Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks

On the Edge

Cybersecurity Health of America's Resource-Constrained Health Providers Findings and Recommendations

May 2025

Table of Contents

Introduction

Successful cyber attacks on the healthcare system are now commonplace, demonstrating repeatedly the hard reality that "it is not if but when" the next cyber attack on a healthcare entity exposes personal health information, disrupts clinical care or halts business operations. Just a few statistics compiled by The HIPAA Journal and other surveys reveal the scope of crisis:

- The HHS Office for Civil Rights data breach web portal shows 725 data breaches of 500 or more records in 2024, the third consecutive year that more than 700 large data breaches have been reported to OCR.
- Hacking and IT incidents accounted for the majority of breached records, with at least 259 million healthcare records exposed across those incidents.
- Breached healthcare information is up to 50 times more valuable than financial information.
- Thirty-six percent of healthcare facilities reported increased medical complications due to ransomware attacks.
- More than three-fourths (74%) of ransomware attacks were aimed at hospitals and 26% at secondary institutions like dental services and nursing homes.
- Fifty-eight percent of the 77.3 million individuals affected by data breaches in 2023 were due to an attack on a healthcare third-party provider — a 287% increase compared to 2022.
- Healthcare is the industry worst affected by this, with the highest volume of third-party breaches, followed by financial services.
- Just 14% of healthcare organizations say their IT security teams are fully staffed. Over half say they need more help, and 30% say they are understaffed or severely understaffed.

These challenges hit Resource-Constrained health providers – rural, critical access hospitals, FQHCs, post-acute care, physician practices, and many others – disproportionately, as they do not have the cross-enterprise trained staff, health IT infrastructure, the funding or the expertise to manage ongoing and evolving cyber threats against their health systems. And while the biggest concern has traditionally been about the number of personal health information exposed by these attacks, the existential threat has evolved to the disruption of actual patient care and the likelihood that a ransomware or other disruptive attack could result in patient harm or death.

Cybersecurity defenses have grown in larger healthcare organizations, but the nation's small, rural, Resource-Constrained healthcare facilities' cyber programs are lagging for a variety of reasons:

1. Insufficient and/or inflexible funding
2. Multiple legacy systems that are outdated and are not certified, hosted, and maintained by trusted partners
3. Inability to attract and retain cybersecurity talent
4. A wide range of competing priorities diverting resources
5. Lack of a formal security program
6. Inadequate or insufficient governance, especially at the state/local/tribal level
7. Abundance of conflicting government requirements, recommendations and guidance
8. Lack of clear and immediate receipt of alerts with guidance on remediation
9. Insufficient development/training/exercising of identification and response to attack.

10. Limited support to fund collaboratives where such providers would be able to leverage economies of scale, shared expertise, and drive efficiencies with limited funding.

These problems are further exacerbated by the following facts:

1. Rural and Resource-Constrained facilities are part of our nation's critical healthcare infrastructure: It is geographically impossible to divert patients during an attack without creating significant patient safety concerns due to the distance patients would need to travel to the next available facility.
2. Small and rural facilities are in some cases connected to larger healthcare institutions and can be the path of least resistance for cyber attackers.
3. Cyber criminals are beginning to focus on small facilities knowing that their defenses are not as robust as larger organizations and that they have at least some cyber insurance to cover losses that are paid out to cyber criminals.
4. At the same time Resource-Constrained facilities are benefitting from broadband access, telehealth and electronic records, greatly expanding their undefended attack surface.
5. AI promises to rapidly transform care delivery, but Resource-Constrained communities that adopt such tools face new cyber vulnerabilities—increasingly sophisticated attacks.

Policymakers are Paying Attention

Meanwhile, increasing awareness among the public and policymakers about these developments is resulting in increasing pressure on health systems to shore up their cyber defenses – to protect patients, data, operational continuity, and liquidity.

With the expectation that new cybersecurity may be forthcoming, the Health Sector Coordinating Council Cybersecurity Working Group launched in June 2024 an outreach to the nation's Resource-Constrained provider community to gather their views about: cyber threats and their relationship to patient safety and operational resiliency; management structures and routines for cyber preparedness; workforce challenges and resource constraints; and ultimately, what they would consider meaningful support from the government for compliance with new stringent cyber regulations.

This white paper summarizes the answers to these and other questions from almost 40 Resource-Constrained provider executives from 12 categories of "Resource-Constrained" providers in 26 states and offers recommendations from those providers to government and community partners to facilitate their preparedness, incident response, and compliance with cybersecurity rules.

About the Health Sector Coordinating Council Cybersecurity Working Group

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) is a government-recognized critical infrastructure industry council of more than 460 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The JCWG membership collaboratively develops and publishes free healthcare **cybersecurity leading practices** and policy

recommendations, and produces outreach and communications programs emphasizing the imperative that ***cyber safety is patient safety***.

Executive Summary

General Findings

Common themes among the interviewees showed perhaps a general awareness and sensitivity to the challenges and requirements of good cyber security management, and a clear recognition of the relationship of cyber safety to patient safety and trust, operational continuity, liquidity, and board oversight. Respondents offered numerous recommendations for how their cybersecurity capabilities can be better served by both government and community assistance.

Perhaps the most repeated recommendation for support was based on the assurance by most interviewees that they "know what to do" to secure their enterprise, but they simply don't have the workforce capacity to do it, and thus the most material support they could receive would be externally provided personnel on a routine, part time basis to assist in basic and more advanced cybersecurity management. A service like this could involve a variety of methods or business models that would be sustainable over time, such as: a larger regional health systems donating security personnel once or twice a week; government-funded deployment of contracted managed security services providers (MSSPs) to health systems that subscribe to the service; a dedicated "Cyber Corps" program administered by state governments or their National Guard units; and others.

Additionally, non-profit health IT collaboratives allow providers in rural and Resource-Constrained providers to leverage economies of scale, reduce costs, and maintain operational continuity during crises. They accomplish this by supporting shared infrastructure to reduce duplicative costs, further shared learnings, and drive rapid cycle learning. In short, without the necessary workforce and secure health IT infrastructure, Resource-Constrained providers are left knowing how to implement cybersecurity best practices—but without the means to do it.

Reimbursement as an incentive model for better cybersecurity also attracted some nods from interviewees, such as CMS providing a "meaningful use"-like funding model involving incentive payments to health systems that can demonstrate deployment of recognized cybersecurity practices such as Health Industry Cybersecurity Practices and NIST Cybersecurity Framework. This concept was enshrined in Public Law 116-321, as a way to direct OCR to accommodate breached entities with potentially less draconian fines and audits in a HIPAA enforcement action if the entity was able to demonstrate implementation of HICP, NIST or other recognized security practices. Funding is vital to develop the workforce and invest in health IT, but existing pathways and reimbursement incentives are insufficient and inflexible.

Lower on the list of assistance priorities expressed by interviewees were: 1) Grants – which are competitive and uncertain one-time restricted expenditures, and costly to apply for and administer; and 2) Training, which relates back to the recognition that they don't need training but people.

Other recommendations follow.

