public health sector faced significant financial struggles long before the ransomware epidemic revealed its frailty. In 2010, one-third of healthcare facility chief financial officers said their hospitals were in worse condition than 10 years prior, and half said their infrastructure was deteriorating faster than they could accrue the capital to improve it.[9] This deteriorating infrastructure compounds financial burdens. Waiting until aging systems fail before replacing them can cost significantly more than proactively replacing them.[10] The COVID-19 pandemic added to the financial burden, costing hospitals an estimated $323 billion in lost revenue in 2020 alone.[11] Because budgets are so tight and providers focus spending on core services, providers have underinvested in cybersecurity, rendering them vulnerable to attack.[12]

Stealing protected health information (PHI) can be lucrative. A single medical record can fetch up to $1,000 on the dark web.[13] PHI commands a high price since it includes not just names, email addresses, and credit card numbers but also medical conditions, health history, and insurance information — all of which criminals can use to commit fraud.[14] Hackers can also blackmail victims by threatening to release personal information, including psychiatric notes and evaluations.[15] Other criminals have used stolen information to file false police reports or otherwise harass patients to extort payments.[16]

Ransomware attacks have proven to be the most disruptive to the availability of healthcare services.[17] Ransomware is a form of malware that encrypts a victim's software, making any systems or files reliant on that software inoperable.[18] The attackers demand a payment in exchange for decryption although such decryption is not guaranteed. When a healthcare provider suffers a ransomware attack, patient files and data may become inaccessible, and medical devices may become unusable.

Figure 1: Types of medical systems that can be disrupted by ransomware attacks



EMERGENCY SERVICES
- Loss of communication with other hospitals
- Diversion of ambulances

OUTPATIENT SERVICES
- Delay or cancellation of elective surgeries

PATIENT PORTAL
- Inability to view records, test results, or upcoming appointments

RADIOLOGY
- Inability to requisition scans or imaging

LABORATORY
- Closure of testing sites
- Day of processing and communicating test results

ELECTRONIC HEALTH RECORDS
- Inaccessible patient records systems
- Staff required to manually record patient progress and treatment

Source: "Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm," Cybersecurity and Infrastructure Security Agency, page 12

Ransomware and data breaches are not always mutually exclusive. Hackers are often able to access patient PHI at the same time they freeze the provider's systems, allowing them to simultaneously extort the providers to deactivate the malware and blackmail patients directly by threatening to release their sensitive information.

The main threat posed by ransomware is the significant delay in patient care that can arise due to system or device shutdowns. A survey of medical organizations affected by ransomware attacks revealed that 36 percent saw more complications in medical procedures and 22 percent saw increased mortality rates.[19] Moreover, when ransomware shuts down medical systems and equipment, patients may need to be rerouted to alternative facilities, often farther away. Studies have suggested that even modest delays in emergency room admissions can result in an increase in patient mortality.[20]

Ransomware can also cause cascading problems for an entire region. Rerouting a large number of patients to other facilities may cause the receiving facilities to experience unexpected strains in bed capacity, supplies, and staffing. When multiple facilities face such strains, an entire region can suffer adverse health outcomes.[21] A study of medical facilities in Vermont showed that relative to their size, facilities in counties with hospitals hit by ransomware attacks experienced higher excess deaths than other counties.[22]

In fact, such studies likely undercount the human toll of ransomware attacks. Calculating the lives lost due to ransomware is hard because of the many confounding variables in emergency medical treatment. A death certificate will cite the medical ailment that directly caused the patient's death, such as a stroke or heart attack, not whether a healthcare worker's inability to access an electronic health record might have delayed or degraded care.[23] Medical complications and deaths can also occur weeks or months after the ransomware attack.[24] Experts believe that the quantity of patient deaths related to ransomware is likely much larger than what is directly reported.[25]

Despite the severity of the problem, healthcare providers are not investing enough in cybersecurity. Hiring and training adequate cybersecurity teams is expensive and difficult. Facing other financial constraints, many providers forgo IT staff completely.[26] To make matters worse, many healthcare providers rely on legacy systems whose outdated software or hardware no longer receives security updates from the manufacturer. In a 2021 survey, 73 percent of respondents reported using legacy operating systems.[27] These outdated, unpatched systems often have known and easily exploitable vulnerabilities. Maintaining legacy systems is costly in the long run but upgrading them often proves to be too expensive in the short run.[28]

Despite the severity of the problem, healthcare providers are not investing enough in cybersecurity. Hiring and training adequate cybersecurity teams is expensive and difficult. Facing other financial constraints, many providers forgo IT staff completely.

Another major challenge is hyper-connectivity, which increases vulnerability to cyberattacks. Hospitals have an immense convergence of information technology and operational technology systems across a plethora of devices.[29] For example, a hospital will have hundreds of medical devices, numerous computers for reviewing and updating medical records, water treatment facilities, electric systems, and building management technology. Each of these systems requires its own patches and updates to keep it secure, but many may be connected through a central network with little to no segmentation. This connectivity may improve efficiency and reduce cost but can present serious cybersecurity risks.[30] The industry-led Health Information Sharing and Analysis Center found that healthcare companies with more "connected medical devices experienced more cyberattacks."[31] If hackers manage to exploit the vulnerabilities of one device, they can gain access to any system on that unsegmented network. Hackers could hypothetically compromise a water purification system running unpatched software, navigate the unsegmented network, and access sensitive patient information.