Recommendations

- Unregulated third-party technology and service providers represent both a major threat vector and costly third-party risk management demands. Health providers should not bear sole burden for policing their vendors; such third parties must be held to an enforceable higher cybersecurity standard when they support critical healthcare infrastructure where lives are at risk.
- Workforce augmentation for needed cybersecurity skills should be funded at the federal level through ongoing commitment of CISA technical support programs, and at the federal and state levels for subsidizing the use of contracted managed security providers, academic institutions' deployment of student engineers and cybersecurity majors in programs such as the Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/); state national guard assistance for cybersecurity incident response, and other programs.
- CMS reimbursement incentives can be helpful, but there may be hesitancy among some providers when money is tied to compliance. CMS should create specific billing codes for such cybersecurity imperatives as staff training. Because Resource-Constrained providers often have negative margins, making cybersecurity a reimbursable expense is paramount so that providers can afford the adoption of cybersecurity best practices. Workforce challenges are due, in part, to a resource constraint problem.
- Continuation and expansion of the U.S. Department of Agriculture's Rural Loan Program, which supports rural entities such health providers with various forms of cybersecurity support:
  - Funding equipment, software, and infrastructure
  - Securing Rural Development's portfolio through managing risk to healthcare facilities
  - Potential technical assistance provider
  - Conduit to rural community leaders and health care providers to share information and resources
- One-time grant support payment would not be enough and generally cannot be used for hiring. Grant programs should be tailored to specific needs for Resource-Constrained health providers and should be ongoing as part of payment structure. They should allow grantees to use funds to hire staff or participate in non-profit health IT collaboratives that provide cost-effective and scalable solutions for cybersecurity and artificial intelligence readiness.
- Regulatory and technical training for IT staff
- Assistance from affiliated health systems
- Access to GSA schedule pricing for cyber expenditures
- Easily accessible library of best practices for healthcare cybersecurity management

The HSCC also supports cybersecurity policy recommendations offered by the National Rural Health Association in 2024.

Project Overview: Structure of the Resource-Constrained Provider Cybersecurity Interview Series

A special task group of the Health Sector Coordinating Council Cybersecurity Working Group convened in the summer of 2024 to identify and recruit a sample of executives in Resource-Constrained provider facilities across the country to collect their views on cybersecurity and needed support. Interviews commenced in August 2024 and concluded in November 2024, involving weekly interviewees in most cases of 2 executives per one-hour video-conference session every week. All interviewees were identified according to the type of health provider they work for, health services they provide, sources of reimbursement, executive titles and other demographic information. All were then asked the same 12 conversational questions, giving the interviewees an opportunity to provide as much context and elaboration about their situations as they felt comfortable sharing.

This process did not involve a formal, broadcast survey, but conversational, qualitative research. This approach provided us more context to credible, consensus findings in research terminology: “saturation”. In qualitative research, "saturation" refers to the point where a researcher has collected enough data that no new themes, insights, or patterns are emerging, indicating that further data collection is likely unnecessary as the research has fully explored the topic and reached a point of completeness in understanding the phenomenon being studied; essentially, the data is "saturated" with information and no new significant details are being uncovered.

Definition of “Resource-Constrained”

For the purpose of this project and the scope of policy recommendations that may emerge from our findings, it was important to be as inclusive as possible in our identification of health providers that should be considered “Resource-Constrained.” Accordingly, we define “Resource-Constrained healthcare provider” as:

- A medical facility or individual practitioner encountering significant obstacles in providing comprehensive healthcare services and conforming to operation standards, often due to financial constraints, geographic isolation, or patient population characteristics. These constraints further impede the ability of Resource-Constrained health providers to implement, maintain, and enhance cybersecurity measures.

Resource-Constrained providers include providers located in rural or economically disadvantaged areas, small practices, community health centers, critical access hospitals, and facilities serving high-risk or special populations.

These providers typically face challenges such as limited financial resources, outdated or limited health IT, insufficient access to cybersecurity expertise and tools, and lower levels of regulatory oversight or support. Furthermore, these constraints are often compounded by a higher dependency on outdated technology and infrastructure, which increases vulnerability to cyber threats.

With this definition and profile, we further specified the types of Resource-Constrained providers we would include in our interviews to ensure a broad perspective of the challenges and approaches related to managing cybersecurity threats. Accordingly, our interviews involved the following categories of Resource-Constrained providers:

- CAH (Critical Access Hospital)
- Disproportionate Medicare/Medicaid dependence

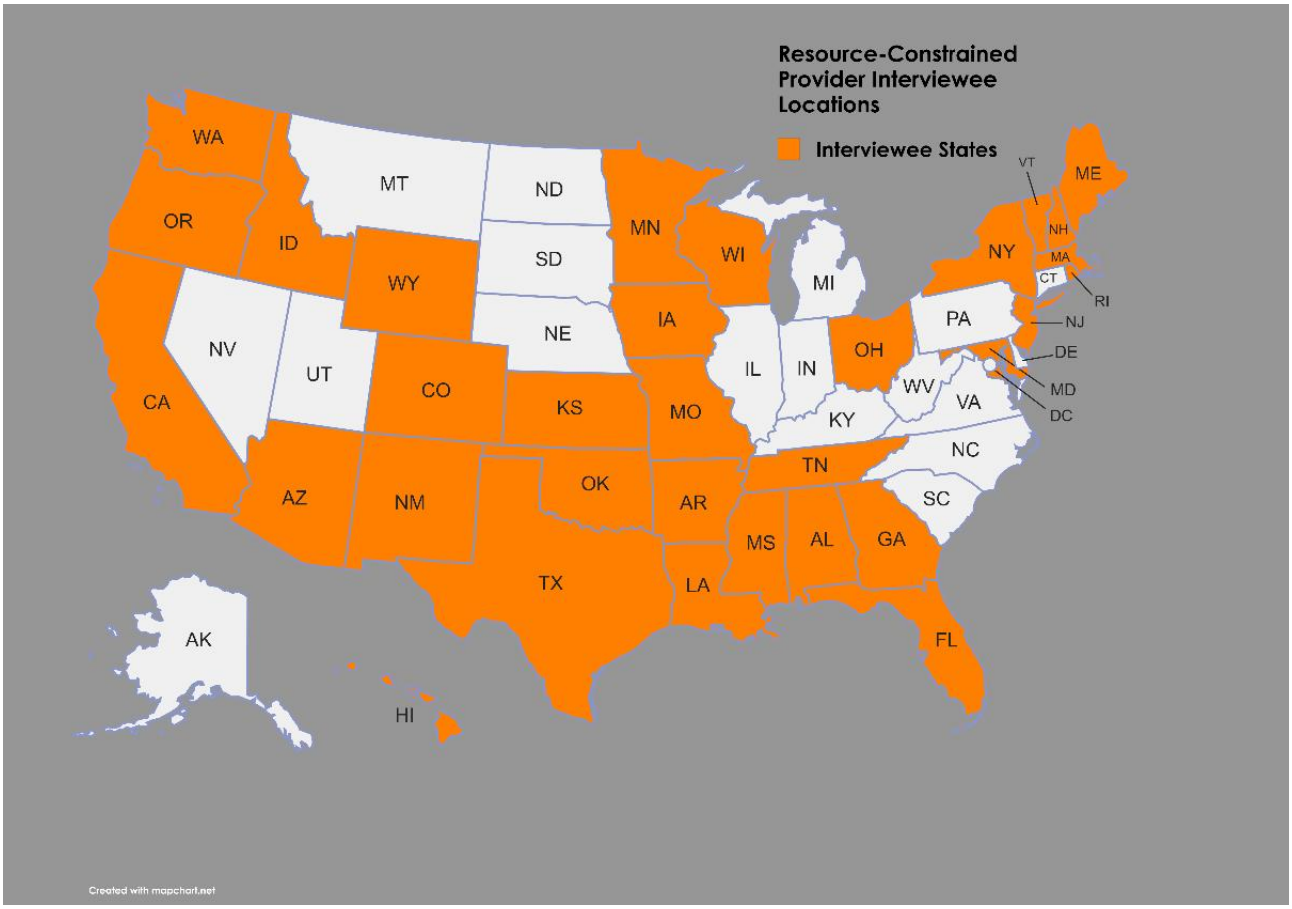
- FQHC (Federally Qualified Health Center)/ Look-Alike
- Free Clinic
- LTC (Long Term Care)
- Native American / Tribal / IHS (Indian Health Service)
- Regional Health System
- REH (Rural Emergency Hospital)
- RHC (Rural Health Clinic)
- SAMHSA (Substance Abuse and Mental Health Services Administration)
- Small Practice/Physician Practice
- SNF (Skilled Nursing Facility)

National Coverage

Between the August 1 commencement and November 14 conclusion of interviews,

42 senior executives of Resource-Constrained healthcare institutions were interviewed from 31 states:

Alabama
Arizona
Arkansas
California
Colorado
Florida
Georgia
Hawaii
Idaho
Iowa
Kansas
Louisiana
Maine
Maryland
Massachusetts
Minnesota
Mississippi
Missouri
New Hampshire
New Jersey
New Mexico
New York
Ohio
Oklahoma
Oregon
Tennessee
Vermont
Texas
Washington
Wisconsin
Wyoming



With a Broad Demographic Profile

- Frontier
- Rural
- Suburban
- Urban

Performing the following services

- Acute Care
- Ambulatory surgery
- Audiology
- Dental Services
- Emergency Care
- Genetic Counseling services

- Geriatric behavior health
- Long-term Care Provider
- Maternity
- Mental Health Services
- Occupational Therapy
- Oncology
- Pharmacy Services
- Physical Therapy
- Primary Care
- Specialty Care
- Speech Pathology
- Substance Use Disorder
- Urgent Care
- Urology

Interviewed Executive Titles / Responsibilities

- CEO / Lead Administrator
- Chief Operating Officer
- Chief Security Officer
- Chief Information Officer
- Chief Compliance Officer
- Chef Privacy Officer
- Information Security Officer
- Chief Nursing Officer
- Partner/Owner
- IT Director
- Physician/Nurse

Resource-Constrained Provider Institutions Interviewed

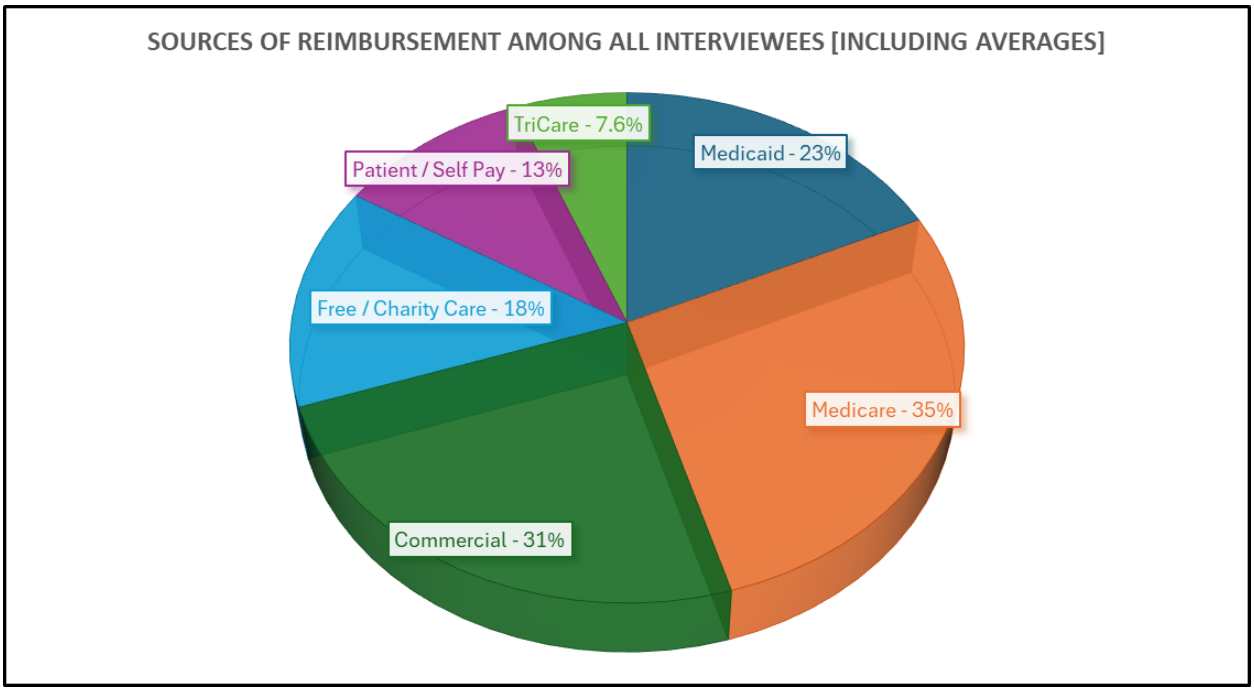
Adena Health System	Chillicothe, OH
Arbor Health	Morton, WA
Ben Archer Health Center	Dona Ana County, NM

CARTI	Little Rock, AR
Chapters Health	Temple Terrace, FL
Citizen's Hospital	Colby, KS
Columbia Basin Health Association	Othello, WA
Community Health Center of Cape Cod FQHC	Falmouth, MA
Downtown Clinic	Laramie, WY
Duncan Regional Health	Duncan, OK
Gifford Hospital	Randolph, VT
Ivinson Memorial Hospital	Laramie, WY
Jefferson Health	Philadelphia, PA
Lakewood Health System	Staples, MN
Lawrence County Medical Center	Montecello,MS
LSU Health Lallie Kemp Medical Center	Independence, LA
Lutheran-Jamestown	Jamestown, NY
Marshfield Clinic Health System	Marshfield, WI
Mason General Hospital	Shelton, WA
Monadnock Community Hospital	Petersborough, NH
Montgomery County Memorial Hospital	Red Oak, IA
Mount Desert Island Hospital	Bar Harbor, ME
National Association of Community Health Centers	Bethesda, MD
National Healthcare Corporation	Murfreesboro, TN
Newman Regional Hospital	Emporia, KS
Northeastern Vermont Regional Hospital	St. Johnsbury, VT
Northern Arizona Healthcare	Flagstaff, Arizona
OCHIN, Inc.	Portland, OR
Open Door Community Health Center	Humbolt, CA
Quality of Life Health Services	Alabama
Ray County Memorial Hospital	Ray County, MO
Regional Eye Associates	Cherry Hill, NJ