For all these reasons, ransomware attacks are rising. The FBI's 2022 Internet Crime Report reveals that the healthcare and public health sector has suffered more ransomware attacks than any other critical infrastructure sector.[32] This is no accident. Cybercriminals usually choose victims with easily exploitable vulnerabilities and a high motivation to pay quickly.[33] Companies in this sector are not only poorly defended but are also more likely to pay the ransom demanded, as the stakes tend to be high — even life or death.[34]

Case Study: Change Healthcare Attack

The healthcare and public health sector is extremely interconnected, and the attack on Change Healthcare demonstrates how this leads to sector-wide fragility. Change Healthcare, a clearinghouse that acts as an intermediary in healthcare financial transactions, suffered a ransomware attack on February 21, 2024, forcing the organization to shut down all its systems. This made it impossible for healthcare providers and pharmacies reliant on Change to submit transactions. Insurance reimbursements and prescription processing ground to a halt, leaving providers without revenue streams for weeks.[35]

Change Healthcare, owned by UnitedHealth Group, the country's largest healthcare company by revenue, covers a massive network of 131 million patients and 67,000 pharmacies.[36] Prior to the ransomware attack, Change Healthcare processed 15 billion healthcare transactions annually. Without this crucial service, smaller practices lacking deep cash reserves were forced to make difficult decisions, furloughing workers or withholding wages and salaries.[37] According to an American Hospital Association survey, 94 percent of hospitals reported a financial impact, with more than half reporting a significant or serious impact.[38] One-third of hospitals had more than half of their revenue impacted.

This cyberattack did not just hurt providers. It also affected patients on a very personal level. Patients across the country saw delays in accessing all types of medications, from diabetes to antipsychotics.[39] Many patients had to go without medication or pay out of pocket, sometimes costing thousands of dollars. One nursing home had to close after the attack halted its ability to pay employees. Staff quit, and the facility shut down, forcing patients to rush to seek care at other facilities.[40]

As pressure from the industry and government grew, UnitedHealth Group loaned providers a total of $6.5 billion, which eligible providers do not have to repay until they determine their claims flows have returned to normal.[41] The Department of Health and Human Services (HHS) also offered accelerated Medicare and Medicaid payments to providers.[42] Following this program's rollout, Senator Mark Warner (D-VA) introduced a bill that would require organizations to meet basic cybersecurity standards to qualify for these advanced payments. The legislation highlights the growing concern in Congress that the healthcare sector may be neglecting cybersecurity but expecting the government to pick up the bill.[43]

This neglect occurs within the smallest providers and the largest. UnitedHealth Group's CEO confirmed during congressional testimony in May that hackers breached Change Healthcare via a client-facing portal lacking multifactor authentication — one of the simplest and most effective cybersecurity measures to implement.[44] The failure to implement such a simple safeguard compromised approximately one-third of Americans' health data, allowed hackers to extort $22 million from UnitedHealth Group, and forced the company to shut down its claims systems. The company reported that its core systems were back online in late March but noted that some auxiliary systems were still not operational.[45]

This attack demonstrates how targeting one critical cross-cutting company can affect healthcare providers nationwide. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recognizes that there are many such organizations, dubbed "systemically important entities," but Change Healthcare was not on the list. The attack's fallout caught the government off guard, prompting CISA Director Jen Easterly to emphasize that CISA needs to "sit down with the sector and with HHS, and really look at what we can do to better highlight those companies that are much more critical than we actually were expecting."[46]

Unique Challenges Facing Rural Hospitals

The fallout from ransomware attacks is greatest in rural hospitals. Rural hospitals make up 35 percent of all hospitals in the United States and serve roughly 14 percent of the population. These hospitals typically have lower patient volumes and service older, sicker, poorer, and uninsured populations with reduced ability to pay for necessary services.[47] These hospitals tend to run on extremely tight budgets, with 50 percent of rural hospitals operating at a loss.[48]

Most rural hospitals fall into the category of critical access hospitals (CAHs), meaning that they have 25 beds or fewer, are at least 35 miles from another hospital, and maintain 24/7 emergency services.[49] CAHs are essential for rural communities due to the communities' distance from other emergency medical care. Accordingly, CAHs receive cost-based reimbursement for Medicare services and other support from the federal government to reduce their financial burden.[50]

Nevertheless, rural hospitals continue to face significant financial challenges. Between 2010 and 2021, 136 rural hospitals closed.[51] Healthcare providers as a whole have experienced significant cost increases, especially since the COVID-19 pandemic. Labor, drugs, purchased services, and personal protective equipment have all gone up in price.[52] Rural hospitals are the least resilient to these changes. COVID-19 also created greater fluctuations in patient volumes and made it difficult for already struggling rural hospitals to pay their fixed costs, contributing to many closures.[53]

With fewer financial resources, rural hospitals are less prepared to prevent or react to ransomware attacks.[54] A 2019 study by the cybersecurity company RiskIQ found that small healthcare providers with under 500 employees suffered 70 percent of cyberattacks.[55] In June 2023, St. Margaret's Health in Spring Valley, Illinois, became the first hospital to attribute its closure directly to the costs accrued from a ransomware attack.[56] The ransomware attack shut down the hospital's computer systems for 14 weeks, which prevented the hospital from submitting insurance claims, leading to a financial crisis.[57]

Urban hospitals serving historically marginalized communities face many of the same financial constraints as rural hospitals.[58] These hospitals tend to have patient bases that are lower-income and more likely to be uninsured or covered by Medicare or Medicaid, which reimburse hospitals just 84 and 88 cents on the dollar for patient care, respectively.[59] However, the fallout from ransomware attacks may not be as severe for patients at urban hospitals, who can secure rapid transfers to other hospitals in the same urban area. By definition, CAHs face greater obstacles to transferring patients.

Current U.S. Government Efforts

Amid the proliferation of attacks on healthcare providers, the government and private sector have accelerated efforts to address the threat. Identified as critical infrastructure, the healthcare and public health sector collaborates with a federal agency partner known as a sector risk management agency (SRMA). SRMAs serve as a link between critical infrastructure providers and the federal government. They coordinate sector-specific issues with CISA, carry out incident management responsibilities, and provide, support, or facilitate technical assistance to identify and mitigate threats.[60]

HHS is the SRMA for the healthcare and public health sector. The Division of Critical Infrastructure Protection (CIP) within the Administration for Strategic Preparedness and Response (ASPR) acts as HHS's lead for critical infrastructure protection and is responsible for fulfilling the SRMA duties. CIP leads and organizes public-private partnerships within the sector and prepares for and responds to all threats, including cyberattacks.[61] One of the major benefits of housing the SRMA responsibilities within ASPR is that ASPR is not a regulator, so its primary goal is to help protect patient lives and assist the sector, not punishing providers for misconduct. ASPR also already acts as the department's incident response arm, which is a main duty of SRMAs.