RiverSpring Living	Riverdale, NY
Rural Collaborative	Olympia, WA
Southwell	Tifton, GA
Southwest MS Regional Medical Center	McComb, MS
Tamarack Health	Hayward, WI
Trinity Rehab Services	St. Clairsville, OH
Urban Health Plan	Bronx, NY
Valley Regional Hospital	Claremont, NH
Winding Waters Community Health Center	Enterprise, OR

Sources of reimbursement among all interviewees included the following averages

- Medicaid 23%
- Medicare 35%
- Commercial 31%
- Free/Charity care 18%
- Patient/self pay 13%
- TriCare 7.6 %



Summary of Interviewees' Answers to the Cybersecurity Question-Set

1. Discuss how you consider cyber threats as they affect your organization. Do you consider the consequences of cyber-attacks to be a material risk to any of the following?

- **Cyber Threats and Risks**: Many respondents consider cyber threats to be a significant concern, affecting various aspects such as financial liquidity, patient safety, reputational damage, and legal jeopardy
- **Patient Safety**: The importance of patient safety is emphasized, particularly in relation to the impact of cyber-attacks on electronic health records (EHR) and clinical workflows.
- **Financial and Resource Constraints**: Financial liquidity and resource limitations, such as time and money, are highlighted as critical issues.
- **Trust and Relationships**: Building and maintaining trust and relationships are considered essential for the successful operation of healthcare facilities.
- **Legal and Regulatory Compliance**: Compliance with regulations such as HIPAA and the duty of care by the board are mentioned as important considerations.
- **Third-Party Support**: The reliance on third-party consultants and the importance of keeping them in good cyber shape are noted.
- Coupled with workforce skills limitation 2 or 5 people doing the work of 20

2. Who is responsible for your information/cyber security program? Do they regularly engage you and/or your board/executive management?

Answers revealed various approaches to information/cyber security programs across different organizations. A sampling of structures:

- Security reports to the IT Director who reports to the CEO. They have bi-weekly meetings with the CEO and daily updates. Monthly board cyber updates and annual education for the board about trends in the region and hospital.
- It's a shared responsibility among senior executives. Regular communication with senior management staff and twice a year with the board.
- Use a third-party service provider.
- Chief Digital Technologist: Reports to the CEO/Board. Monthly meetings on cybersecurity and ongoing communication on cyber issues.
- Cyber lead reports to the board, but the position reports to the CFO. Works with compliance on policies, third-party audits, and yearly work plans with the Compliance Committee that reports to the board.
- Regular briefings to the CEO who asks about spending. Reports to the board annually, usually the first topic.
- Role encompassing HIPAA security officer, reports to the safety/compliance team which reports annually to the board. Recently joined the fire and life safety team, led by the facilities group.
- All hospitals in system have an IT director. The Compliance Committee is one of the most active, with awareness that cyber needs to touch every component of the hospital.
- Virtual CISO Service: No formal team in-house, leveraging a virtual CISO service on a 2-day-a-week basis.
- Hired a fractional CIO and PMO for EPIC implementation. They run cyber, and the CEO meets with them weekly.
- Security officer on the executive leadership team, in compliance with rules, but it's not their full-time job.
- All nursing homes are required to have a security officer; however, not all enforcement auditors/examiners have the expertise to ask the right questions.
- Use a managed security service provider (MSSP) rather than hiring someone. Annual HIPAA security risk assessment, but has never been audited by HHS.
- Merit-based Incentive Payment System (MIPS) Certification: Conducts security risk analysis as part of the IPs certification.
- Board Updates: Shows the board the number of hits on the network, which occur every day, every hour.
- Compliance Reporting: Information security reports into Compliance.

3. How does your organization identify and prioritize cybersecurity risks?

Responses highlight various approaches to identifying and prioritizing cybersecurity risks within organizations:

- **Risk Identification and Prioritization:**

  - Cybersecurity is identified as the number one risk by the board1.
  - Organizations conduct annual penetration tests and monthly vulnerability scans by third parties.
  - Data is registered in a risk registry.
  - Participation in Infragard and communication with CISA representatives1.
- **Access and Compliance:**
  - Limiting access and following HIPAA guidelines.
  - Ensuring outside providers comply with these guidelines.
- **Insurance and Communication:**
  - Maintaining a good relationship with cyber insurance firms.
  - Educating team members about cybersecurity hygiene.
- **Technological Measures:**
  - Utilizing third-party vendor tools, patch management, EDR technologies, and firewalls6.
  - Conducting phishing tests and exfiltration tests.
- **Risk Assessment and Management:**
  - Annual risk assessments with third-party assistance, especially for HIPAA compliance.
  - Table-top exercises to bring operations on board.
  - Formal risk management plans with regular IT team meetings.
- **Sources and Monitoring:**
  - Monitoring CISA and vendor announcements for potential threats.
  - Using internal telemetry, MDM scanning, vulnerability scanning, and CMDB.
- **Additional Measures:**
  - Privileged access management (PAM) and resetting administrator access privileges after each session.
  - Exercising outages, backup, and recovery.
  - Using ServiceNow platform.

4. Which cybersecurity risk mitigation strategies do you employ, including proportionally on any of the following:

a) Cybersecurity technology/tools

b) Cybersecurity Services (e.g., penetration testing, red-teaming, V-CISO, exercises, risk assessment, monitoring, etc. - internal or outsourced?)

c) Cybersecurity Staff

d) Governance, Risk & Compliance platform

e) Business Resiliency

f) Employee Training

g) Cybersecurity Insurance

- **Cybersecurity Technology and Tools:** Many responses mention the use of various cybersecurity technologies and tools, such as managed detection and response (MDR), IT routers, and network monitoring tools like Darktrace.
- **Cybersecurity Services:** There is a significant emphasis on utilizing cybersecurity services, including penetration testing, red-teaming, virtual CISO (V-CISO), risk assessments, and monitoring. These services are often outsourced to external vendors.
- **Cybersecurity Staff:** A recurring theme is the challenge of staffing with dedicated cybersecurity personnel. Many organizations rely on help desk staff and cultivate workforce development to address this shortage.
- **Governance, Risk & Compliance (GRC):** Several responses highlight the importance of having a robust GRC platform to manage security compliance and risk assessments.
- **Business Resiliency:** Business resiliency and the need for effective backup and redundancy measures are frequently mentioned. Some organizations have extensive backup systems in place to ensure continuity.
- **Employee Training:** Employee training on cybersecurity awareness is a common strategy. Regular training sessions and awareness programs are conducted to keep employees informed about cybersecurity threats.
- **Cybersecurity Insurance:** Many organizations have cybersecurity insurance to mitigate financial risks associated with cyber incidents. However, obtaining and maintaining cyber insurance is becoming increasingly challenging.
- **Budget and Spending:** There is a notable focus on the budget allocated for cybersecurity. Organizations are spending a significant portion of their IT budget on cybersecurity measures, often ranging from 13% to 15%.
- **Medical device maintenance and replacement costs:** This topic came up less frequently than expected, perhaps suggesting a general lack of appreciation for the complexity of securing legacy devices and the cost of replacement as they age out of support to product end of life.
- These themes reflect the multifaceted approach organizations are taking to address cybersecurity risks, combining technology, services, staff training, compliance, and financial protection.

5. Do you feel you are spending an adequate amount on cybersecurity, and if not, what is preventing you from spending more?

- **Resource Constraints**: Many respondents mentioned the lack of time, money, and staff as significant barriers to improving cybersecurity. For example, two interviewees both highlighted the need for more resources to balance cybersecurity and patient care.
- **Balancing Cybersecurity and Patient Care**: Several respondents expressed the challenge of allocating funds between cybersecurity and direct patient care, mentioning the difficulty of prioritizing cybersecurity spending over patient care needs.
- **Support and Funding**: Some respondents noted that they have support from their boards or C-Suite for cybersecurity spending but still face challenges.

- **Legacy Systems**: The issue of outdated technology and legacy systems was a recurring theme. This refers to those medical devices and other technology that in some cases have outlived software support, updating and patching, and hence require costly and inefficient work-arounds and compensating controls to maintain functionality and security. Respondents mentioned that legacy systems, especially those regulated by the FDA, take up a significant portion of their budget and complicate cybersecurity efforts.
- **Benchmarking and Metrics**: There were mentions of using benchmarks and metrics to assess cybersecurity spending. However, respondents also pointed out that national benchmarks might not be suitable for smaller or Resource-Constrained organizations.
- **Insurance and Liability**: Some respondents discussed the role of cyber insurance and the need for better coverage. For instance, one mentioned the lack of cyber insurance in their practice and the potential benefits of having it.

6. How would you characterize your readiness for a significant cyber-attack that could disrupt patient care or other critical services and administrative functions?

- **Readiness for Cyber-Attacks:** Many respondents expressed concerns about their readiness for significant cyber-attacks. While some felt relatively prepared, others acknowledged gaps in their preparedness. For example, one interviewee mentioned that they were hacked once but managed to continue care despite the disruption. Similarly, another felt well-prepared but noted that financial freedom would enhance their readiness.
- **Impact of Past Incidents:** Several respondents shared experiences of past cyber incidents and their impact, with one pointing to a data breach that led to extortion of stolen data and another highlighting a two-month downtime due to a cyber incident.
- **Third-Party Vendor Concerns:** The reliance on unregulated third-party vendors and the associated risks were common concerns, with one saying third-party vendors keep him up at night, and another discussed the need to protect billing from disruption due to third-party events.
- **Medical device maintenance and replacement costs:** This topic came up less frequently than expected, perhaps suggesting a general lack of appreciation for the complexity of securing legacy devices and the cost of replacement as they age out of support to product end of life.
- **Backup and Recovery Plans:** The importance of having robust backup and recovery plans was emphasized, with two insisting on the need for backups right away.
- **Continuous Improvement and Training:** There was a recurring theme of continuous improvement and the need for regular training, exercises, and alliances.
- **Challenges with Staff Turnover:** Some respondents pointed out the challenges posed by staff turnover, which makes business and clinical continuity difficult.

7. Has your organization experienced any cybersecurity incidents or breaches in the past two years, and if so, how were they responded to?

- **Cybersecurity Incidents:** Several responses mention experiencing cybersecurity incidents or breaches. These incidents include third-party incidents, impending DDoS attacks, email breaches, and server vulnerabilities.
- **Response to Incidents:** The responses highlight various ways organizations responded to these incidents. Actions taken include removing affected servers from the network, inspecting by third parties, mitigating risks through EDR, and installing MFA after email compromises.
- **Preparedness and Challenges:** There is a recurring theme of preparedness and the challenges faced. Some responses indicate that organizations feel prepared on the technical side but are concerned about patient interface devices and the unpredictability of future attacks.
- **Third-Party Risks:** Many responses emphasize the risks associated with third-party suppliers and incidents originating from third-party vendors.
- **Communication and Coordination:** Some responses mention the importance of communication and coordination, such as setting time aside for incident response and business continuity/disaster recovery plans and ensuring appropriate people are included in these conversations.

8. How do you evaluate and manage third-party vendors and service providers cybersecurity risk?

- **Vendor Evaluation and Management**: Many organizations have processes in place to evaluate and manage third-party vendors and service providers. This includes using questionnaires, compliance checks, and requiring vendors to provide security reports like SOC 212345.
- **Cybersecurity Risk**: There is a strong emphasis on assessing and managing cybersecurity risks associated with third-party vendors. This includes categorizing and scoring security risks, monitoring vendors, and ensuring they comply with security standards.
- **Compliance and Accountability**: Organizations are focused on ensuring that vendors comply with legal and regulatory requirements. This includes having Business Associate Agreements (BAAs) and holding vendors accountable for any security breaches or vulnerabilities.
- **Challenges and Improvements**: Several responses highlight challenges in the vendor evaluation process, such as inconsistent practices, lack of information from vendors, and the need for better tools and processes. There is also a recognition that improvements can be made in how vendors are assessed and managed.
- **Collaboration and Support**: Some organizations collaborate with associations or other networks to evaluate vendors and share resources. This helps in leveraging collective knowledge and ensuring better vendor management.
- **Medical device maintenance and replacement costs**: This topic came up less frequently than expected, perhaps suggesting a general lack of appreciation for the complexity of securing legacy devices and the cost of replacement as they age out of support to product end of life.

9. Cyber Insurance:

a) *Are you fully covering your risk?*
b) *What % risk do you still carry?*
c) *What is the deductible?*
d) *What is included: ex: lost business operations, paying ransomware, OCR fines?*

- **Coverage Levels:** Many responses discuss the level of coverage provided by their cyber insurance policies. Some have increased their coverage limits, while others feel their coverage is inadequate. For example, one response mentions coverage of $3 million, which was later increased to $5 million.
- **Risk Retention:** There is a recurring theme of organizations carrying some level of risk despite having insurance. Some responses indicate that they are not fully covering their risk, with percentages of risk still carried ranging from 10% to 50%.
- **Deductibles:** The amount of deductible varies among the responses. Some have low deductibles, while others have higher deductibles. For instance, one response mentions a deductible of $60,000 while another mentions a deductible of $5,000.
- **Inclusions and Exclusions:** The types of incidents and expenses covered by the insurance policies also vary. Some responses mention coverage for lost business operations, paying ransomware, and OCR fines. Others indicate that certain aspects, such as litigation or operations lost, may not be covered.
- **Cost and Affordability:** The cost of cyber insurance and its affordability is another common theme. Some responses mention that the premiums are high, and they cannot afford higher coverage limits.