HHS separately assigns regulatory enforcement responsibility to its Office of Civil Rights, which regulates compliance with cybersecurity standards relevant to the Health Insurance Portability and Accountability Act (HIPAA). In short, HIPAA requires entities with access to PHI to follow physical, network, and process security measures.[62] HIPAA applies to providers, health plans, clearinghouses, and all other covered entities. The Office of Civil Rights can impose financial penalties on entities that violate HIPAA regulations.[63] For minor HIPAA violations or cases where the offender has implemented cybersecurity best practices, the penalties are often relatively light. But they can be massive for large violations or in cases where the covered entity has purposefully neglected cybersecurity. After Chinese hackers breached a health insurance provider in 2015, resulting in the theft of PHI of almost 79 million people, the Office of Civil Rights levied a record $16 million fine.[64]

HIPAA enforcement has historically been one of the federal government's primary tools for pushing the industry to improve cybersecurity. While this is an important mechanism for holding businesses accountable for protecting patient privacy, the fear of regulatory action may discourage healthcare providers from reaching out to CIP for assistance in a cyber incident. More recently, therefore, HHS has attempted to use other mechanisms.

In December 2023, HHS released a four-pillar strategic concept paper to improve the cyber resiliency of the healthcare and public health sector.[65] First, HHS announced it would issue a series of voluntary healthcare-specific cybersecurity performance goals (CPGs), which HHS then published a month later.[66] These CPGs are designed to help the sector prioritize the implementation of the most important cybersecurity practices to better prevent, respond to, and recover from attacks.[67] In collaboration with CISA and industry partners, HHS adapted these 20 CPGs from CISA's 38 cross-sector CPGs, which serve as guidelines for small- and medium-sized businesses that may struggle to implement other, more complex cybersecurity frameworks.[68] To help healthcare organizations understand the relative importance of the 20 CPGs, HHS divided them into "essential" and "enhanced" categories. CPGs in the "essential" category serve as a floor to address common vulnerabilities and include goals such as instituting multifactor authentication and deploying encryption tools. CPGs in the "enhanced" category are meant to build on those basic steps. They include goals such as instituting penetration testing and network segmentation strategies.

Pillar two includes plans to provide resources and incentives for healthcare providers that adopt the voluntary CPGs. If funded by Congress, the program would provide upfront investments to under-resourced hospitals to institute essential CPGs. HHS also plans to provide an incentive program to all hospitals to implement "enhanced" CPGs. The HHS FY 2025 budget requests a notable $1.3 billion to kick off this program, with $800 million going to supporting "essential" CPGs and $500 million for "enhanced" practices. While the program is based on a sound premise, the $800 million for "essential" practices will not find its way to hospitals until FY 2027, and the money for "enhanced" practices will not arrive until FY 2029, according to the budget request.[69] As it stands, the program does nothing to address today's challenges and is little more than positive rhetoric.

More broadly, while the concept paper is a worthy start, HHS resourcing for SRMA duties has historically been inadequate for the size of the sector, which accounts for over 17 percent of the U.S. economy.[70] Within a nearly $2 trillion HHS budget, ASPR's cybersecurity funding dedicated to SRMA capabilities was only $708,000 as of 2023.[71] Last year, ASPR requested $7 million in funding to expand its capabilities for healthcare readiness and recovery. Some of those funds would go directly to CIP's SRMA duties.[72] According to a Government Accountability Office (GAO) report, HHS sought five additional full-time or equivalent positions — a significant increase over the current staff.[73]

While the concept paper is a worthy start, HHS resourcing for SRMA duties has historically been inadequate for the size of the sector, which accounts for 17 percent of the U.S. economy.

While ASPR houses and coordinates all SRMA duties for the sector, it does not directly execute all responsibilities or control all the resources associated with protecting the sector. For example, HHS's Health Sector Cybersecurity Coordination Center helps liaise with and disseminate cybersecurity information to the healthcare and public health sector. While the center coordinates with ASPR, it has its own budget, separate from ASPR oversight. Many other offices within HHS interact with ASPR in similar ways, decentralizing the SRMA model.

In March 2024, Congress appropriated FY 2024 funding for ASPR that enabled it to dedicate more manpower to a greater scope and scale of cybersecurity incidents in the sector. In March, ASPR requested an additional $5 million for CIP in its FY 2025 request, anticipating the growing need to expand its SRMA workforce and capabilities.[74] If funded by Congress, this increase will begin to resolve some of ASPR's historical under-resourcing.

With the exception of the CPG grant program, which is still years away from implementation, successive administrations and Congresses have done little to directly address the cybersecurity needs of rural hospitals. In May 2023, however, a bipartisan group of senators introduced the Rural Hospital Cybersecurity Enhancement Act.[75] The bill would have CISA develop a cybersecurity workforce development strategy for rural hospitals through collaboration with rural healthcare providers and relevant government agencies. The bill would also require CISA to make cybersecurity instruction materials available for rural hospitals to train staff on fundamental best practices. While the bill stalled in the Senate Committee on Homeland Security and Governmental Affairs, its bipartisan support, including from the committee's chairman, may provide it with a path forward in 2024.

Industry-Led Collaboration

The healthcare and public health sector has multiple associations and affinity groups. As it relates to cybersecurity and risk management, the two most important ones are the Health Sector Coordinating Council (HSCC) and the Health Information Sharing and Analysis Center (Health-ISAC).

The HSCC, alternatively known as the Healthcare and Public Health Sector Coordinating Council,[76] is the sector's chartered council, recognized by HHS. The body works with government partners to coordinate strategic planning and response efforts for cyber and physical threats to healthcare owners and operators.[77]

Within HSCC is its Cyber Working Group, composed of healthcare critical infrastructure owners and operators who produce much of HSCC's actionable content. The working group is responsible, in collaboration with HHS, for producing the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP).[78] HICP, first released in January 2019, is similar to HHS's new CPGs in that it provides 10 cybersecurity practices and risk mitigation strategies to reduce cyber risks.[79] Many of the best practices overlap with HHS's CPGs, and HHS ties each of the CPGs to related HICP guidelines for easy comparison.[80] These guidelines are voluntary and intended to be instituted at the preferred pace of individual organizations.