10. The US Government is proposing enhancements to the HIPAA Security Rule with specific mandatory cybersecurity management regulations on health providers: Do you believe these regulations, if supplemented with assistance from the government (options below), would be:

a) *Helpful to reducing risk to your organization while providing more clarity about compliance requirements, or*
b) *An additional, costly regulatory burden with uncertain benefit*
c) *Better applied to third party vendors/service providers rather than regulating the victim*
d) *Other*

- **Regulation and Compliance:**
  - Many respondents believe that the proposed regulations would be helpful in reducing risks and providing more clarity about compliance requirements.
  - However, there are concerns about the regulations being an additional, costly burden with uncertain benefits.
- **Third-Party Vendors:**
  - A recurring theme is the need for regulations to be applied to third-party vendors and service providers rather than just the healthcare organizations themselves.
  - There is a call for vendors to be held more accountable for cybersecurity measures.

- **Government Assistance and Funding:**
  - Many respondents emphasize the need for government assistance, grants, and subsidies to support the implementation of these regulations.
  - There is also a desire for more guidance and support from the government to help smaller organizations comply with the regulations.
- **Challenges and Concerns:**
  - Respondents highlight various challenges, such as the complexity and cost of applying for grants, the struggle to hire and retain qualified staff, and the need for clear and effective cybersecurity requirements.
  - Some express frustration with the current state of cybersecurity and the lack of specific guidance on how to conduct risk assessments.
- **Overall**, while there is support for the proposed regulations, there are significant concerns about the cost, implementation, and the need for third-party vendors to be held accountable. Government assistance and clear guidance are seen as crucial for the successful adoption of these regulations.

11. Financial Assistance: Please rate the usefulness and importance of the following options for government or industry financial assistance with your organization's cybersecurity, using a scale of 1-5, where 1 is "not useful/important at all" and 5 is "extremely useful/important:"

a) Grants
b) Subsidies
c) Reimbursement incentives
d) Tax incentives
e) Government assistance (e.g., CISA, HHS, FEMA)
f) Free trainings/Workforce Development
g) Other

The following compilation of answers is in raw format to give readers a sense of how concerns and ideas were expressed by interviewees.

- Problem with "Hammer" in cyber, is you're affecting patient access. Think of all the migrants coming into the country we now need to take care of.
- With dawning of AI, govt should be using it as a cyber protection tool, especially international ingress/egress
- Need to address unregulated third party technology and service vendors to improve their security when they connect to or are installed in health provider networks
- Funding for outsourced cybersecurity service providers
- Reimbursement incentives: nice, but financial folks would not like because money tied to compliance
- Staffing help or funding for partnering with MSPs; "manpower" and time would be the value to them
- *These 3 are the only things that will improve our posture:*

  - Grants
  - Subsidies
  - Reimbursement incentives
- Health plans to give positive incentives
- Reimbursement incentives would be welcome, but there is general concern about tying incentive to compliance
- USDA Grant continuation
- Billing code for staff training
- Grants: one-time payment would not be enough; wouldn't be used for hiring; that's what we need is someone on staff
- If you're not going to give positive incentives, then send money through those who can help.
- Ongoing support preferred, as part of payment structure; something you don't have to apply for.

12. Specific Assistance: Please rate the usefulness and importance of the following factors to your organization, using a scale of 1-5, where 1 is 'not useful/important at all' and 5 is 'extremely useful/important.

The following compilation of answers is in raw format to give readers a sense of how concerns and ideas were expressed by interviewees.

a) Infrastructure/technology upgrades for cybersecurity
b) Funding for outsourced cybersecurity service providers
c) Regulatory and technical training for IT staff
d) Communities of interest (e.g., information sharing analysis organizations)
e) Assistance from affiliated health systems
f) Cyber insurance company support
g) Basic cybersecurity training for administrative and clinical staff
h) Easily accessible library of best practices for healthcare cybersecurity management
i) Other (grant writing, grant management, etc.)

- Funding for outsourced cybersecurity service providers
- Regulatory and technical training for IT staff
- Assistance from affiliated health systems
- Funding for outsourced cybersecurity service providers would be fantastic
- Having access to GSA schedule pricing for cyber expenditures would be helpful
- Easily accessible library of best practices for healthcare cybersecurity management
- Funding for outsourced cybersecurity service providers – if government took the liability off of us with, say, regional security officers.

- Basic cybersecurity training for administrative and clinical staff; private insurance should have a role to play; need standardization among the payers for a way of incentivizing. They're also funding EHR upgrades.

Resource-Constrained Cybersecurity Alignment with Health Sector Council Strategic Objectives and Government Recommendations

Health Industry Cybersecurity Strategic Plan

The HSCC CWG, our government, and health sector partners are united in our call to action to coalesce around the principle that cyber safety is patient safety and make the appropriate investments in the people, processes, technology, and partnerships to strengthen the sector against – and weaken the effectiveness of – cyber threats.

In 2024 the HSCC published the Health Industry Cybersecurity 5-Year Strategic Plan (HICSP). The intent of this document is to guide C-suite executives, information technology and security leaders, 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.

As applied to Resource-Constrained providers, public health organizations, and all stakeholders in direct patient care, medical technology, pharmaceuticals and labs, payers and health IT, HICSP can mitigate risk, protect the nation's public health infrastructure and safeguard the interoperable movement of essential data that ensures the public health of entire populations.

Achievement of several of the 12 Implementing Objectives of the Strategic Plan would directly address the cybersecurity concerns and recommendations of our nation's Resource-Constrained providers, including:

Objective 2	*Simplify access to resources and implementation approaches related to adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, & data*
Objective 6	*Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health)*
Objective 7	*Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs*
Objective 8	*Increase utilization of automation and emerging technologies such as AI to drive efficiencies in cybersecurity processes.*
Objective 12	*Develop mechanisms to enable "mutual aid" support across sector stakeholders to allow for timely and effective response to cybersecurity incidents*

HSCC 2025 Recommendations for Government Policy and Programs Applicable to Resource-Constrained Healthcare Cybersecurity

In March 2025 the HSCC offered considerations and ideas for how government policy and programs can support the health sector's investment in and management of stronger cybersecurity risk reduction. These proposals are neither exhaustive nor rigid in their descriptions but by focusing more on the "what" than the "how", they are meant to stimulate discussion and creativity within government and with industry around possible initiatives the government can develop.

If implemented under existing or new statutory authorities, these concepts could help reduce risk across the sector through incentive- or grant-based financial assistance and operational support, particularly to under-resourced health systems, including small practice, critical access, safety net and rural emergency hospitals.

The recommendations are grouped into the following topical categories: 1) Preparedness Support and Information Sharing; 2) Financial Support and Incentives; 3) Incident Response and Recovery; 4) Workforce; and 5) Regulatory Reform. The recommendation numbers below correspond to those excerpted from the original Recommendations document for easy reference and context with other related recommendation.

1.6 Designate high impact cyber and ransomware attacks, which result in widespread disruption and delay of health care delivery at critical access, safety net and rural emergency hospitals, as "all hazards" incidents to activate appropriate Federal government response support for state, regional and local emergency response services.

1.7 HHS should encourage health sector organizations to join and actively participate in Health-Information Sharing and Analysis Center (Health-ISAC) as part of a robust resilience strategy. The U.S. Department of Treasury set the precedent in 2014 in issuing a statement recommending that all financial institutions "... participate in the [Financial Services] ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities....Rapidly evolving cybersecurity risks reinforce the need for all to have methods for obtaining, monitoring, sharing, and responding to threat and vulnerability information (source)." HHS should adopt a similar recommendation with appropriate financial support and incentives particularly for resource-constrained health providers described below so that healthcare and public health organizations can benefit from the rapid sharing of cybersecurity risks and mitigating controls.