There are no fees to join HSCC's Cyber Working Group.[81] However, smaller, under-resourced, or independent hospitals not affiliated with a parent company may not have the necessary expertise or staff to benefit from joining the group. Without such participation, the unique perspectives and concerns of these kinds of hospitals may not receive sufficient attention within the HSCC group.

Owners and operators in the healthcare industry can also become members of Health-ISAC, which collaborates across the industry to share information on best practices for cyber incident prevention.[82] Health-ISAC disseminates threat information to its members to help them build more resilient systems and identify emerging threats.[83] While membership in Health-ISAC is not free, it is prorated depending on the annual revenue of the organization. For example, organizations with annual revenue over $100 billion pay a yearly membership fee of $95,000, whereas organizations bringing in less than $100 million pay $2,400 for the same membership.[84]

Recommendations

Healthcare providers' resiliency to cyberattacks is essential for the continuity of public health services. The solution to current gaps is not reactive regulation that seeks cybersecurity through compliance. Instead, the sector needs a proactive, collaborative approach. This effort should prioritize the security and operational resilience of systems most directly connected to patient care and bolster the capabilities of under-resourced industry stakeholders.

For the Executive Branch

Develop New, Long-Term Sector-Specific Cybersecurity Objectives

The last full-length strategy regarding hospital critical infrastructure protection by HHS was the Healthcare and Public Health Sector-Specific Plan of 2016.[85] While comprehensive at the time, the threat landscape has changed drastically. HHS released this strategy before the rapid rise of ransomware and emerging technology such as generative AI that malicious actors can exploit to further their attacks. HHS should extensively update this document to address new threats. Collaboration among HHS, healthcare providers, and organizations such as Health-ISAC and HSCC is vital to creating a robust strategy. HHS should seek out perspectives from a range of providers, diverse in size and location. This strategy should identify the new challenges the sector faces and create a detailed guide to help operators mitigate these risks.

Concurrently, HHS should continue to expand its efforts to provide simplified access points to cybersecurity resources, such as Health-ISAC and programs from HHS and CISA, as well as guidelines like the proposed strategy. This should help less-experienced healthcare providers quickly recognize and understand the resources available to them.

Work With Industry to Identify, Prioritize, and Secure Life-Saving Services

While securing the entire network within a hospital should be the goal, financial and workforce constraints will prevent many providers from implementing it immediately. In the meantime, hospitals should prioritize securing the life-saving services whose degradation would result in the highest risk to patients. Machines, network-connected equipment, and diagnostic tools needed in time-critical patient care should be identified and segmented from the rest of a provider's network. HHS should hold discussions with CISA, HSCC, healthcare providers, and cybersecurity firms to identify the most critical services and create a free roadmap for segmentation that is easily accessible on HHS's website. HHS should also design a resourcing program, funded by Congress, to help financially insecure providers implement the segmentation guidelines, similar to the program for instituting "essential" CPGs.

In addition, HHS should explore the feasibility and potential positive impacts of procuring and storing critical equipment in the Strategic National Stockpile. The existing stockpile is designed to facilitate a federal response in the case of a widespread disaster. HHS should assess whether the stockpile could store equipment, such as clinical diagnostics materials, that could be quickly deployed to help maintain critical operations in regions crippled by cyberattacks.[86]

Iteratively Update HHS's CPGs

The healthcare sector-specific CPGs are a step toward guiding the sector to take proactive cybersecurity measures. However, HHS should not just release and forget about these CPGs. HHS narrowed down the 38 cross-sector CPGs released by CISA to streamline the goals for the sector, but the efficacy of this alteration should be carefully monitored. HHS should continue to seek input from the sector, making sure the department receives feedback from healthcare providers of different sizes and locations. Should healthcare providers push back significantly on part or all of the CPGs, HHS should improve the CPGs. HHS should begin by requesting information on the CPGs' efficacy and adaptability on a yearly basis at first, then shift to a bi-annual basis after relative stabilization.

Accelerate the CPG Compliance Incentivization Program's Timeline

HHS must ensure that providers get the resources requested for CPG compliance as quickly as possible and that funds are not reappropriated in future budgets to non-cybersecurity priorities. Careful planning is essential to ensure the incentive program is effective, but this must not cause significant execution delays. HHS must prioritize this planning now and move up the start date of the incentive program to FY 2025.

Create a Rural Hospital Cybersecurity Workforce Development Strategy

As discussed, rural hospitals often struggle to afford dedicated, well-trained cybersecurity teams, leaving the hospitals more vulnerable to attacks. For some providers, even managed IT service providers may be financially unobtainable. HHS should organize a collaborative effort with rural hospitals and industry leaders to determine how best to address the cyber workforce gap in rural hospitals. This effort should explore ideas such as sharing IT teams across a region and migrating data to secure cloud storage providers. Congress should fund HHS to conduct relevant pilot programs. Different solutions should be tested for rural hospitals experiencing significant financial constraints, and an assessment of these solutions should determine how deeply HHS should become directly involved in helping rural hospitals build cybersecurity capacity.

Reassess Systemically Important Entities List

Consequential cyberattacks like the one on Change Healthcare are bound to happen again. CISA and HHS should review and update the list of "systemically important entities" to ensure better preparedness and response when another cross-cutting organization is impacted.

For Congress

Ensure SRMA Resources and Organizational Structure Are Optimally Efficient

Congress should direct GAO to conduct and publish a one-time audit of HHS's resources dedicated to SRMA roles and responsibilities. As discussed, ASPR houses and coordinates HHS's SRMA functions but is not directly responsible for all SRMA tasks and does not receive all SRMA-related resources. The GAO should determine if this diffuse structure is optimal or whether all SRMA funding should be centralized under ASPR. If GAO determines the SRMA structure contains inefficiencies that negatively impact the sector, it should provide recommendations to Congress and HHS on how to allocate and consolidate resources and responsibilities more efficiently.

Increase Funding for HHS's SRMA Capabilities

HHS's funding to help the healthcare sector secure itself is insufficient. HHS has requested additional resources to expand its workforce and capabilities dedicated to incident response and mitigation. It is critical that Congress approve this request. HHS cannot accomplish its goals without the required appropriations and manpower.

Fund HHS's CPG Resourcing and Incentive Program

Many rural and under-resourced hospitals do not have the budget to invest in basic cybersecurity best practices. A grant program specifically targeted at improving the sector's cybersecurity could help significantly. Congress should work with HHS to determine the scope and size of such a program. Along with the funding, Congress should mandate an annual impact report to determine if the program is being adequately utilized or if more work is needed.

Direct and Resource HHS to Establish a Rural vCISO Pilot Program

Chief information security officers (CISOs) are executive-level security professionals who address forward-thinking concerns such as risk posture, mitigation strategies, IT program construction, and educated budgeting know-how. By virtue of holding an executive-level position, they can air concerns directly to other senior executives. While CISOs can provide invaluable expertise to hospitals, many underfunded hospitals may not be able to afford a full-time CISO.

To help critical access hospitals improve their cybersecurity, Congress should fund and direct HHS to create a pilot program that provides part-time CISOs, called "fractional CISOs" or "virtual CISOs" (vCISOs), to help the most vulnerable and underfunded rural hospitals. This program should target hospitals that are most critical to their community and have the lowest profit margins. This program should assess the benefits of vCISOs for cybersecurity practices at rural hospitals, taking inventory of their cybersecurity capabilities and resiliency before and after the program. Should the pilot program show positive results at relatively low costs, it can be expanded.

For Industry

Spend More on Cybersecurity

Cyberattacks can threaten patients' lives, and the healthcare sector must start treating them as lethal threats. Cybersecurity has become just as critical to ensuring patient care as other mandatory expenditures such as infection control or air quality assurance. Healthcare providers must ensure that they allocate funding for a robust team of cyber professionals to prevent and react to cyber incidents.

Many independent, under-resourced hospitals lack the means to hire an appropriate cybersecurity team or even a single IT professional. Luckily, many part-time cybersecurity options exist. Managed IT service providers are third-party vendors that outsource IT management to numerous companies.[87] These vendors can be contracted on a part-time subscription basis, providing a set number of hours of IT support over a given period of time. This allows small businesses access to a team of professionals at a fraction of the cost of hiring multiple full-time IT staffers.

Upfront investments in cybersecurity, while burdensome in the short run, not only can save patient's lives but can be the difference between millions of dollars in lost revenue, mitigation expenses, and HIPAA enforcement penalties. With the rate and severity of cyberattacks on the healthcare sector increasing, healthcare providers have both an ethical and a financial responsibility to invest in cybersecurity.

Provide Cyber Hygiene Training to All Employees

Even with a robust cybersecurity team, employee mistakes or ignorance can still pose catastrophic risks. In fact, studies indicate that 91 percent of all cyberattacks begin with a phishing email — an email that appears to be legitimate but contains malicious links or instructions to install malware or give away personal information.[88] Cyber hygiene training can teach employees basic digital safety and allow them to recognize attempted scams or attacks. Many cyber hygiene training courses are free or relatively inexpensive and can prevent attacks that would otherwise cost providers millions of dollars or endanger patient lives or privacy. All employees should receive this training on a regular, recurring basis, which will vastly reduce the chance of a successful attack.

Develop Regional Contingency Plans for Healthcare Providers

Ambulance diversions can increase the chance of patient mortality, and hospitals scrambling to figure out the best course of action can compound these issues. Healthcare providers within the same geographic region should establish contingency plans for patient care in case of ransomware attacks. These plans could involve coordinating ambulance diversions and identifying hospitals with segmented and secure infrastructure to reduce the threat of systemic degradation and impact on patients when an attack does occur. Critical access hospitals, in particular, should receive special focus in the development of contingency plans.

Conclusion

Ransomware attacks against healthcare providers not only can inflict immense financial burdens but also lead to serious and deadly impacts on patient care. Cybercriminals have proven they are willing to put American lives at risk to make a quick buck, and they are unlikely to stop. Perhaps more worrisome, if opportunistic cybercriminals can cause significant harm to healthcare providers, more powerful foreign adversaries could wreak havoc if an opportunity presents itself. Until providers develop proactive cybersecurity practices and improve their resiliency to attacks, malicious actors will continue to exploit vulnerabilities. The federal government should utilize extensive public-private collaboration through HSS to strengthen healthcare providers' cyber resiliency and protect the health and safety of the people they serve.

Endnotes

1. Robert King, “May cyberattack cost Scripps nearly $113M in lost revenue, more costs,” *Fierce Healthcare,* August 11, 2021. (https://www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs)

2. Christian Dameff, Jeffrey Tully, Theodore C. Chan, Edward M. Castillo, Stefan Savage, Patricia Maysent, Thomas M. Hemmen, Brian J. Clay, and Christopher A. Longhurst, “Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US,” *JAMA Network Open*, May 8, 2023. (https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585)

3. James Rundle, Catherine Stupp, and Kim S. Nash, “Medical Providers Fight to Survive After Change Healthcare Hack,” *The Wall Street Journal Pro*, March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a)

4. “AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals’ Finances,” *American Hospital Association*, March 2024. (https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances)

5. Joel Witts, “Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know,” *Expert Insights*, February 9, 2024. (https://expertinsights.com/insights/healthcare-cyber-attack-statistics)

6. Ibid.

7. Kat Jercich, “Rural hospitals are more vulnerable to cyberattacks – here’s how they can protect themselves,” *Healthcare IT News*, September 8, 2021. (https://www.healthcareitnews.com/news/rural-hospitals-are-more-vulnerable-cyberattacks-heres-how-they-can-protect-themselves)