1.10 Continue development, outreach and provision of innovative CISA support programs, such as the Cyber Hygiene (CyHy) program and cyber exercises, that can be tailored in close consultation with HHS to healthcare entities.

2.1 CMS reimbursement incentives: If an institution demonstrates implementation of HICP, the NIST CSF, or other recognized security practices as incentivized in P.L. 116-321 as mitigation for HIPAA-enforcement liability following a data breach, CMS similarly can offer additional reimbursement under a concept of "meaningful protection." This could include additional CMS reimbursement to HDO's participating in the Health-ISAC or other ISAO's, implementation of active legacy medical technology cyber security management and replacement programs, and cybersecurity being included among performance goals overseen by hospital boards. Such incentive programs could be phased-in, measuring progress over time,

aligning with HICP or other recognized security practices and tying incentives to the cost/difficulty/scale of particular control frameworks and other cybersecurity investments in the clinical environment.

2.2 *Unregulated third-party technology and service providers represent both a major threat vector and costly third-party risk management demands. Health providers should not bear sole burden for policing their vendors; such third parties must be held to an enforceable higher cybersecurity standard when they support critical healthcare infrastructure where lives are at risk.*

2.3 *Workforce augmentation for needed cybersecurity skills should be funded at the federal level through ongoing commitment of CISA technical support programs, and at the federal and state levels for subsidizing the use of contracted managed security providers, academic institutions' deployment of student engineers and cybersecurity majors in programs such as the Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/); state national guard assistance for cybersecurity incident response, and other programs.*

2.4 *Maintain and expand of the U.S. Department of Agriculture's Rural Loan Program, which supports rural entities such health providers with various forms of cybersecurity support:*

- *Funding equipment and infrastructure*
- *Securing rural development's portfolio through managing risk to healthcare facilities*
- *Potential technical assistance provider*
- *Conduit to rural community leaders and health care providers to share information and resources*

2.5 *As one-time grant support payments generally cannot be used for hiring, grant programs should be tailored to the specific needs the Resource-Constrained health providers and should be ongoing as part of the payment structure.*

2.6 *CISA and HHS should encourage state insurance regulatory agencies to work with insurance companies to devise incentive programs that tie reduced premiums and/or improved coverage for cyber insurance to participation in the Health-ISAC and other information sharing and analysis organizations as one element of an appropriate cybersecurity risk management program.*

2.7 *HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) to assist critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to take advantage of information made available via various channels including agencies, information sharing organizations, product vendors, etc. State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.*

2.8 *HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations.*

2.9 *Add specified cybersecurity tools; services and surge workforce capacity as allowable expenses under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.*

2.10 *HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.*

3.4 Cyber-attack victim reporting requirements should be waived while an incident response is underway in the early stages of discovery and operational triage.

3.5 Provide federal-sponsored incident response support for organizations that are experiencing security incidents and in need of assistance getting through and recovering from the breach.

3.8 Provide Military, State, or National Guard cyber/medical personnel, equipment and services support for providers meeting specific need thresholds after an attack (incident response and recovery), with appropriate reimbursement from HHS/CISA.

4.1 HHS should administer a healthcare cybersecurity workforce development and cyber training program with assistance from NIST, CISA, and/or Veterans Administration. A program could include access to free cyber training, assistance to providers under an expanded Regional Extension Centers program, and student loan forgiveness programs modeled after physician loan forgiveness programs, or the National Science Foundation's CyberCorps(R) Scholarship for Service (SFS) program. This program provides a full scholarship plus stipend for undergraduate and master's degrees in cybersecurity and requires two years of government service.

4.2 Fund federal, and supplement state-subsidized - "civilian cyber health corps" programs. This could take the form of loan forgiveness; i.e., a Federal program pays / helps pay for a cyber education in exchange for a minimum number of years served, modeled after a uniformed health corps such as the U.S. Public Health Service Commissioned Corps - https://www.hhs.gov/surgeongeneral/corps/index.html. Consider establishing career pathways that do not require a full 4 years of college (i.e. certificate programs and associates).

4.3 Augment workforce development programs such as in the HITECH Act, which funded health IT workforce training programs: the University-Based Training Program and Community College Consortia Program. In total the two programs trained 21,437 students from all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands at 91 academic institutions. See: https://www.healthit.gov/data/quickstats/hitech-workforce-development-programs.

4.4 HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) as workforce augmentation to assist critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to operationalize information provided by government agencies, information sharing organizations, product vendors, etc. State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.

4.5 HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations (ISAOs).

4.6 Add specified cybersecurity tools, services and surge workforce capacity as allowable expenses under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.

4.7 HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

Conclusion

The need for cybersecurity in healthcare is only growing stronger. Yet Resource-Constrained providers lack the workforce, partners, and means to implement cybersecurity best practices. Through our interviews with 42 healthcare leaders at Resource-Constrained institutions, we learned that most providers know what needs to be done, they simply lack the capacity and resources to put best practices into action. Providers need workforce augmentation, trusted partners to help certify, host, maintain, and support health IT systems with modern cybersecurity capabilities, and the financial flexibility to invest in cybersecurity. Looking at today's healthcare landscape, artificial intelligence is accelerating delivery transformation in large institutions who can afford novel technologies and the cybersecurity costs that come with them. Resource-Constrained providers will fall further behind in the adoption of this technology because they cannot bear the increased cyber vulnerabilities. Now is the time for action and investment to secure valuable information and ensure innovative health care delivery remains available in rural and Resource-Constrained communities.

Members of the HSCC Resource-Constrained Provider Cybersecurity Task Group

The HSCC Cybersecurity Working Group recognizes the many members who contributed to this initiative:

Co-Leads:

Jennifer Stoll	**OCHIN, Inc.**
Jim Roeder	**Lakewood Health System**
Mark Early	Adena Health System
Zack Hornberger	Advanced Medical Technology Association
Ronald Fitzherbert	Amador Health Center
Jeff Coughlin	American Medical Association
Damian Grant	Amgen Inc.
Mike Roberts	Appalachian Regional Healthcare
Bill Aerts	Archimedes Center for Healthcare and Medical Device Cybersecurity at Northeastern University
Priyanka Upendra	Asimily
Thomas Robulack	ATEC Spine
Doug Copley	AtlantiCare Health System
Mike Green	Availity
Gabriel Oberfield	Bond, Schoeneck & King
Dallas Smith	Burn and Reconstructive Centers of America
Jim St. Clair	C3HIE
Michael Prakhye	CareTech Solutions
Michael Duncan	Center for Internet Security (CIS)
Cassie Ballard	CHIME