8. “Rural Hospital Closures Threaten Access: Solutions to Preserve Care in Local Communities,” *American Hospital Association*, September 2022, pages 3-4. (https://www.aha.org/system/files/media/file/2022/09/rural-hospital-closures-threaten-access-report.pdf)

9. Don D. King, Chad E. Beebe, Joan L. Suchomel, Peter L. Bardwell, and Vincent Della Donna, “A closer look at U.S. health care infrastructure,” *Health Facilities Management*, January 8, 2018. (https://www.hfmmagazine.com/articles/3239-a-closer-look-at-infrastructure)

10. Ibid.

11. “Hospitals and Health Systems Continue to Face Unprecedented Financial Challenges due to COVID-19,” *American Hospital Association*, June 2020, pages 1-2. (https://www.aha.org/system/files/media/file/2020/06/aha-covid19-financial-impact-report.pdf)

12. Nick Culbertson, “Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity,” *Forbes Technology Council*, June 7, 2021. (https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=78ed03945650)

13. Emily Skahill and Darrell M. West, “Why hospitals and healthcare organizations need to take cybersecurity more seriously,” *The Brookings Institution*, August 9, 2021. (https://www.brookings.edu/articles/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously)

14. “What is Protected Health Information?” *The HIPAA Journal*, accessed April 2, 2024. (https://www.hipaajournal.com/what-is-protected-health-information)

15. William Ralston, “They Told Their Therapists Everything. Hackers Leaked It All,” *Wired*, May 4, 2021. (https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach)

16. Jessica Lyons, “After injecting cancer hospital with ransomware, crims threaten to swat patients,” *The Register*, January 5, 2024. (https://www.theregister.com/2024/01/05/swatting_extorion_tactics)

17. Joel Witts, “Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know,” *Expert Insights*, February 9, 2024. (https://expertinsights.com/insights/healthcare-cyber-attack-statistics)

18. “Stop Ransomware,” *Cybersecurity and Infrastructure Security Agency*, accessed April 2, 2024. (https://www.cisa.gov/stopransomware)

19. Nicole Wetsman, “Hospitals say cyberattacks increase death rates and delay patient care,” *The Verge*, September 27, 2021. (https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients)

20. Simon Jones, Chris Moulton, Simon Swift, Paul Molyneux, Steve Black, Neil Mason, Richard Oakley, and Clifford Mann, “Association between delays to patient admission from the emergency department and all-cause 30-day mortality,” *Emergency Medicine Journal*, 2022. (https://emj.bmj.com/content/39/3/168)

21. Cybersecurity and Infrastructure Security Agency, “Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm,” September 2021, pages 6-8. (https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf)

22. Dale Peterson, “Josh Corman – Healthcare Security, SBOMs, & More,” *Unsolicited Response*, June 28, 2023. (https://dale-peterson.com/podcast-2)

23. Cybersecurity and Infrastructure Security Agency, “Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm,” September 2021, page 12. (https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf)

24. Maggie Miller, "The mounting death toll of hospital cyberattacks," *Politico*, December 28, 2022. (https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638)

25. Cybersecurity and Infrastructure Security Agency, "Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm," September 2021, pages 8 and 12-14. (https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf)

26. "Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods," *Risk IQ*, April 9, 2020, page 3. (https://www.riskiq.com/wp-content/uploads/2020/04/Ransomware-in-Health-Sector-Intelligence-Brief-RiskIQ.pdf)

27. "2021 HIMSS Healthcare Cybersecurity Survey," January 28, 2022, page 18. (https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf)

28. Bill Siwicki, "How best to manage, or dump, legacy healthcare IT systems," *Healthcare IT News*, March 2, 2023. (https://www.healthcareitnews.com/news/how-best-manage-or-dump-legacy-healthcare-it-systems)

29. Jill McKeon, "Operational Technology (OT) Security Risks, Best Practices in Healthcare," *TechTarget from Health IT Security*, June 16, 2022. (https://healthitsecurity.com/features/operational-technology-ot-security-risks-best-practices-in-healthcare)

30. Ibid.

31. "Current and Emerging Healthcare Cyber Threat Landscape," *Health-ISAC and Booz Allen Hamilton Cyber Threat Intelligence*, February 2023, page 7. (https://h-isac.org/wp-content/uploads/2023/03/Health-ISAC-Exec-Summary-Annual-Threat-Report_TLP-White-2023.pdf)

32. U.S. Federal Bureau of Investigation, Internet Crime Complaint Center, "Federal Bureau of Investigation Internet Crime Report 2022," March 2023, page 14. (https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)

33. "Current and Emerging Healthcare Cyber Threat Landscape," *Health-ISAC and Booz Allen Hamilton Cyber Threat Intelligence*, February 2023, page 3. (https://h-isac.org/wp-content/uploads/2023/03/Health-ISAC-Exec-Summary-Annual-Threat-Report_TLP-White-2023.pdf)

34. Andreja Velimirovic, "Ransomware in Healthcare: Stats and Recommendations," *Phoenix NAP*, March 16, 2023 (https://phoenixnap.com/blog/ransomware-healthcare)

35. James Rundle, Catherine Stupp, and Kim S. Nash, "Medical Providers Fight to Survive After Change Healthcare Hack," *The Wall Street Journal Pro*, March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a)

36. "2024 ranking of the global leading 10 Health care provider and services companies based on revenue," *Statista*, January 29, 2024. (https://www.statista.com/statistics/1373400/top-health-care-provider-and-services-companies-worldwide-by-revenue); James Rundle, Catherine Stupp, and Kim S. Nash, "Medical Providers Fight to Survive After Change Healthcare Hack," *The Wall Street Journal Pro*, March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a)

37. James Rundle, Catherine Stupp, and Kim S. Nash, "Medical Providers Fight to Survive After Change Healthcare Hack," *The Wall Street Journal Pro*, March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a); Jill McKeon, "Understanding the Impact of the Change Healthcare Cyberattack on Providers," *Health IT Security*, March 1, 2024. (https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers)

38. "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances," *American Hospital Association*, March 2024. (https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances)