Anahi Santiago	Christiana Care
Lisa Munro	Clearwater Security
Steve Cagle	Clearwater Security
Jackie Mattingly	Clearwater Security
Sharee Dorsey	Cleveland Clinic
Christopher Ross	Clover Health
Lori Beeby	Community Hospital
Brian Blackburn	Compassus
Gerry Blass	Comply Assistant
Karen Greenhalgh	Cyber Tygr
Laura Baker	Cyber Wyoming
Christopher Plummer	Dartmouth-Hitchcock Health
Janette Arencibia	Defense Health Agency
Sarah Moore	Digital Medicine Society (DiMe)
Aaron de Montmorency	Elevate Health
Rick LeMay	First Health Advisory
Bijan Anvar	Flushing Hospital Medical Center
Eric Campbell	Friend Health
Taylor Lehmann	Google Cloud
Bill Reid	Google Cloud
Janine Fadul	GW Medical Faculty Associates
TJ Bean	HCA Healthcare
Leon Vinci	Health Promotion Consultants (HPC)
Adriane Burton	Health Resources and Services Administration (HRSA)
Troy Adams	HHS HC3
Andrea Greene-Horace	HHS/CMS
Phil Englert	Health-ISAC
Don Weary	Health-ISAC
Michael Potter	Huron Behavioral Health
John Suarez	Institute for Homeland Security at SHSU
Robert Kerwin	International Association of Medical Equipment Remarketers and Services (IAMERS)
Hazel Chappell	ishca health
Tom Jones	John Fitzgibbon Memorial Hospital
Donna Grindle	Kardon
Rick Jiggens	Kinwell Physician Network
Michael Sanders	Lawrence County Memorial Hospital
Bill Proffer	Leidos
Edwin Dreyden	McKesson
Ty Greenhalgh	Medigate by Claroty
Christopher Byrd	Messer Financial Group
Margie Zuk	MITRE

Penny Chase	MITRE
Leslie Marsh	Nebraska Rural Health Association
Janice Reese	NetworkPDF Inc.
Sara Coverstone	Northern Arizona Healthcare
Chris Graham	Presbyterian Healthcare Services
Mike Ratliff	Providence
Sahan Fernando	Rady Children's Hospital
Muhammad Siddiqui	Reid Health
Kim Hogstad	Sanford Health
David Nathans	Siemens Healthineers
Cherrie Murphy	Southwest Regional Health Systems
Shawna Hofer	St. Luke's Health System
Kristi Arndt	St. Luke's University Health Network
Hugo Lai	Temple Health
Tamara Lauterbach	The Guthrie Clinic
Nikiah Nudell	The Paramedic Foundation
Janine Medina	Thermo Fisher Scientific
Gregory Ewing	Trillium Health
Scott Trevino	TRIMEDX
Bob Latz	Trinity Rehabilitation Services
William Hall	UNC Health
Chayapol Pakachaipong	University of Minnesota
JohnJeffries	University of Tennessee Medical Center
Jake Edwards	UVA Health
Bill McDonald	WRM Consult.com, Inc.

Appendix: Definitions

Term	Definition
Attack Surface	The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment. [NIST Special Publication 800-53 Rev. 5]
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose. [NIST Special Publication 800-53 Rev. 5]

Configuration Management Database (CMDB)	Is a data repository that stores information about all hardware and software assets in your IT environment. This critical component of the ITIL framework allows for efficient oversight and management of organizational assets, known as configuration items (CI), and delivers greater insight into how they relate to one other across the company. [CIO.com]
Critical Access Hospital (CAH)	The Medicare Rural Hospital Flexibility Program (Flex Program), created by Congress in 1997, allows small hospitals to be licensed as CAHs and offers grants to States to help implement initiatives to strengthen the rural health care infrastructure. CAHs must be located in a rural area and be more than 35 miles from another hospital (15 miles by secondary roads or in mountain terrain) or have been certified before January 1, 2006 by the State as being a necessary provider of health care services. Additionally, to be considered a CAH, the hospital must have an emergency room that operates 24 hours a day and 7 days a week using either on-site or on-call staff. A CAH is normally limited to 25 inpatient beds used for either inpatient or swing bed services. CAHs are also subject to a 96-hour (4-day) limit on the average length of stay. [U.S. Assistant Secretary for Technology Policy]
Distributed Denial of Service (DDoS)	A denial of service technique that uses numerous hosts to perform the attack. [NIST Glossary of Cybersecurity Terms]
Endpoint Detection and Response (EDR)	Category of security tools that monitor end-user hardware devices across a network for a range of suspicious activities and behavior, reacting automatically to block perceived threats and saving forensics data for further investigation. [CSO Online]
Federally Qualified Health Center (FQHC)	Entities that must qualify for funding under Section 330 of the Public Health Service Act (PHS), qualify for enhanced reimbursement from Medicare and Medicaid (as well as other benefits), serve an underserved area or population, offer a sliding fee scale, have an ongoing quality assurance program, have a governing board of directors, and provide comprehensive services (either on-site or by arrangement with another provider), including: (1) preventive health services, (2) dental services (3) mental health and substance abuse services (4) transportation services necessary for adequate patient care (5) hospital and specialty care. [U.S. Department of Health and Human Services, Centers for Medicare & Medicaid Services]
Incident Response	Is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms. [NIST Special Publication 800-35]
Infragard	Is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes: business executives, entrepreneurs, lawyers, security personnel, military and government

	officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security. [Infragard]
Legacy System	IT system or component that runs end of life software, hardware, and/or firmware which cannot be upgraded to fix any new vulnerability that has been discovered that may affect the end of life software, hardware, and/or firmware.
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. [NIST Special Publication 800-30 Rev. 1]
Mobile Device Management (MDM)	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices. [NIST Glossary of Cybersecurity Terms]
Multi-Factor Authentication (MFA)	The means used to confirm the identity of a user, process, or device (e.g., user password or token). [NIST Glossary of Cybersecurity Terms]
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. [NIST Glossary of Cybersecurity Terms]
Penetration Test	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system. [NIST Special Publication 800-53 Rev. 5]
Privileged Access Management (PAM)	Tools that provide an elevated level of technical access through the management and protection of accounts, credentials and commands, which are used to administer or configure systems and applications. [Gartner]
Ransomware	Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. [U.S. Cybersecurity & Infrastructure Security Agency]
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. [NIST Glossary of Cybersecurity Terms]

Remediation	The neutralization or elimination of a vulnerability or the likelihood of its exploitation [NIST Glossary of Cybersecurity Terms]
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST Special Publication 800-53 Rev. 5]
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. [NIST Special Publication 800-30 Rev. 1]
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [NIST Glossary of Cybersecurity Terms]
Risk Registry / Risk Register	A central record of current risks, and related information, for a given scope or organization. [NIST Glossary of Cybersecurity Terms]
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST Special Publication 800-53 Rev. 5]
V-CISO	Acronym for Virtual Chief Information Security Officer.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST Special Publication 800-53 Rev. 5]
Vulnerability Scanning	Can be performed by software from outside or inside the network or the network segment that's being evaluated. Organizations can run external scans from outside their network perimeter to determine the exposure to attacks of servers and applications that are accessible directly from the internet. Meanwhile, internal vulnerability scans aim to identify flaws that hackers could exploit to move laterally to different systems and servers if they gain access to the local network. [CSO Online]