39. Daniella Silva and Aria Bendix, "Patients struggle to get lifesaving medication after cyberattack on a major health care company," *NBC News*, March 6, 2024. (https://www.nbcnews.com/health/health-care/cyberattack-change-healthcare-patients-struggle-get-medication-rcna141841)

40. "Jefferson Hills care home abruptly closes, forcing residents to quickly find care at other facilities," *Pittsburgh Post-Gazette*, March 6, 2024. (https://www.post-gazette.com/business/healthcare-business/2024/03/05/jefferson-hills-healthcare-and-rehabilitation-center-closure/stories/202403050057)

41. Andrew Witty, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," *Testimony before the Senate Committee on Finance*, May 1, 2024. (https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next)

42. U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services, "Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers," March 9, 2024. (https://www.cms.gov/newsroom/fact-sheets/change-healthcare/optum-payment-disruption-chopd-accelerated-payments-part-providers-and-advance)

43. Healthcare Cybersecurity Improvement Act of 2024 Act, S.4054, 118th Congress (2023-2024). (https://www.congress.gov/bill/118th-congress/senate-bill/4054)

44. Andrew Witty, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," *Testimony before the Senate Committee on Finance*, May 1, 2024. (https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next)

45. Ibid.

[46] Jen Easterly, "Fortifying Cyber-Physical Resilience: Recommendations from the President's Council of Advisors on Science and Technology," *Speaking before the Foundation for Defense of Democracies*, March 13, 2024. (https://www.fdd.org/wp-content/uploads/2024/03/FDD_Event_FortifyingCyber-PhysicalResilienceRecommendationsfromthePresidentsCouncilofAdvisorsonScienceandTechnology_Transcript-1.pdf)

[47] "Rural Hospital Closures Threaten Access," *American Hospital Association*, September 2022, page 5. (https://www.aha.org/system/files/media/file/2022/09/rural-hospital-closures-threaten-access-report.pdf)

[48] "Unrelenting Pressure Pushes Rural Safety Net Crisis into Uncharted Territory," *Chartis*, February 2024, page 1 and 2. (https://www.chartis.com/sites/default/files/documents/chartis_rural_study_pressure_pushes_rural_safety_net_crisis_into_uncharted_territory_feb_15_2024_fnl.pdf)

[49] Paula Chatterjee, "Critical Access Hospitals Still Struggling," *University of Pennsylvania Leonard Davis Institute of Health Economics*, December 21, 2021. (https://ldi.upenn.edu/our-work/research-updates/critical-access-hospitals-still-struggling); "Critical Access Hospitals (CAHs)," *Rural Health Information Hub*, December 22, 2023. (https://www.ruralhealthinfo.org/topics/critical-access-hospitals)

[50] "Critical Access Hospitals (CAHs)," *Rural Health Information Hub*, December 22, 2023. (https://www.ruralhealthinfo.org/topics/critical-access-hospitals)

[51] "Rural Hospital Closures Threaten Access," *American Hospital Association*, September 2022, pages 3 and 5. (https://www.aha.org/system/files/media/file/2022/09/rural-hospital-closures-threaten-access-report.pdf)

[52] Ibid., pages 7 and 8.

[53] Ibid., page 8.

[54] Kat Jercich, "Rural hospitals are more vulnerable to cyberattacks – here's how they can protect themselves," *Healthcare IT News*, September 8, 2021. (https://www.healthcareitnews.com/news/rural-hospitals-are-more-vulnerable-cyberattacks-heres-how-they-can-protect-themselves)

[55] "Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods," *RiskIQ*, April 9, 2020, page 3. (https://www.riskiq.com/wp-content/uploads/2020/04/Ransomware-in-Health-Sector-Intelligence-Brief-RiskIQ.pdf); Jessica Davis, "Hackers Favor Small Hospitals, Health Centers as Ransomware Targets," *Health IT Security*, April 14, 2020. (https://healthitsecurity.com/news/hackers-favor-small-hospitals-health-centers-as-ransomware-targets)

[56] Alicia Hope, "Ransomware Attack Linked to Permanent Shut Down of Illinois Hospital St. Margaret's Health in Spring Valley," *CPO Magazine*, June 20, 2023. (https://www.cpomagazine.com/cyber-security/ransomware-attack-linked-to-permanent-shut-down-of-illinois-hospital-st-margarets-health-in-spring-valley)

[57] Tina Reed, "Hospitals could be one cyberattack away from closure," *Axios*, June 16, 2023. (https://www.axios.com/2023/06/16/hospitals-cyberattack-away-closure)

[58] Ashley Thompson, "New NORC Report Details Financial Pressures & Critical Role of Hospitals Serving Urban Communities," *American Hospital Association*, October 21, 2022. (https://www.aha.org/news/blog/2022-10-21-new-norc-report-details-financial-pressures-critical-role-hospitals-serving-urban-communities)

[59] "Underpayment by Medicare and Medicaid Fact Sheet," *American Hospital Association*, February 2022. (https://www.aha.org/system/files/media/file/2022/02/medicare-medicaid-underpayment-fact-sheet-current.pdf)

[60] "Sector Risk Management Agencies," *Cybersecurity and Infrastructure Security Agency*, accessed April 2, 2024. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies)

[61] "Critical Infrastructure Protection Division Structure," *Administration for Strategic Preparedness and Response*, accessed April 2, 2024. (https://aspr.hhs.gov/cip/Pages/Structure.aspx)

[62] Juliana De Groot, "What is HIPAA Compliance?" *Data Insider*, February 8, 2023. (https://www.digitalguardian.com/blog/what-hipaa-compliance)

[63] "What are the Penalties for HIPAA Violations?" *The HIPAA Journal*, accessed April 2, 2024. (https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096)

[64] U.S. Department of Health and Human Services, "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History," June 8, 2020. (https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach)

[65] U.S. Department of Health and Human Services, "Healthcare Sector Cybersecurity," December 2023. (https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf)

[66] Administration for Strategic Preparedness & Response, Press Release, "HHS Releases New Voluntary Performance Goals to Enhance Cybersecurity Across the Health Sector and Gateway for Cybersecurity Resources," January 24, 2024. (https://aspr.hhs.gov/newsroom/Pages/HHS-Releases-CPGs-and-Gateway-Website-Jan2024.aspx)

[67] Ibid.

[68] "Cross-Sector Cybersecurity Performance Goals," *Cybersecurity and Infrastructure Security Agency*, accessed April 2, 2024. (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

69. U.S. Department of Health and Human Services, "Fiscal Year 2025 Budget in Brief," March 2024, pages 82-83. (https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf)

70. "Historical National health expenditure data," Centers for Medicare and Medicaid Services, accessed April 2, 2024. (https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/historical)

71. Department of Health and Human Services, Administration for Strategic Preparedness and Response, "Justification of Estimates for Appropriations Committee," March 2023, page 137. (https://aspr.hhs.gov/AboutASPR/BudgetandFunding/Documents/FY2024/ASPR-cj.pdf)

72. Department of Health and Human Services, Administration for Strategic Preparedness and Response, "Justification of Estimates for Appropriations Committee," March 2023, pages 53 and 56. (https://aspr.hhs.gov/AboutASPR/BudgetandFunding/Documents/FY2024/ASPR-cj.pdf)

73. U.S. Government Accountability Office, "CRITICAL INFRASTRUCTURE PROTECTION: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities," February 2023, page 35. (https://www.gao.gov/assets/gao-23-105806.pdf)

74. "FY 2025 President's Request: ASPR Highlights," *Administration for Strategic Preparedness and Response*, accessed April 2, 2024. (https://aspr.hhs.gov/AboutASPR/BudgetandFunding/Pages/2025POTUS-budget-highlights.aspx)

75. Rural Hospital Cybersecurity Enhancement Act, S.1560, 118th Congress (2023-2024). (https://www.congress.gov/bill/118th-congress/senate-bill/1560/text)

76. "HPH SCC Cybersecurity Working Group: A Primer," *Healthcare & Public Health Sector Coordinating Councils*, March 26, 2024, page 1. (https://s3.amazonaws.com/amo_hub_content/Association618/files/HSCC%20Cyber%20Working%20Group%20Primer%20Webinar%20-%20March%202018.pdf)

77. "Sector Coordinating Council," *Administration for Strategic Preparedness and Response*, accessed April 2, 2024. (https://aspr.hhs.gov/AboutASPR/ProgramOffices/ICC/Pages/HPH/Sector-Coordinating-Council.aspx); "About, Health Sector Coordinating Council Cybersecurity Working Group," *Health Sector Coordinating Council*, accessed April 2, 2024. (https://healthsectorcouncil.org/about/health-sector-council-cyber-working-group-introduction)

78. Health Sector Coordinating Council Working Group, Press Release, "HHS and HSCC Release Voluntary Cybersecurity Practices for the Health Industry," January 2019. (https://healthsectorcouncil.org/hicp)

79. Jill McKeon, "Exploring the Health Industry Cybersecurity Practices (HICP) Publication, How to Use It," *TechTarget for Health IT Security*, February 27, 2024. (https://healthitsecurity.com/features/what-is-the-hicp-and-how-can-healthcare-use-it-to-strengthen-cybersecurity)

80. "HPH Cybersecurity Performance Goals," *Department of Health and Human Services*, accessed April 2, 2024. (https://hphcyber.hhs.gov/performance-goals.html)

81. "Membership In The Healthcare Sector Coordinating Council Cybersecurity Working Group," *Health Sector Coordinating Council Cybersecurity Working Group*, accessed March 28, 2024. (https://healthsectorcouncil.org/about/join)

82. "Health-ISAC Membership Offers Significant Benefits," *Health-ISAC*, accessed March 28, 2024. (https://h-isac.org/membership-account/join-h-isac); "Home," *Health-ISAC*, accessed March 28, 2024. (https://h-isac.org)

83. "Health-ISAC Frequently Asked Questions," *Health-ISAC*, accessed March 28, 2024. (https://h-isac.org/h-isac-faq)

84. "Health-ISAC Membership Offers Significant Benefits," *Health-ISAC*, accessed March 28, 2024. (https://h-isac.org/membership-account/join-h-isac)

85. Cybersecurity and Infrastructure Security Agency and the Department of Health and Human Services, "Healthcare and Public Health Sector-Specific Plan," May 2016. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf)

86. "Strategic National Stockpile," *U.S. Department of Health and Human Services Administration for Strategic Preparedness & Response*, accessed April 2, 2024. (https://aspr.hhs.gov/SNS/Pages/default.aspx)

87. Geoffrey Willison, "What are managed IT services?" *ConnectWise*, January 23, 2024. (https://www.connectwise.com/blog/managed-services/what-is-managed-it-services)

88. "91% of all cyber attacks begin with a phishing email to an unexpected victim: 8 simple practices towards cyber-resilience," *Deloitte*, January 9, 2020. (https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html)

About the Authors

Michael Sugden is a research analyst and editorial associate at FDD's Center on Cyber and Technology Innovation, where he works on issues related to nation-state cyber threats, critical infrastructure protection, and U.S. cybersecurity policy.

Annie Fixler is the director of the FDD's Center on Cyber and Technology and an FDD research fellow. She works on issues related to cyber-enabled economic warfare, the national security implications of cyberattacks on economic targets, and U.S. cyber resilience.

ACKNOWLEDGEMENTS

The authors would like to thank the experts in industry and government who provided invaluable perspective and feedback during the research and writing process. Their input was integral in forming the paper's analysis and conclusions, and the final report would have truly been disadvantaged without them. While many experts helped refine the report, any errors in fact or judgment are ours alone. We are especially grateful to John Hardie and David Adesnik for their rigorous edits and to Daniel Ackerman and Erin Blumenthal for the design and production of this report.

Cover Photo: The safe and efficient provision of health services is a matter of both personal safety and national security, yet the healthcare and public health sector has suffered more ransomware attacks than any other critical infrastructure sector (Getty Images/ 123RF).

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partner

FDD

CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission