

S. Hrg. 118–55

IN NEED OF A CHECKUP: EXAMINING THE CYBERSECURITY RISKS TO THE HEALTHCARE SECTOR

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 16, 2023

Available via the World Wide Web: <http://www.govinfo.gov>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

52–484 PDF

WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

CHRISTOPHER J. MULKINS, *Director of Homeland Security*

JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*

WILLIAM E. HENDERSON III, *Minority Staff Director*

CHRISTINA N. SALAZAR, *Minority Chief Counsel*

KENDAL B. TIGNER, *Minority Professional Staff Member*

LAURA W. KILBRIDE, *Chief Clerk*

ASHLEY A. GONZALEZ, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Peters	1
Senator Hassan	13
Senator Carper	15
Senator Hawley	17
Senator Blumenthal	20
Senator Padilla	22
Senator Rosen	24
Senator Sinema	26
Prepared statements:	
Senator Peters	31

WITNESSES

THURSDAY, MARCH 16, 2023

Scott Dresen, Senior Vice President, Information Security and Chief Information Security Officer, Corewell Health	3
Kate Pierce, Senior Virtual Information Security Officer, Fortified Health Security	5
Greg Garcia, Executive Director, Cyber Security, Healthcare and Public Health Sector Coordinating Council	7
Stirling Martin, Senior Vice President and Chief Privacy and Security Officer, Epic Systems	9

ALPHABETICAL LIST OF WITNESSES

Dresen, Scott:	
Testimony	3
Prepared statement	33
Garcia, Greg:	
Testimony	7
Prepared statement	56
Martin, Stirling:	
Testimony	9
Prepared statement	83
Pierce, Kate:	
Testimony	5
Prepared statement	36

APPENDIX

Ms. Pierce supplemental response	86
American Academy of Family Physicians Statement for the Record	88
Responses to post-hearing questions for the Record:	
Mr. Dresen	95
Ms. Pierce	97
Mr. Garcia	100

IN NEED OF A CHECKUP: EXAMINING THE CYBERSECURITY RISKS TO THE HEALTHCARE SECTOR

Thursday, March 16, 2023

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD-562, Dirksen Senate Office Building, Hon. Gary Peters, Chairman of the Committee, presiding.

Present: Senators Peters [presiding], Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Scott, Hawley, and Marshall.

OPENING STATEMENT OF SENATOR PETERS¹

Chairman PETERS. The Committee will come to order.

Today's hearing will examine cybersecurity threats facing the healthcare sector, how both the Federal Government and health care providers are working to combat these threats, and what actions Congress should take to bolster our cybersecurity defenses against these attacks.

Health care is a rapidly growing sector of our economy that employs more than 18 million workers, and is made up of both public and private sector organizations related to patient services, medical devices and manufacturers, and electronic health and medical records, that store considerable amounts of personal information, making them frequent targets of attacks.

In recent years, increasingly sophisticated cyberattacks in the health care and public health sectors have posed alarming threats to people in Michigan as well as all across the country.

Cyberattacks on hospitals, and other health care providers, can cause serious disruptions to their operations and prevent them from effectively providing critical, lifesaving care to their patients. Breaches can also lead to the exposure of sensitive personal and medical information of patients and health care personnel.

Most recently, the DC Health Link, a health insurance marketplace for residents and lawmakers in the nation's capital, experienced a cyberattack that exposed the personal data and information of tens of thousands of people, putting victims at risk of identity theft, scams, and additional cyberattacks.

Earlier this year, in my home State, the University of Michigan Health System experienced a cyberattack that temporarily limited

¹The prepared statement of Senator Peters appears in the Appendix on page 31.

access to their public websites. Thankfully in that attack, no patient information was compromised and the issue was quickly resolved.

These relentless cyberattacks show that foreign adversaries and cybercriminals will stop at nothing to exploit cybersecurity vulnerabilities, our critical infrastructure, and most essential systems.

What is most concerning about these attacks is that they do not just compromise personal information. They can actually affect patient health and safety. Last month, a ransomware attack on Tallahassee Memorial HealthCare in Florida took the hospital's information technology (IT) systems offline for more than a week, and required them to divert patients to other facilities and cancel procedures until they could restore those networks.

A 2019 catastrophic ransomware attack on the Spring Hill Medical Center in Mobile, Alabama, may have even led to a patient's death. The attack prevented health care providers from using equipment to monitor a baby's condition during delivery. As a result, the infant tragically passed away because of delayed medical care.

This shocking example shows just how grave the consequences of cyberattacks in the health care sector can be. Given the threats facing this sector, and the potential life or death consequences, there is no question that investments in health care cybersecurity are also investments in patient care.

This Committee has already taken important steps to strengthen cybersecurity for our critical infrastructure sectors, including the health care sector. Last Congress, the Committee advanced a bipartisan bill that I introduced along with Senator Portman to require these organizations to report cyberattacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA).

This law will help ensure that government is able to better track cybersecurity threats to our critical infrastructure, provide more transparency and situational awareness for our cybersecurity defenses, and enable CISA to warn potential victims of ongoing attacks, so they know if they could be the next target.

This is an important first step, but there is much more Congress can do to ensure that critical networks in our health care and public health sector remain resilient against cyberattacks.

I am grateful our colleague, Senator Rosen, is leading efforts that would improve the way CISA and the Department of Health and Human Services (HHS) share information about cybersecurity threats with the health care sector, as well as provide cybersecurity training to medical professionals. I look forward to working together to build on these efforts.

Today, I am pleased to have an expert panel of health care cybersecurity professionals who can speak more about the challenges we face and discuss potential solutions.

With that I would normally turn it over to our Ranking Member, who is not here, so I will move to swear in our witnesses.

It is the practice of Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses, so if each of you would please stand and raise your right hand.

Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. DRESEN. I do.

Ms. PIERCE. I do.

Mr. GARCIA. I do.

Mr. MARTIN. I do.

Chairman PETERS. Thank you. You may be seated.

Our first witness is Scott Dresen. Mr. Dresen serves as the Chief Information Security Officer (CISO) of Corewell Health. In his role, he is responsible for maintaining and managing the Enterprise Business Assurance Program including emergency management, business continuity, and operational readiness. Previously he served as the Chief Information Officer (CIO) for Wayne State University Physician Group.

Mr. Dresen, thank you for being here. You may proceed with your opening remarks.

TESTIMONY OF SCOTT DRESEN,¹ SENIOR VICE PRESIDENT, INFORMATION SECURITY AND CHIEF INFORMATION SECURITY OFFICER, COREWELL HEALTH

Mr. DRESEN. Thank you, Chairman Peters and Members of the Homeland Security and Governmental Affairs Committee. It is an honor to be speaking with you about cybersecurity risks. I am the Chief Information Security Officer of Corewell Health, an integrated health system committed to health and wellness so that people can live their healthiest life possible.

Cybersecurity threats to the health care sector could compromise our health system's ability to effectively provide access to and deliver health care services to our patients and members. Of particular concern are high-impact ransomware attacks, which disrupt and delay health care delivery, may cause risks to patient safety, and can be used to conceal activity by threat actors to exfiltrate personal health information.

We live in a world where health care is highly digital and highly connected, making us vulnerable given the value of the data we manage. We have a responsibility to protect the data of our patients and members, and this obligation is of the highest priority across our system leadership and board of directors.

Health care is a complex business model whereby multiple, often independent entities come together to form what the patient sees as a cohesive care delivery process. Over time and out of necessity, this model has evolved in ways that have made us more vulnerable to cyberattacks, has expanded the footprint of health care systems that must be protected, and increases the opportunities for threat actors to compromise us.

Media reports of cyberattacks, data breaches, and unintended exposure of sensitive data underscores the vulnerability of health care systems to these disruptive incidents and the impact to our patients and members. Operational disruption prevents patients from being able to receive the care they need when they need it. Material financial impact in the form of fines, penalties, and associ-

¹ The prepared statement of Mr. Dresen appears in the Appendix on page 33.

ated remediation costs increase financial pressures significant. Brand and reputational impacts can have lasting consequences on organizations victimized by cyberattacks.

These issues only serve to undermine the trust our communities have in our health care system and our ability to serve them in their most vulnerable time of need. A comprehensive information security program is critical to manage these risks, yet there exists significant disparity in the health care sector for organizations to resource an effective security team and the necessary technology to provide their requisite protections to reduce the risk of an attack. Small and medium-sized health care systems are at a significant disadvantage compared to larger systems to be able to recruit, retain, and fund an effective information security program. Despite the advantage larger organizations have in comparison, the increasing trend of attacks prove even the largest organizations are vulnerable and can be compromised.

The increasing frequency of attack from nation-state actors and organized crime has created a sense of urgency within the health care sector, and we need help from the United States government to respond to these threats more effectively. Requirements for interagency sharing of cybersecurity threat intelligence is a productive step forward. We need more of this and need that enhanced collaboration to include critical infrastructure sector participation, including the ability to automate threat intelligence data sharing with sector participants, enabling rapid, near-real-time automatic ingestion of threat intelligence into the technologies participating members use to protect their respective organizations.

The United States government has actionable intelligence that would be of immediate value to the health care sector. While there is some degree of automated intelligence sharing, we need to make more of that intelligence accessible.

We are in an environment where keeping up with technology to defend against advanced, persistent threat is extremely expensive. Many of these technologies are an option for financially disadvantaged health care systems due to cost. We recommend creating incentives to make technology more affordable and accessible to the entire health care sector.

We recommend reforms on the penalties health care entities face because of cyberattacks and related data breaches. We understand and support the legislative intent to encourage adoption of best practices and the implementation of appropriate protections to safeguard our data. However, penalizing victims of cyberattack, when defensive measures cannot keep up with the sophistication of hackers, is not the fair approach.

We are at our best and most capable when it comes to caring for our patients and members. That is our expertise. Our adversaries are at their best and most capable when they are attacking us. They are extremely well funded, extremely talented, and highly motivated. Many are either nation-state actors or sponsored and supported by nation-states. We cannot beat them alone, but together we can be more effectively protecting this vital, critical infrastructure sector.

Thank you for this opportunity to testify, and I look forward to your questions.

Chairman PETERS. Thank you, Mr. Dresen, for your testimony. Our next witness is Kate Pierce. Ms. Pierce serves as the Senior Virtual Information Security Officer at Fortified Health Security. Ms. Pierce has over two decades of experience in North Country Hospital, where she served as the Chief Information Officer and Chief Information Security Officer. Ms. Pierce is also part of the Fortified Health Security, one of the leading health care-only cybersecurity managed services companies in the United States.

Ms. Pierce, welcome to our Committee. You may proceed with your opening remarks.

TESTIMONY OF KATE PIERCE,¹ SENIOR VIRTUAL INFORMATION SECURITY OFFICER, FORTIFIED HEALTH SECURITY

Ms. PIERCE. Chairman Peters and Members of the Committee, my name is Kate Pierce. I served as the CIO and CISO for a critical access hospital in Vermont for over 21 years, and I currently serve as the Virtual Information Security Officer for Fortified Health Security. I thank you for this opportunity to address the Committee to provide an industry perspective on cybersecurity threats, specifically in the small and rural facilities.

In 2022, health care continued to be the most targeted critical infrastructure sector, with nearly a quarter of ransomware attacks directed at health care. We also saw cyber criminals shift their focus to small and rural hospitals, with this group lagging behind in strengthening their defenses. Average recovery times expanded, and costs for health care attacks increased to over \$10.1 million per incident.

Our rural hospitals are facing unprecedented budget constraints, with up to 30 percent or more in the red. With the public health emergency scheduled to end in May, hospitals anticipate a rise in free care, with as many as 15 million Medicaid patients projected to lose coverage.

Cyber programs continue to lag behind with budgeted security spending redirected to cover higher priority expenses. These small hospitals struggle to employ and retain skilled cybersecurity professionals, and often have little to no staff solely dedicated to security. Cyber insurance coverage can no longer be considered an alternative, with skyrocketing premiums, lower limits, and increasing requirements.

The value of health care records in the dark web continues to be up to more than 60 times higher than other records. The risk of identity theft, credit card fraud, and reputational harm is now supplemented by patients being directly exploited with threats to release their sensitive information on the web. Post attack, hospitals are now seeing a rise in civil cases, costing millions of dollars.

The impact on our rural communities during an attack is hard to overstate. While attacks in urban areas are impactful, populated areas provide other health care options for patients to choose. In most rural areas, the nearest health care facility may be 45 miles or more away, making the diversion of patients unfeasible. With direct attacks causing outages lasting weeks and sometimes months, the impact on patient safety is easy to comprehend.

¹ The prepared statement of Ms. Pierce appears in the Appendix on page 36.

Delays in care can directly contribute to negative outcomes for many high-risk conditions. Facilities that continue to treat patients are challenged to provide high levels of patient care without access to patient information, safety alerts, delays in results, and other key tools.

To meet these challenges I recommend implementing several measures to improve the cybersecurity for our small and rural facilities.

First, we must move beyond guidance and recommendations and create minimum standards for cybersecurity. These standards must be effective, reasonable, achievable, and continually evolving as cybersecurity requirements change. Specific recommendations are in my written testimony.

Second, we cannot leave our small and rural hospitals behind. Funding opportunities must be made available to these hospitals. My insights on subsidies, grants, and other incentives are also included in my written testimony.

Third, we need better coordination of government cyber efforts. While guidance and services from many agencies is appreciated, there is often a knowledge gap regarding the unique health care challenges that must be considered. Also, most rural hospitals are not effectively utilizing available resources. To be effective, government services must be streamlined, knowledgeable, and available.

Last, establishing a Federal Emergency Management Agency (FEMA) cyber disaster relief program would provide this vulnerable sector with important resources. This could assist organizations in their recovery process and increase the likelihood that hospitals can survive beyond an attack.

In conclusion, small and rural health care organizations are losing the cybersecurity battle. The Cybersecurity Act of 2015 is now eight years old. While advancement have been made with respect to published documents, services, and guidance, as a nation definitive, coordinated action is needed now. Our rural hospitals are in crisis, and further delay would jeopardize health care for our rural communities.

Thank you for your time. I look forward to answering your questions.

Chairman PETERS. Thank you, Ms. Pierce. Thank you for your testimony.

Our next witness is Greg Garcia. Mr. Garcia serves as the Executive Director for Cyber Security of the Healthcare and Public Health Sector Coordinating Council (HSCC). It is a convening organization that works in partnership with other Federal agencies to protect the security and resilience of these sectors. Mr. Garcia served as the nation's first Department of Homeland Security (DHS) Assistant Secretary for Cybersecurity and Communications under President George W. Bush.

Previously, Mr. Garcia held executive positions with the Bank of America and served as professional staff on the Committee on Science, Space, and Technology in the U.S. House of Representatives.

Welcome to the Committee, sir. You may proceed with your opening comments.

TESTIMONY OF GREG GARCIA,¹ EXECUTIVE DIRECTOR, CYBER SECURITY, HEALTHCARE AND PUBLIC HEALTH SECTOR COORDINATING COUNCIL

Mr. GARCIA. Thank you, Chairman Peters and Members of the Committee. Thanks for inviting me to testify today. I am the Executive Director of the Health Sector Coordinating Council. We are an industry-led advisory council of more than 350 health care organizations and government agencies, working together as a public-private partnership.

The main point I want to leave you with today is that the industry is mobilizing collaboratively against evolving cyber threats in the health system, and our government is doing the same and can be doing more.

The industry is regulated for cybersecurity in various ways, and more is being contemplated. But there are ways that HHS, CISA, and other government offices can improve coordination, in programs and funding, to facilitate the security of the health sector.

What matters most about cyber insecurity in the health sector is the potential impact on patient safety. We have heard that from our previous witnesses. In particular, ransomware events over the past few years have resulted in clinical disruptions that can cause and have caused harm to patients. Consider when a health system is disabled by a cyber incident, stroke, trauma, cardiac imaging, and other systems and services as closed to admission. Ambulances with patients en route to hospitals are diverted. Radiation and surgery for cancer patients are delayed. Medical records for prescriptions, diagnoses, therapies are inaccessible or lost. Clinical trial data are lost. Payment systems are down. Order and receiving supplies is disrupted.

What we see now and in the future is a changing health care system that may complicate this challenge. Consider that health care innovation is going direct to the consumer, to wearable and home medical technology and telemedicine. This expands the so-called attack surface for connected technology outside the clinical environment, which is harder for hospitals to secure remotely with patients.

There is an increase in mergers and acquisitions among provider institutions, and that involves having to integrate incompatible systems, different suppliers. That adds to complexity, cost, and risk.

There is an increased migration to cloud service providers, in which technology, clinical data management systems and software are outsourced to third parties, and that can increase the scalability of attack to thousands of customers with just one mouse click.

There are workforce shortages, that Ms. Pierce referred to, in both clinical and cybersecurity support, which strains the ability to manage those intersecting needs, cyber and clinical.

Finally, the cyber insurance market is simultaneously retrenching, increasing premiums, reducing coverage, and this is severely limiting its risk reduction value.

¹ The prepared statement of Mr. Garcia appears in the Appendix on page 56.

What are we doing about it? How do individual enterprises deal with these threats, and how does the sector collectively deal with it. I am going to concentrate my answer on the latter question.

As I mentioned earlier, the Health Sector Council is one of many federally designated critical infrastructure sector coordinating councils. Health care is in the same category as financial services, telecommunications, electricity, and others, and we are organized to work with our government counterparts to identify and mitigate threats and incidents, from pandemics, natural disasters, supply chain disruptions, and cyberattack.

In government, there are designated sector risk management agencies (SRMA), in our case HHS. They are directed by statute and Executive Orders (EO) to work with their corresponding critical sectors on this shared mission, not just with regulation but with partnership and innovative problem-solving.

Indeed, cyber regulation on the nation's small and under-resourced health systems cannot succeed without corresponding support from the government. To reduce that cyber and patient risk, our Council, over the past five years, has worked tirelessly. We started with fewer than 50 members, in 2017, and now the Council has grown to 380 industry organizations and 16 government organizations. We are all motivated by the same unifying imperative, that patient safety requires cyber safety.

We are structured into task groups that work on specific cybersecurity problems. The result over the past four years is the publication of 18 cybersecurity best practices and guidance documents by the sector, for the sector: medical device security, cybersecurity for health systems, workforce development, information sharing, intellectual property protection, et cetera.

Two of these resources were published jointly, by our Council and by HHS. This demonstrates the importance we place on this shared responsibility, and four more resources are in the pipeline for publication in the second quarter of this year, one of which is another joint publication with HHS.

But as a partnership with government, we are making positive steps but we can do more. We are encouraged that HHS is reorganizing to enhance its SRMA responsibilities. That means working with us, in industry, to develop cybersecurity initiatives, incentives, and programs. It means improving information sharing, impact analysis, and incident response. It means coordinating across the agency and with industry to make cybersecurity policy development and enforcement more matrixed and coherent. Some of that may require congressional action.

It is commendable that CISA, in its role as the national coordinator for critical infrastructure protection, has directed more of its attention to health care cybersecurity. But that level of attention needs to be triangulated, among HHS as the sector lead, CISA as the technical support, and industry as the owners and operators. In our view, that necessary relationship is improving, and we are glad for that, but more improvement can be done.

In conclusion, my written statement includes options we are considering as recommendations for how the government can better partner with that critical infrastructure sector against evolving

threats, and I will be happy to discuss them during the question period.

To finalize, we are working collectively in pursuit of the imperative of patient safety. It requires cyber safety, and succeeding at this will mean, as my friend and former National Cyber Director, Chris Inglis, would tell us, “To beat one of us you have to beat all of us.”

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Mr. Garcia, for your testimony.

Our final witness is Stirling Martin. Mr. Martin is the Senior Vice President for Epic. In his over 25 years at Epic he has helped develop, implement, and support Epic’s products and worked closely with customers around the world to ensure their needs are met.

Mr. Martin also serves as the Chief Security and Privacy Officer and President of Epic’s hosting business.

Mr. Martin, thank you for being here today. You may proceed with your opening remarks.

**TESTIMONY OF STIRLING MARTIN,¹ SENIOR VICE PRESIDENT
AND CHIEF PRIVACY AND SECURITY OFFICER, EPIC SYSTEMS**

Mr. MARTIN. Thank you. Distinguished Members of the Committee, thank you for the opportunity to provide my testimony today. My name is Stirling Martin, my formal training is as a computer scientist, and I am the Chief Security and Privacy Officer and Senior Vice President at Epic.

Since 1979, we have created clinical, financial, and administrative systems, including the patient portal, MyChart, for health care organizations in the United States and around the world. Our customers include academic medical centers, large integrated health systems, small critical access hospitals, and federally qualified health centers.

Our focus, first and foremost, is on helping patients. Personal health data is uniquely sensitive if compromised because it cannot be reset like passwords or changed like credit card information. A patient’s health information can also be immensely personal, and even just the threat of exposure can create angst for an individual. If exposed, private health care data can be leveraged by malicious actors through identity theft and the potential for blackmail. In an extreme case, patient safety could be directly impacted if a bad actor were to manipulate health care data.

Within a community, cyberattacks can reduce access to care. In a rural community with only one health care facility, patients may need to delay preventative care or elective treatments until an incident is resolved.

In a larger community, a cyberattack can have a cascading effect as patients may be diverted to an unfamiliar care team at another facility, and those facilities need to deal with an influx of additional patients.

We have been shoulder-to-shoulder with our customers as health care has become increasingly targeted by cyberattacks. For a health system, a cyberattack disrupts their patient care mission and causes both reputational harm and financial burden. Organiza-

¹ The prepared statement of Mr. Martin appears in the Appendix on page 83.

tions often take their systems offline as they mitigate the impact of a security incident. Doing so places stress on staff to provide high-quality care without the IT systems that drive their workflows. As organizations may see fewer patients, the financial impact extends beyond the cost of incident response to lost revenue as well.

Organizations face several challenges in improving their security posture. First is staffing, and their ability to hire and retain high-demand security talent.

Second, security is a constant effort, and there are always more steps that can be taken to make systems more secure. In working with health care organizations across the country, we see both basic and highly sophisticated security programs in use, and yet there is no defined benchmark of what security practices are considered sufficient.

An additional challenge is the lack of cybersecurity information-sharing among health care organizations, as well as the limited threat intelligence from government agencies and private industry.

These challenges are exacerbated as many health care organizations currently face unprecedented financial and staffing pressures. The costs to improve one's security posture through new technology or staff must be weighed against other needs such as hiring or retaining nurses at the bedside.

There are a variety of ways the Federal Government could help health care organizations prevent and respond to cyberattacks.

Starting first with prevention, there is a dire shortage of security talent in the United States. To build a deeper bench of skilled IT security professionals, the Federal Government could develop security training programs and incentivize newly trained professionals working in health care. This could be similar to the Rural Community Loan Repayment program for physicians who agree to provide care to rural communities after medical school and residency.

Second, the industry needs a single set of prescriptive security practices, whether defined by Federal agencies such as the National Institute of Standards and Technology (NIST) or CISA, industry efforts such as Health Information Trust Alliance (HITRUST), or a collaboration such as the Healthcare Sector Coordinating Council. This will raise the overall security posture of health care organizations by encouraging them to meet those acceptable security practices.

The government should take the further step of establishing a legal safe harbor for organizations that meet the defined benchmark if they fall victim to an incident. This would also encourage information sharing to remediate active issues more quickly and prevent similar issues in the future, and could be further bolstered by government agencies sharing deeper threat intelligence.

Lastly, on incident response, similar to how FEMA responds to a natural disaster, at-the-elbow support from the government could help health care organizations remediate an attack. For example, an organization recovering from a ransomware attack may need assistance cleaning and redeploying the computers used by their staff. On-the-ground support could help reduce the time it takes to bring systems back online by patching devices or by delivering a strategic reserve of computers and network equipment that can be

used immediately. This could reduce recovery time by hours or even days, providing tremendous value to health care organizations and the patients they serve.

In closing, people often ask me what keeps me up at night, and it is the fact that we have to be perfect 100 percent of the time, and the bad guys, they only need to get lucky once.

Thank you for the opportunity to share Epic's perspective on this important topic.

Chairman PETERS. Thank you, Mr. Martin, and thank you for your opening comments.

My first question is for Mr. Dresen. Clearly we know that cyberattacks are pervasive all through our society and all across our economy now, and they are increasing in intensity. But my question for you is what do you see as a distinguishing characteristic of working to secure the health care sector from cybersecurity attacks when we look at it in total? What is the distinguishing factor with health care?

Mr. DRESEN. Thank you, Senator, for that question. I appreciate the opportunity to answer. For me, the defining characteristic of the work that we do really comes down to the clarity of focus we have around the impact of the decisions we make, the actions we take, and the things we are doing to help protect our organization, understanding that when a cyberattack does occur and has the potential for significant operational disruption, financial penalties, longstanding reputational impact to the organization, it ultimately affects our families, it affects our neighbors, it affects our community. There is a clear connection to purpose for the work that we do, understanding that the impact if things do not go well can be significant on the people who are closest to us. For me that is the defining characteristic of what it means to protect the health care sector from cyberattack.

Chairman PETERS. Thank you.

My next question is for you, Ms. Pierce. Certainly all hospitals across the country are still dealing with the impact of Coronavirus Disease 2019 (COVID-19) pandemic. But rural hospitals, in particular, are really challenged. They are often bound to provide care to a high concentration of patients with limited financial resources. As you mentioned, these hospitals are often located many miles apart. They are very far from urban centers which present a number of other challenges for them.

My question for you, ma'am, is how can the Federal Government help ensure that small and rural hospitals are able to invest in cybersecurity while also balancing all the needed investments that they have to make to provide quality patient care?

Ms. PIERCE. Thank you for that question, Senator Peters. Senator Warner stated it well when he said that cybersecurity is patient safety. Cybersecurity initiatives cannot be considered in isolation. They have direct and immediate impact on patient care, and small and rural facilities are currently devastated still by the pandemic, with staffing shortages. They have seen significant increases in cost with supply chain and technical costs skyrocketing.

Rural facilities also tend to serve lower-income patients, and they have shown that the longer patients have to travel is a direct correlation to the income levels for the patients. This means that our

Medicaid population is typically higher in these rural facilities. Medicaid reimbursement tends to lag behind and is lower than the average cost of care for these rural facilities. Even Medicare reimbursements for critical access hospitals (CAHs), tend to lag two to three years behind as cost reports for those facilities take time to reconcile.

We are experiencing these high costs, but it is taking a long time for the reimbursement levels to catch up, which is creating a crisis in budgets. I have seen small hospitals running 5 to 10 percent below budget for their facilities, and we cannot continue at that rate.

While I agree it is important to control costs, cybersecurity should be a built-in requirement for all hospitals, with minimum standards that are required. Medicaid should also reimburse at cost. The subsidies for hospitals could be in the form of grants, it could be in the form of CMS increased reimbursement for services, or incentive programs similar to meaningful use, sort of a meaningful security type incentive program.

I urge you, however, to not delay any longer. Many rural hospitals are already on the brink of closure. Thank you.

Chairman PETERS. Thank you, Ms. Pierce.

Mr. Garcia, in your experience how does the Health Sector Coordinating Council, along with the Federal Government, working right now to address some of these significant challenges faced by our small and rural hospitals?

Mr. GARCIA. We have a number of engagements with our government partners on a regular basis. Every other Friday, in fact, we meet with our HHS and CISA counterparts to think about longer-term strategic direction. In fact, we are beginning the process now of developing a five-year strategic plan, looking at how is the health care industry changing over the next five years, what cybersecurity challenges do those changes introduce, and how do we prepare for them.

I will say one of the flagship resources that we produced that is scalable from small, rural, critical access hospitals all the way up to the large national and regional systems is something called the Health Industry Cybersecurity Practices (HICP). This is initially, the result of an act of Congress, and it comes out of something called the 405(d) program, section 405(d) of the Cybersecurity Information Sharing Act of 2015. It directed HHS to work with industry to develop a series of cybersecurity best practices for health systems. That process took about a year and a half to develop these best practices, which is a joint effort between HHS, which owns the 405(d) program, and the Health Sector Coordinating Council.

This is partnership at its best, where there is consensus about what health systems need to do in cybersecurity, some of the basic blocking and tackling, not necessarily expensive and a high investment level, but some of the foundational elements of good cybersecurity practices.

That is one example, and on our website, healthsectorcouncil.org, there are 18 resources, best practices that are accessible to any stakeholders who need them, all the way from medical device security best practices to workforce development to intellectual property

protection, supply chain security, which is a huge issue for all of us. I would commend the public to those resources.

Chairman PETERS. Thank you, Mr. Garcia.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thanks, Mr. Chair, and thanks for holding this hearing, and thank you to our witnesses not only for being before the Committee today but for the work you do to protect patient privacy and safety. We really appreciate it.

Ms. Pierce, I want to start with a couple of questions for you that really follow up on what Senator Peters was asking about with the focus on rural hospitals. I am really concerned, as someone from a small State, your next-door neighbor, New Hampshire, about cybersecurity threats to rural or smaller health care providers.

In 2021, a ransomware attack targeted a small health service in Berlin, New Hampshire, forcing the provider to shut down some of its clinics for several days. Based on your experience as a cybersecurity professional, what are the most significant cybersecurity challenges facing rural and smaller health care providers?

Ms. PIERCE. Thank you for that question, Senator. I believe that some of the biggest issues that these organizations face is the fact that nearly all the staff in a critical access hospital or a small facility wear many hats. They do not specifically focus on cybersecurity, and with the competing priorities that we are now seeing in health care, it is very difficult to focus on something that is not required. If I had 10 things to do today and I knew that two of them were mandated and required for me to do, those are the things that I will focus on.

As we continue to provide guidance and recommendation from the Federal Government we have not seen any minimum standards or requirements from the government which would take us to the point where those would become imperative for facilities to implement. I would urge us to go in that direction but do not do that without supporting us in achieving those standards.

Senator HASSAN. Right, because one of the differences I think you are really referencing is a larger, more metropolitan hospital might have the capacity to have an administrative staff, where somebody with the expertise and focus can really devote themselves to cyber, and in our smaller places, even when they are fully staffed on the patient care side, the administrative staffing tends to be very sparse.

Ms. PIERCE. I agree.

Senator HASSAN. There are a number of resources and tools available for health care entities to improve their cybersecurity, such as the best practice guidance that Mr. Garcia described today in his testimony. But as we have just discussed, rural hospitals are under-resourced, understaffed.

You got at this a little bit with Senator Peters, Ms. Pierce. You were talking about the need to make sure funding is really reimbursing costs. But what specifically can the Federal Government do to ensure that small and rural health care providers are both aware of and have the ability to utilize existing resources and tools for cybersecurity?

Ms. PIERCE. I think the first step that we need to take is to move from guidance and recommendations to minimum standards. Once we do that I believe that those recommendations and guidance will be very helpful in moving that sector to secure their environments.

Currently I have worked with a lot of small hospitals, being with Fortified, hospitals across the country, and invariably they are at a state where there is either absolutely no security program or it is very minimal.

We asked all of our health care organizations to perform risk assessments when we implemented the Health Information Technology for Economic and Clinical Health Act (HITECH). Everyone is now aware of where their risks are, but they are choosing to accept those risks mostly for financial reasons, where they cannot afford or cannot staff their personnel to address those risks.

Senator HASSAN. Your thinking is that some baseline standards and requirements would kind of drive hospitals to work with the Federal Government and others to find out the resources they need and then to actually prioritize that. Is that fair?

Ms. PIERCE. That is fair. Also do not forget, we need to also provide them the ability to actually implement their security measures.

Senator HASSAN. Fair enough. OK.

A question for you, Mr. Garcia. The Health Information Sharing and Analysis Center (Health-ISAC), is a valuable forum where health care partners can share vital cybersecurity information such as intelligence about current and future threats or best practices for addressing those threats. However, as we just heard, smaller health care entities are already under-resourced and understaffed. In your experience, do rural and smaller health care entities have adequate access to the Health-ISAC?

Mr. GARCIA. The Health-ISAC does provide a lot of free resources to the public at large. I think, as Ms. Pierce expressed, however, there is a lot of information out there, and trying to sift through it in ways that would be relevant and actionable to your particular instance, is difficult.

Many hospital systems around the country rely also on regional clusters, information sharing and analysis organizations, peer organizations within a region where there is a trust relationship.

There are a lot of options for how you gather your information. At this point, the Health-ISAC is populated by a lot of very well-resourced organizations that do have sophisticated information security professionals who are really tracking this on a 24/7 basis.

The priority is for every organization to consider what kind of information are you able to actually take in and then take action on.

Senator HASSAN. Are there incentives that we could use to help smaller rural hospitals really access the Health-ISAC, or are there barriers that they have to membership in it right now? How can we help them become more integrated into the Health-ISAC?

Mr. GARCIA. My feeling is it is a small investment. It is an investment into collective defense. But absolutely, I think that some kind of subsidies or financial support for smaller systems to get involved either in the Health-ISAC or other information-sharing organizations. If it is a cost-matching subsidy that would help them

into this kind of a community I think would be tremendously beneficial.

Small hospitals have to make all kinds of existential financial decisions about resource prioritization, so to help them get into a collective organization where you have this communal situational awareness I think is a good first step. You cannot protect against what you do not see.

Senator HASSAN. Thank you. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hassan.

Senator Carper, you are recognized for your questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks. Thanks so much, Mr. Chairman. Thanks for pulling this all together. Important subjects. To our panel, thank you for joining us as well.

My first question I am going to ask each of you to respond to. My second question, if I have time, Mr. Garcia, it will come to you.

A question for all of you, and let us just start with Mr. Martin. It deals with cyber best practices and preventive measures. But when I think about health care I focus on a few key points. One of those is access to health care, making sure Americans broadly have access to health care, affordable health care hopefully. I focus on the quality of the health care that is provided. I focus a lot on prevention, not just dealing with the symptoms or problems but also working on prevention. I also think about a right to privacy and empowering people to do things to help keep themselves healthy.

When it comes to cybersecurity I believe these same issues apply, which leads me to two questions that I want to ask each of you to take a moment to respond to. The first of those question is how can the Federal Government improve access to information on cyber best practices for the health care industry? That would be the first question. The second is how can we make sure that the health care systems are doing their part to take preventive measures to protect their own networks?

Mr. Martin, would you lead us off please?

Mr. MARTIN. Senator, thank you for your questions. In terms of providing access to best practices, there is no shortage of recommendations and guidance and things that organizations could be or should be doing. As I look across the broader industry, the challenge we see is taking stock of all of those different resources and deciding what to actually do, given all those different inputs. As I talked about in my opening statement, one of the key things that the Federal Government can do to help would be to establish a minimum threshold for security best practices, and that threshold can and should continue to change through time. We need to continue to raise all boats here by continuing to advance the state of security in the industry, but having that minimum threshold would be incredibly helpful for our organizations, which then gets to your second question of what can the organizations do.

Today, they are trying to balance lots of different competing priorities, whether you are a large organization or a smaller organization, as Ms. Pierce talked about, trying to balance all those different competing priorities is incredibly challenging. Having that

minimum target to shoot for will help make sure everyone is marching toward that target and ultimately raise the security posture of everyone in the community.

Senator CARPER. All right. Again, the same two questions for the others, and Mr. Garcia, we will go to you. How can the Federal Government improve access to information on cyber best practices for the health care industry? That is No. 1. No. 2, how can we make sure that the health care systems are doing their part to take preventive measures to protect their own networks? Go right ahead.

Mr. GARCIA. Yes, sir. Thanks for the question, Senator. Within the Department of Health and Human Services is an office called the Health Care Cyber Coordination Center (HC3), which is a knowledge center which is growing, and we would like to see that grow more. It is the center that collects information about cyber threats, vulnerabilities, incidents, provides analysis, and then, in turn, pushes it back out to the health sector. They have regular monthly briefings, talking about various threats and what to do to mitigate against those threats. That is a very helpful resource.

On top of that I mentioned earlier the Section 405(d) task group that has produced the Health Industry Cyber Practices. That update is coming out in just a few weeks. It is going to be called HICP 2023. This is a set of best practices, just as Mr. Martin was referring to, that are minimum security practices that all health systems should be implementing, and those are developed by the sector, for the sector, and jointly with HHS.

There is, as Ms. Pierce said, a glut of information security best practices out there. We need to pick one because there is a lot of confusion. We advocate that the Health Industry Cyber Practices is probably the best effort at a joint government publication, freely accessible to all. Then CISA needs to follow and push that along with us. That is No. 1.

Question No. 2 is how can health systems do their part. We have talked about that a lot, and we need to do a culture change. It has been a cultural problem for as long as I have been in cybersecurity that everyone outside of the security team says, "Cybersecurity, that is the security team's job. It is not my job. I am the CIO. I am the Chief Executive Officer (CEO). I am in administration." No. It is actually everybody's job, right down to the clinician.

Indeed, one of the biggest threats in cybersecurity generally is the frontline user, anybody who is touching a keyboard or a tablet or a phone or any kind of medical technology.

Senator CARPER. I am going to ask you to hold it right there. I want to give these folks an opportunity.

Mr. GARCIA. Certainly.

Senator CARPER. Thanks for those responses, though. Ms. Pierce.

Ms. PIERCE. I agree with Mr. Garcia and Mr. Martin. There are a number of best practices available. As Mr. Garcia said, they have published many documents on cybersecurity, so I do not think that there is a lack of information.

What I think is happening, especially for small and rurals, is there is a lack of attention to the information. It is not a priority currently because there are so many other things that are competing for immediate attention. There is no one taking those best

practices off the shelf and actually putting them in practice within those organizations because it is currently a recommendation or a guidance. It is not a requirement.

Senator CARPER. OK.

Ms. PIERCE. I would say the best thing we can do is set some minimum requirements and then begin to embed them into everything that we do in health care. Even with the 21st Century Cures Act there were mandates on interoperability. There has been a big expansion of devices and technologies that have been implemented. But cybersecurity is always a second thought.

Senator CARPER. OK. Hold it right there. Mr. Dresen, I am running out of time. Just very briefly, if you can, to both questions please.

Mr. DRESEN. Thank you, Senator. Very briefly, to complement what my panelists have already stated, I think the other aspect of making best practice information available is ensuring that we have adequate staff to execute and implement those best practices, so advocacy and sponsorship of programming to help build a cyber-educated workforce so that we have qualified individuals who can participate in our organizations to implement those best practices would be extremely useful.

In the context of the health care sector's ability to do that is to hire those people and get them implementing those best practices to support our protections.

Senator CARPER. Great. Mr. Chairman, I will ask, for the record, a question dealing with communications between CISA, HHS, and the health sector. If you receive that question for the record, please respond. That is all I ask.

Thanks, Mr. Chairman.

Chairman PETERS. Thank you, Senator Carper.

I need to leave briefly to be at an Armed Services Committee hearing, so Senator Padilla will take the gavel. But before I leave I will recognize Senator Hawley for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you very much, Mr. Chairman, and thanks to all the witnesses for being here.

This is a topic that is very important to us in the State of Missouri, where we have not only many hospitals, of course, but many rural hospitals, and there have been a number of major cyberattacks against hospitals in the State of Missouri. In September 2021, for example, a ransomware group stole confidential patient information which included names, Social Security numbers, and medical information from a health center in Sikeston, Missouri, which is in the southeast part of our State. In March of last year, it was reported that a hospital affiliated with the University of Missouri Health System experienced a cyberattack in which a third party gained sensitive patient data. A few months ago a hospital based in Marshall, Missouri, found out that more than 112,000 individuals were affected by a data breach. Obviously this is a very significant problem, and I am also concerned about the interplay of foreign adversaries here like China, and I want to get to that in just a second.

Ms. Pierce, if I could start with you and focusing, in particular, on rural hospitals. In Missouri we have 67 hospitals classified as rural hospitals, including one in the town where I grew up. That is about 40 percent of the hospitals in my State. We are a rural State, and proudly so, but I am obviously very concerned about the threat that cyberattacks pose for rural hospitals in particular.

And wonder if just building on the statements you made to Senator Hassan, can you give us a sense, what are the one or two most important steps that you think rural hospitals and rural health care facilities can take to shore up their cyber defenses?

Ms. PIERCE. Thank you for that question. I have had the pleasure of working with some hospitals from your State, and I can assure you that it is not for lack of wanting to address these issues. Part of the issue that I am seeing across the board, from not just Missouri but from other States, is just a lack of funding, and lack and ability to be able to address the issues that they know about.

Some of the things that they could do I had included in my written statement, but top priorities would be they need to obviously have strong passwords and multifactor authentication (MFA). We have done a poor job at implementing strong passwords and MFA, and that is one of the areas where attackers are able to breach our networks. Another aspect that is important is being able to monitor our networks 24/7. Most small facilities have no staff to be able to monitor. Even if they have the tools for a log management or for monitoring the endpoint devices, if nobody is watching the console and nobody is there to pick that attack up then it could be hours, critical hours in a cyberattack, before they even notice that somebody has gotten into their network.

Senator HAWLEY. Let me ask you about the urban-rural divide. How do you assess the current state of cybersecurity in rural hospitals versus urban, and if there is a disparity, as I imagine there is, to what do you attribute that? Is it funding? What are the factors there?

Ms. PIERCE. I would say from my experience, urban hospitals predominantly have staff within their facility, most of them have multiple staff that are addressing each area of the complex issue of cybersecurity. Smaller facilities, from my experience most of them have no staff that are directly assigned to cyber or they have very little staff in that area. I think there is a huge disparity between them.

What is important to know is that most small hospitals are connected to larger tertiary care centers. They need a place to refer their sicker patients. This is the path of least resistance for cyber attackers. When they are trying to figure out how to attack large health systems they are coming in through small hospitals, and we have seen that play out in 2022, where a small hospital is the avenue of least resistance. The cyber attackers attack there, where they know the defenses are low, and actually gain access to a plethora of information.

Senator HAWLEY. Is part of what needs to happen here, these rural hospitals that, as you say, are often part of larger hospital networks, I mean, at the network level do we need to have more staff there that can perform the monitoring? Because I am thinking about the hospital in the town where I grew up. My little town was

the county seat and it was the county hospital, but they did not have excess staff—not that it is excess to cybersecurity, but they did not have a lot of staff. Let us put it that way. What staff they did have were treating patients, which is exactly the scenario you have described.

Trying to think about when we try to find a solution for these rural hospitals and we say, “You need to have staff that are devoted to cybersecurity,” they are going to say, “How in the world would we do that?” Do we need the larger hospital networks, who, at the administrative level, probably do have staff, should they be the ones who are taking on this burden? I mean, what is the path forward here, do you think?

Ms. PIERCE. I think we did allow, through Stark law changes, for larger facilities to assist smaller facilities with their cyber defense, and we saw absolutely no traction in that area. Large health systems were given some leeway to assist and they have not extended those opportunities to small facilities.

I believe that the answer would be to incentivize those facilities to secure their own networks, to ensure that they have access to some funds that will enable them to implement the security that they need to protect their networks.

Senator HAWLEY. Very good. Thank you for that.

Mr. Dresen, if I could just switch to you for a second, I want to talk about China. You write, in the testimony you submitted, about the increasing frequency of attacks from nation-state actors and organized crime. Just drilling in on China for a second, do you have any sense of the number or percentage of the attacks we have seen recently, these cyberattacks, that are committed by Chinese hackers?

Mr. DRESEN. I do not have specific details of the source of attack from China versus Russia versus other countries. It is just significant in terms of the daily barrage we get, and are repelling to help protect us.

Senator HAWLEY. What could the government do, the U.S. Government be doing to help protect hospitals and health care systems from attacks by these nation-state actors, and particularly again given China, where we have heard testimony in this Committee before about the huge increase in cyberattacks, across industries, but arguably none more important than the health care industry. What could the U.S. Government be doing to help counter that?

Dr. DRESEN. We need to take a whole-team approach to solve this problem, where the hospitals and health care sector are the defensive side of that equation and that relationship, where we are defending our organizations and then having the Federal Government bringing higher levels of risk and consequences to those who are attacking us. I think the recent example of the Hive being taken down is a great one to celebrate, a reduction of risks to our organizations.

Getting more aggressive like that to help protect the organizations, and then again, helping to provide more actionable intelligence to the health sector in a real-time manner, to allow us to be as able as possible to protect ourselves with the most current threat information that the government has access to.

Senator HAWLEY. Thank you.

Senator PADILLA [presiding.] Thank you, Senator Hawley.
Senator Blumenthal is next.

OPENING STATEMENT OF SENATOR BLUMENTHAL

Senator BLUMENTHAL. Thank you, Senator Padilla. Let me pursue that question. Would it not be important for our law enforcement and intelligence agencies to take more proactive and maybe more aggressive action with respect to China and Russia if they are condoning or even encouraging ransomware attacks?

Mr. DRESEN. We would certainly promote and advocate for increased collaboration between government agencies, especially those who have threat intelligence and awareness of those types of activities.

Senator BLUMENTHAL. More than just collaboration. Should there not be greater focus, or resources devoted to it, and more prosecution? Obviously, prosecution may be difficult because the actors may be beyond our jurisdictional reach, but certainly there are sanctions that can be imposed.

Mr. DRESEN. Opportunities for attribution are challenging in these types of circumstances, and so when that is possible I would certainly support it. The actionable threat intelligence that these entities can share with us to help us better protect ourselves defensively would be extremely helpful.

Senator BLUMENTHAL. Do you think there is actionable intelligence that right now is unshared?

Mr. DRESEN. I think there probably is in the context of active investigations that may be taking place. The opportunity to share that with our sector as much as they can would be encouraged.

Senator BLUMENTHAL. Do you know of specific investigations that have not been shared?

Mr. DRESEN. I do not.

Senator BLUMENTHAL. Do you hear from colleagues in the industry about such investigations?

Mr. DRESEN. Not typically, no.

Senator BLUMENTHAL. Why do you say there are?

Mr. DRESEN. I think there is a perception that from law enforcement, when they tell us that they may have investigations they cannot share information with us, they do not give us specifics. They just make us aware that there are active investigations. Then we see through press reports when they do release information, like the Hive getting taken down. You understand that was a very long process that it took them to take that action, and so you understand that those types of activities take time to work themselves through.

Senator BLUMENTHAL. If there were more effective prosecution, either by the Department of Justice (DOJ) or by other agencies, it would have some deterrent effect.

Mr. DRESEN. I think any improvement in our ability to defend ourselves from those threats would be helpful.

Senator BLUMENTHAL. Do any of the other members of the panel have responses on this issue?

Mr. GARCIA. Yes, I would say that there are innovative ways to deal with this before there is an opportunity for prosecution, that is various forms of takedown. I was with the financial services sec-

tor some before this, and we worked closely with the Justice Department to identify criminal groups that were waging botnet battles, that is hundreds of thousands or millions of computers infecting major system. We worked with the Justice Department, using available statutory authorities such as Racketeer Influenced and Corrupt Organizations (RICO) Act, to do simply take down the network that was operating the botnet. It was a proactive way of dealing with it.

Other actions are clearly classified in the intelligence community (IC) that the private sector does not participate in, but there is a lot of information that cannot be shared with industry because it has been classified or it is under investigation, as Mr. Dresen said.

Senator BLUMENTHAL. Should more of it be unclassified to help industry safeguard itself?

Mr. GARCIA. I think there is general consensus that there is a problem of over-classification in the government. Too much information is being classified unnecessarily. Indeed, information that sometimes flows from the private sector to the government is subsequently classified.

Senator BLUMENTHAL. In other words, information comes from open public sources, it is provided to an agency of government, and then it is classified?

Mr. GARCIA. Because there may be additional intelligence attached to that, that adds nuance or context.

Senator BLUMENTHAL. Would you like to see more effective investigation, more takedowns, more prosecution by the Department of Justice or other agencies?

Mr. GARCIA. Certainly. Absolutely. Any way that the government can help disrupt incidents before they happen, based on intelligence that it may or is about to happen, that would be helpful to the industry, to all critical infrastructure industries.

Senator BLUMENTHAL. Do you or other members of the panel have any indication that there is sometimes cooperation within the victim institution that enables the hackers to gain access?

Mr. GARCIA. Insider threat is a typical problem. Most often, insiders within a company are just making inadvertent errors. Others, there are disgruntled employees, and that is pretty common anywhere, whether it is cyber or financial fraud or other issues.

Senator BLUMENTHAL. I do not know whether anyone else has anything to add on this topic, but it is one of great interest to me because I think we have devoted insufficient resources and priority to these kinds of attacks, which are threatening, seriously threatening to the health of our Nation, not to mention to privacy. Would you agree?

I see most heads are shaking in the affirmative, let the record show.

Let me ask, in terms of the other aspects that are problematic, as you may know, Cerebral and BetterHelp are mental health startups that shared data with social media platforms, in other words, sold or monetized that data. The Federal Trade Commission (FTC) fined BetterHelp for sharing that health care data to profit from targeted advertising.

Given the increasing sharing of health care data, what kind of privacy and security standards would you think should be en-

hanced or improved to prevent the abuse of that sharing? I will ask the panel as a whole.

Mr. GARCIA. I would say, Senator, that there is an increasing amount of personal health information that is circulated and not regulated, based on wearable technologies and home medical technologies. There have been groups, other than ours, that are looking into what kinds of data are being shared that are not under some kind of regulatory scrutiny, and then how do we shore that up. I do not have specific answers on that for you.

Senator BLUMENTHAL. Cerebral recently disclosed it had shared personal data of over 3.1 million American patients with TikTok, Facebook, and Google. Obviously, this is not a cyberattack, but it is an attack on the patients, not an attack as perhaps we would characterize it normally. But it is an attack on their privacy, and I invite you to think more about it and respond in writing if you have any additional ideas.

Thanks, Mr. Chairman.

Senator PADILLA. Thank you, Senator Blumenthal.

OPENING STATEMENT OF SENATOR PADILLA

It is my opportunity to ask questions next, and continuing on with that last question, or issue that you raised, Senator Blumenthal, I may, in my time, hopefully get to a follow-up question on that, because it may not be a cyberattack but hugely significant vulnerability that you raise.

Our health care system is uniquely important and vulnerable to cybersecurity attacks and vulnerabilities, and the issue touches all of our constituents. As has been discussed, data breaches and ransomware attacks on health care providers and third-party device makers have affected millions of Californians alone. I reviewed the mandatory breach notifications filed with the Department of Health and Human Services, and as of yesterday morning, there are 63 different California-based breaches of unsecured protected health information under investigation, affecting over 90 million people. That is more than two times the State's population, so the national scale of the problem is alarming.

In addition to the inappropriate disclosure of personal information, any disruption to the systems used in the health care and public health care settings could be catastrophic for many Americans who rely on their services for care. I thank Chairman Peters for holding this important hearing.

The first question may seem a little basic, and maybe a little softball, but I think it is critical for folks that are following this person, in person and online.

Breaching in the health care sector allow for the disclosure of patient health information as well as Social Security, other personal identifiable information (PII), and sensitive information. I want to be sure that the public appreciates why this information is so sensitive for patients and why the health care sector, in particular, is such an attractive target for attacks.

I will direct the question to Mr. Martin. Why is personal health information so sensitive and valuable to those who seek to steal it?

Mr. MARTIN. Senator, thank you for the question. Part of what makes health care data so sensitive is that it does not change, that

it is something that continues to grow, but it is not something that can be reset or changed, like a password or credit card number or something like that. Once it falls into a bad actor's hands, that information can be used in perpetuity to purport future crimes, whether that is identity theft or blackmail the individual. Those types of things then become possible forever as opposed to something where an individual could take an action to stop that happening in the future.

Senator PADILLA. Thank you. It is, again, important, I think, to put a spotlight on.

Now according to a report last year from the cybersecurity firm, Sophos, 66 percent of health care organizations, two-thirds, were hit by ransomware attacks last year. Forty-four percent of health care organizations suffered an attack in the last year, and took up to a week to recover from the most significant attack, and 25 percent of them took up to a month.

I will direct the question to Mr. Garcia. Can you speak to the specific challenges that health care organizations face in recovering from a ransomware attack and the resulting impact on people seeking medical care? I think a more direct version of the question that Senator Hawley asked, vis-a-vis foreign actions, how can the government help reduce the recovery time?

Mr. GARCIA. That is a very good question. Many hospitals that are disrupted by ransomware attacks are unable to schedule appointments, they are unable to perform procedures or surgeries. They have to go to a paper-based environment. Our graduating medical students these days have never seen a pad of prescription paper with a pen. It is all electronic now.

Senator PADILLA. Does that mean their penmanship is even worse?

Mr. GARCIA. Their penmanship is even worse. It is now all thumbs.

Getting back online, we actually put together a resource for health systems that have been disabled for an extended period of time. It is called "Operational Continuity After a Cyber Incident," and there are many steps that need to be taken to ensure that you appropriately sequence getting infected systems back online so that they are not reinfected, and prioritizing continuity of care to those patients who need it most, and that includes getting your financial systems back online so that you can get reimbursement so that you do not go into the red and insolvent.

Recommendations about what the government can do to help, one of the things we have been discussing and we sort of touched on, on this panel, is can there be a strike force from the government that can come in and help with, whether it is CISA or HHS, to help with reconstituting systems and bringing things back online, doing the forensics and the triage at a cybersecurity level for those smaller systems. That could include some kind of financial assistance to make sure that the priority is going to patients while they are bringing systems back online.

Senator PADILLA. Thank you. In my time left I want to raise one more issue and question. Today there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide. Both private and public sector employers face challenges in recruiting,

personnel, hiring, and retaining professionals to fill these vacancies, which negatively affects our collective cybersecurity.

Growing talents is a priority under the recently released White House National Cybersecurity Strategy and Congress. Mr. Garcia and Ms. Pierce, can you speak to the specific and unique challenges in the health care sector as far as identifying, recruiting, hiring, and retaining IT professionals, and do you have any recommendations for us today?

Ms. PIERCE. Thank you for the question. I can personally share that recruiting and retaining cybersecurity staff is a daunting task for a small facility. I do not believe that there will be a time when small hospitals will have dedicated cybersecurity staff in-house. I believe moving to a managed service provider type environment where those types of services are outsourced to the people whose business is cybersecurity defenses.

Hospitals' main priority is taking care of patients. It is health care. That is their mission. It is not cybersecurity. I believe if we go to a model where those things are more outsourced it would be beneficial for smaller facilities.

Senator PADILLA. First do no harm, and I think that is inclusive of protecting somebody's personal and health information. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Senator Padilla. I really appreciate it. We are all going to build off of each other on these questions, and I really want to thank you all for being here today, for the work you are doing.

Of course, we are here to talk about health care cybersecurity. As one of the 16 critical infrastructure sectors, securing the health care and public health sector we know is critical to protecting our national security, for obvious reasons. Over the past three years, the health care data breaches have doubled. In addition to threatening patient privacy and security, as all of my colleagues have mentioned, these attacks ultimately drive up the cost of health care as well, as there have to be more investments made in protecting this data.

Last Congress Senator Cassidy and I introduced the Healthcare Cybersecurity Act. It was bipartisan legislation that would require CISA to coordinate with and make resources available to health care entities, including by developing products tailored to the specific needs of small and rural hospitals and health clinics, to what you are speaking to, Ms. Pierce. You spoke to maybe a task force or separate businesses for ransomware security issues.

But Mr. Garcia, and then Mr. Dresen, maybe you can speak about how we could maybe, in the meantime, or instead of doing that, or in conjunction, how can we provide cybersecurity training to the health care assets owners and operators so that we can empower them to be partners in this, instead of just maybe turning it over, that they are engaged and empowered, especially these small and rural hospitals. Like you said, they do not have the capacity to have IT staff. But we want their empowerment and engagement.

If you could speak to that. First, Mr. Garcia, and then Mr. Dresen.

Mr. GARCIA. Certainly. Thanks for that question, Senator. I mentioned previously a resource that the health care industry, our Council, and HHS together produced called Health Industry Cybersecurity Practices, which is intended to provide the top ten cybersecurity best practices that health systems need to implement to be cybersecure. This is a strong partnership between HHS and the sector, and we look to CISA with the technical support. They have regional cybersecurity advisors all over the country and they do provide assistance, technical assistance, not just to health systems but to many other industry sectors.

We would like to see them use the HICP in their engagement with health systems around the country, because CISA does not itself have health care expertise. They need to rely on their sector risk management agency, HHS, as the guiding force for the technical support that CISA should provide. We believe that the HICP and the HICP which is based on the NIST Cybersecurity Framework, which is by now a de facto standard, that is the best way to provide focused level of controls to the health care industry and try to remove some of the noise around too many choices to implement.

Senator ROSEN. That is right.

Mr. DRESEN. Thank you, Senator Rosen. I would call two examples of opportunities I think could demonstrate how we could be more effective collaborating together. The first is an organization in the State of Michigan called the Michigan Healthcare Cybersecurity Council, and it is an organization that has been together for about 10 years, and originated with the sponsorship from the Governor's Office at the time. It brought together all the health care entities in the State of Michigan to create an environment where we could have a collaborative discussion around cybersecurity issues, we could share best practices. It connected large systems with small systems so that you gave that connectivity and access to expertise to everybody in the State to help improve the State of the health care sector overall.

Connecting programs like that to CISA, as Mr. Garcia suggested, is an excellent way to connect the knowledge with the ability to deliver that information to the people who most need it.

The other example I would share is an organization in Grand Rapids called the West Michigan Center for Arts and Technology, and they have an innovative program, and Senator Peters had a chance to visit last year, and we thank you, Senator Peters, for you doing that. It is a program to train diverse students who are interested in entering the cybersecurity field, and is a tuition-free program that puts them through education delivered by a partner entity out of California. They come out of that program with certifications and employability in the cybersecurity field, which enables them to have a living wage for them and their families and provides a well-needed access to talent that is needed in the health care sector.

Advocacy for and sponsorship of those types of programs at the Federal level can help local entities deliver that talent where it is most needed.

Senator ROSEN. Thank you. Collaboration amongst entities and building the pipeline through apprenticeships, those are some of my future questions, so we will collaborate and get the information from Chair Peters.

But also we have been talking a lot about our medical device cybersecurity. It is very important people have the test of pacemakers, all kinds of things. You just call in on your phone and they get all of those results. I did have a bill last year to strengthen medical device cybersecurity, the updated the Food and Drug Administration (FDA) guidance, and it was included in last year's FDA package and became law as part of the omnibus. I do hope, in conjunction with the other things we are working on, that this legislation becomes a platform for FDA and CISA to work together going forward. You have spoken a lot about it, but we are beginning to give those tools.

But I want to build out a little bit about your, in the minute I have left, Senator Padilla's question and everyone's question, is building and expanding our workforce because there are nearly 800,000 cyber jobs. In every single sector we are facing these same challenges. I have introduced a bill with Marsha Blackburn, the Cyber Ready Workforce Act, to surge up capacity with the Department of Labor (DOL) to award grants to increase access to things like a registered apprenticeship program that is going to lead to an industry-recognized certification, encourage those stackable and portable credentials so people can get into the system.

Mr. Garcia, since Mr. Dresen already talked about it, can you explain how we could improve and expand these apprenticeship programs through public-private partnership, through a community college, that will really help get people working in the industry and then they can move up where they need to?

Mr. GARCIA. There are lots of ideas to that effect, and one that could even be modeled the medical profession itself, that is there is a loan forgiveness or some other kind of subsidies for medical students when they go into small to rural settings, that they will be forgiven some medical school debt.

Senator ROSEN. I have some of that legislation myself I have sponsored.

Mr. GARCIA. That is perfect. The same can be done for cybersecurity, and we have that with the National Security Agency Centers for Academic Excellence in Cybersecurity, scholarship for service by National Science Foundation (NSF). There are various ways that we can incentivize students to study cybersecurity and then go into the workforce where it is most needed and get some level of compensation for that.

Senator ROSEN. Thank you. I see my time has expired. Chair, you are back, Chair Peters. Thank you.

Chairman PETERS [presiding.] Thank you, Senator Rosen.

Senator Sinema, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Mr. Chairman, and thank you to the witnesses for joining us today.

Last year, when Yuma Regional Medical Center fell victim to a ransomware attack, 700,000 patients were notified that their per-

sonal health data had been stolen. But when a hospital is hacked it is not just Arizonans' sensitive data that is placed at risk. Particularly in rural communities where alternative hospitals may not be available, crippling cyberattacks can literally be matters of life and death.

This is also true in other health care contexts. Last year, the National Suicide Hotline was brought offline by a cyberattack, resulting in an entire day where Arizonans facing mental health emergencies could not call 988 and receive the support they needed.

My first question is for Mr. Dresen. Imagine looking in the eyes of a parent whose child may have called the Suicide Hotline on December 1st but was not able to get through due to the cyberattack. I am committed to ensuring that our nation's suicide prevention system is better prepared for the next attack. The question for you is, what lessons should other public health stakeholders take from the hack on the 988 lifeline?

Mr. DRESEN. Thank you, Senator, for your question. It is unfortunate. The event on the 988 attack was a sobering reminder of the impact to critical health care services when cyberattacks have successful outcomes. It reminds us all of the importance of being very aware of the risks we face as a health care sector to deliver those services, the need to have an adequately funded and staffed team that can implement the protections to protect us, and the understanding that we can only do so much to protect us and cannot eliminate all risk. It requires the partnership of the government to help us provide additional protections, increasing risk and consequences for those who attack us, and the understanding and the support when we are attacked that we are the victims, and help us work through that process and do not penalize us for being attacked.

Senator SINEMA. Thank you. Ms. Pierce, a few years ago hackers took Wickenburg Community Hospital, the only hospital in a small Arizona community, offline. Fortunately, the talented IT team in Wickenburg had backed up the hospital's data and then worked around the clock to quickly rebuild their system from scratch. But not all community hospitals or other rural or tribal health care providers are so fortunate. Many simply do not have the resources or the cybersecurity expertise to quickly recover.

Given your experience with the rural health system, can you discuss some of the unique cybersecurity challenges that are facing smaller hospitals?

Ms. PIERCE. Thank you for the question. I think that smaller hospitals have a varying degree of ability to recover from those attacks. One of the things that is imperative is that the attacks are identified and remediated quickly. I am not aware of the particular attack you are speaking of, but I would imagine that they identified quickly that there was an issue, took things offline immediately, and were able to restore from backup.

Frequently cyberattackers have been within the network and been able to not only compromise existing systems but have also compromised the backups. The challenges can be extensive in recovery to that type of attack and we have seen some health systems, even larger systems, take weeks, if not months, to recover.

I would say that there is no one answer to that question. There is a wide range of abilities and talent within rural communities. I think that your particular hospital was the exception, not the rule, when it comes to cyberattacks.

Senator SINEMA. Thank you. Mr. Garcia, today ransomware attacks against hospitals are mostly financially motivated, but tomorrow cyberattacks may target specific patients with the intent to kill or injure them. As more Arizonans receive wireless medical device implants, the possibility that a hacker could disable a pacemaker or manipulate an insulin pump is something we need to take seriously.

How could public and private sectors get ahead of this threat and ensure that wireless medical devices meet the most rigorous cybersecurity standards?

Mr. GARCIA. Yes, that is a very good question. Thank you, Senator. There is a lot of work being done in ensuring the security of a variety of connected medical devices—wireless, wired, and otherwise. The idea of pacemakers and such, the one issue about that is it is one of those low probability, high impact kinds of events. You have to be right next to somebody with a phone to actually communicate with the pacemaker.

Senator SINEMA. Right now.

Mr. GARCIA. Yes, right now. What we are concerned about, however, is a much broader attack, where patient data can be corrupted in a much broader scale within a hospital system, so that anybody who is being treated in a hospital can be given the wrong dose of medicine, or the wrong treatment based on corrupted data about their specific patient data.

That is the much higher risk that we need to be concerned about. Meanwhile, the medical device industry, through the Sector Coordinating Council, is working hard to develop standards of practice for how you design, develop, manufacture cybersecurity into medical devices, connected wirelessly, Bluetooth, whatever, from the ground up, so that they are secure by design. That is an ongoing and long-term program that the medical device community is acutely aware of.

Senator SINEMA. Thank you. Mr. Dresen, if a ransomware attack affects an emergency room, even if we are able to restore those systems within one hour, some patients may not live that long. This sense of urgency incentivizes hospitals to pay ransoms to hackers, something, of course, that the Federal Bureau of Investigation (FBI) and CISA advise against. Although paying may protect specific patients in hospitals in the short term, it also, of course, guarantees and perhaps incentivizes that hackers will continue targeting hospitals in the future.

How do you believe that hospitals should navigate the decision of whether or not to pay a ransom, and how can the Federal Government help hospitals enhance their cyberattack prevention and mitigation capabilities so that the question of whether to pay or not to pay becomes irrelevant?

Mr. DRESEN. It is our policy to align with the FBI guidance to not pay ransomware, and so we do everything we can to mitigate the risk that that is going to happen. We do that by evaluating the risk we have to our organization of a cyberattack, making invest-

ments with our leadership support to ensure we have protections in place to reduce the likelihood that that is going to happen.

The support we can gain from the government to help further mitigate that risk is improved threat intelligence sharing that is actionable and near real-time, so we can have the most up-to-date information available to us to help protect us, as well as, again, reinforcing educational programs that can help train qualified staff that we can have work with us to ensure we can implement the best practice recommendations to protect our organization.

Senator SINEMA. Thank you. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Sinema.

I would like to thank our witnesses for joining us here today and for your contributions to what is a very important conversation. As we heard today, cyberattacks against our health care sector can result in tragic consequences and can cause serious disruptions to patients' lives.

As Chairman of this Committee, I have worked on a bipartisan basis to significantly strengthen our nation's cybersecurity, and I hope that we can build on those efforts by making sure the Federal Government can provide additional support for our most frequent targets of ransomware, including the health care sector. I urge my colleagues to join me in these efforts to ensure our nation can continue to combat these threats and build resiliency into our critical infrastructure. Our witnesses' testimony today will help inform the Committee's future legislative activity as well as oversight on this issue.

The record for this hearing will remain open for 15 days, until 5 p.m. on March 31, 2023, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:34 a.m., the hearing was adjourned.]

A P P E N D I X

**Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: In Need of a Checkup: Examining the Cybersecurity Risks to the
Healthcare Sector
March 16, 2023**

Today's hearing will examine cybersecurity threats facing the healthcare sector, how both the federal government and health care providers are working to combat these threats, and what actions Congress should take to bolster our cybersecurity defenses against these attacks.

Health care is a rapidly growing sector of our economy that employs more than 18 million workers, and is made up of both public and private sector organizations related to patient services, medical devices and manufacturers, and electronic health and medical records, that store considerable amounts of personal information, making them frequent targets of attacks.

In recent years, increasingly sophisticated cyber-attacks in the healthcare and public health sectors have posed alarming threats to people in Michigan and across the country.

Cyber-attacks on hospitals, and other health care providers, can cause serious disruptions to their operations, and prevent them from effectively providing critical, lifesaving care to their patients. Breaches can also lead to the exposure of sensitive personal and medical information of patients and health care personnel.

Most recently, the DC Health Link, a health insurance marketplace for residents and lawmakers in the nation's Capital, experienced a cyber-attack that exposed the personal data and information of tens of thousands of people, putting victims at risk of identity theft, scams, and additional cyber-attacks.

Earlier this year, in my home state, the University of Michigan Health System experienced a cyber-attack that temporarily limited access to their public websites. Thankfully in that attack, no patient information was compromised and the issue was quickly resolved.

These relentless cyber-attacks show that foreign adversaries and cybercriminals will stop at nothing to exploit cybersecurity vulnerabilities our critical infrastructure and most essential systems.

What is most concerning about these attacks is that they don't just compromise personal information, they can actually affect patient health and safety.

Last month, a ransomware attack on Tallahassee Memorial HealthCare in Florida took the hospital's IT systems offline for more than a week, and required them to divert patients to other facilities and cancel procedures until they could restore their networks.

A 2019 catastrophic ransomware attack on the Spring Hill Medical Center in Mobile, Alabama may have even led to a patient's death. The attack prevented health care providers from using equipment to monitor a baby's condition during delivery. As a result, the infant tragically passed away because of delayed medical care.

This shocking example shows just how grave the consequences of cyber-attacks in the healthcare sector can be. Given the threats facing this sector, and the potential life or death consequences, there is no question that investments in healthcare cybersecurity are also investments in patient care.

This Committee has already taken important steps to strengthen cybersecurity for our critical infrastructure sectors, including the healthcare sector. Last Congress, the Committee advanced a bipartisan bill I introduced along with Senator Portman to require these organizations to report cyber-attacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency.

This law will help ensure that government is able to better track cybersecurity threats to our critical infrastructure, provide more transparency and situational awareness for our cybersecurity defenses, and enable CISA to warn potential victims of ongoing attacks, so they know if they could be a target next.

This is an important first step, but there is much more Congress can do to ensure that critical networks in our healthcare and public health sector remain resilient against cyber-attacks.

I'm grateful our colleague, Senator Rosen, is leading efforts to that would improve the way CISA and the Department of Health and Human Services share information about cybersecurity threats with the healthcare sector, as well as provide cybersecurity training to medical professionals. I look forward to working together to build on these efforts.

Today, I am pleased to have an expert panel of healthcare cybersecurity professionals who can speak more about the challenges we face and discuss potential solutions.



*In Need of a Checkup: Examining the
Cybersecurity Risks to the Healthcare Sector*

Witness Testimony of Scott Dresen
Senior Vice President, Information Security &
Chief Information Security Officer

Before the Senate Homeland Security
and Governmental Affairs Committee

March 16, 2023

Chairman Peters, Ranking Member Paul, and members of the Homeland Security and Governmental Affairs Committee: thank you for inviting me to testify this morning. It is an honor and privilege to be speaking with you about this very important issue. I am the Chief Information Security Officer for Corewell Health which, as the largest integrated health system and largest employer in Michigan, is committed to health and wellness so that people can live their healthiest life possible.

In the spirit of our mission to improve health, instill humanity, and inspire hope, I am here to talk about cybersecurity threats to the healthcare sector which could compromise our health system's ability to effectively provide access to and deliver healthcare services to our patients and members. Of particular concern are high impact ransomware attacks which disrupt and delay health care delivery, may cause risk to patient safety, and used to conceal activity by threat actors to exfiltrate personal health information.

Healthcare is digitally dependent; we are in a world where healthcare is highly digital and highly connected. And that makes us vulnerable given the value of the data we manage. We have a responsibility to protect the data of our patients and members. This obligation and the associated risks are of the highest priority across our system leadership and Board of Directors.

Healthcare is a complex business model whereby multiple, often independent, entities come together to form what the patient sees as a cohesive care delivery process. Over time and often out of necessity, this model has evolved in ways that has made us more vulnerable to cyber-attacks. For example, the rapid expansion of network-connected technologies to provide telehealth during the COVID-19 pandemic increased the attack surface targeted by criminals. Other examples include increased use of third parties to provide services, expanded use of Software as a Service, and other cloud-based solutions. This has expanded the footprint of healthcare systems that must be protected and increases the opportunities for threat actors to compromise an organization.



Media reports of cyber-attacks, data breaches, and unintended exposure of sensitive data underscores the vulnerability of healthcare systems to these disruptive incidents and the impact to our patients and members. Operational disruption prevents patients from being able to receive the care they need when they need it. Material financial impact in the form of fines, penalties, and associated remediation costs increase financial pressures significantly. Brand and reputational impacts can have lasting consequences on organizations victimized by cyber-attacks. These issues only serve to undermine the trust our communities have in our healthcare system and our ability to serve them in their most vulnerable time of need.

A comprehensive information security program is critical to manage these risks. Yet there exists significant disparity in the healthcare sector for organizations to resource an effective security team and the necessary technology to provide the requisite protections to reduce the risk of an attack. Small and medium sized healthcare systems are at a significant disadvantage compared to larger systems to be able to recruit, retain, instrument, and fund an effective information security program. And despite the advantage larger organizations have in comparison, the increasing trend of attacks prove even the largest organizations are vulnerable and can be compromised.

The increasing frequency of attack from nation state actors and organized crime has created a sense of urgency within the healthcare sector and we need help from the United States government to respond to these threats more effectively. Requirements for inter-agency sharing of cybersecurity threat intelligence is a productive step forward. We need more of this and need that enhanced collaboration to include critical infrastructure sector participation including the ability to automate threat intelligence data sharing with sector participants enabling rapid, near real time automatic ingestion of threat intelligence into the technologies participating members use to protect their respective organizations. The United States government has actionable intelligence that would be of immediate value to the healthcare sector. While there is some degree of automated intelligence sharing, we need to make more of that intelligence accessible.

We are in an environment where keeping up with the technology to defend against advanced persistent threat is extremely expensive. Many of these technologies aren't an option for financially disadvantaged healthcare systems due to cost. We recommend creating incentives to make technology more affordable and accessible to the entire healthcare sector.

We recommend reforms on the penalties healthcare entities face because of cyberattacks and related data breaches. We understand and support the legislative intent to encourage adoption of best practices and the implementation of appropriate protections to safeguard our data. However, penalizing victims of cyberattack, when defensive measures can't keep up with the sophistication of hackers, is not the fair approach.

We are at our best and most capable when it comes to caring for our patients and members. That is our expertise. Our adversaries are at their best and most capable when they are attacking us. They are extremely well-funded, extremely talented, and highly motivated. Many are either nation state actors or sponsored and supported by nation states. We can't beat them alone.



In conclusion, we can be more effective by enhancing existing partnerships with and between U.S. government agencies, expanding the sharing of actionable threat intelligence, incentivizing access to affordable technology to defend against advanced threats, and reforming legislation to encourage the adoption of best practices while not penalizing the victims of cyberattacks.

Thank you for this opportunity to testify and I look forward to your questions.

Testimony of

Katherine (Kate) Pierce

Former Chief Information Officer & Chief Information Security
Officer,

North Country Hospital

and

Current Senior Virtual Information Security Officer
& Executive Director of Subsidy,
Fortified Health Security

Before the

United States Senate

Homeland Security & Government Affairs Committee

March 16, 2023

Introduction

Chairman Peters, Ranking Member Paul, and members of the Committee, my name is Katherine (Kate) Pierce. I served as the CIO and CISO for a Critical Access Hospital for over 21 years and I currently serve as a Senior Virtual Information Security Officer and Executive Director of Subsidy for Fortified Health Security. I want to thank you for this opportunity to address the Committee on Homeland Security and Government Affairs and provide an industry perspective on cybersecurity threats in the health sector, the current challenges small and rural healthcare organizations face, the dangers of exposing healthcare sensitive data to adversaries, and the impact to communities when healthcare organizations experience cyberattacks. I also herein respectfully submit recommendations on how this committee can assist healthcare organizations in improving their overall cybersecurity posture.

Background

North Country Hospital and Health Center, Inc.

North Country Hospital is a Critical Access Hospital (CAH) located five miles from the Canadian border in the Northeast Kingdom of Vermont. It offers healthcare services to the 27,000 residents in Orleans and North Essex County, as well as visitors who travel to enjoy the area's recreational resources. In its 100 years, the medical campus has grown to include fourteen clinics, including primary care, a surgical suite, obstetrics & gynecology, 24-hour emergency department, pediatrics, an intensive care unit, medical/surgical floor and branches for dialysis, orthopedics and sleep

disorders, as well as areas for radiology, laboratory and physical therapy. In addition, services are provided at four rural health clinics in Orleans County.

Fortified Health Security

Fortified is a leading national cybersecurity partner to thousands of healthcare facilities across the U.S., providing managed advisory and security services that help clients protect patient data and reduce risk. A recipient of multiple industry accolades, Fortified was recently awarded a second Best in KLAS award for Security and Privacy Managed Services. Since its inception, Fortified has works alongside healthcare organizations to build customized programs and processes that reduce risk and increase their security posture over time by helping them address challenges with human capital, technology and security best practices. Led by a team of industry-recognized cyber experts, Fortified publishes the nationally recognized "Horizon Report."

Fortified is actively driving the national conversation around healthcare cybersecurity. Its monthly Roundtables address current threats, new technology, and strategies to harden cybersecurity postures and address incidents. Fortified's experienced cybersecurity leaders are frequently interviewed and featured in national trade publications. And Fortified is also a member of the Cybersecurity Working Group of the Healthcare Sector Coordinating Council.

Current Cyber Threat Landscape in Healthcare

Recent Healthcare Cybersecurity Updates

The top cyber threats for healthcare in 2022 were phishing, ransomware, data breaches, and DDoS Attacks. While these threats were prevalent across the breadth of critical infrastructure, in 2022 healthcare continued to be the top focus, with 148 of the 649 cyberattacks on critical infrastructure targeted at healthcare organizations.

There are multiple reasons for this, but two primary lines of thought are that healthcare data records are worth in excess of fifty times more than other records on the dark web ([Industry Voices-Forget Credit Card Numbers. Medical Records are the Hottest Items on the Dark Web](#)), and that, due to the time-sensitive nature of healthcare services, hospitals are more likely to pay the ransom (61% paid ransom in 2022) ([The State of Ransomware in Healthcare 2022 - Sophos News](#)).

Shift in Focus of Cyber Attackers

Another alarming trend that escalated in 2022 was cyber attackers shifting focus to small and rural hospitals. While most larger health systems have implemented advanced cybersecurity hygiene to thwart attacks and are employing large cybersecurity teams with sophisticated defenses, small facilities continue to struggle. In fact, there is a large disparity in cybersecurity spending when it comes to small- to medium-sized rural facilities. Sadly, this is not only well-known to hospital systems, but to cyber criminals as well. Fierce Healthcare reported in August of 2022 that “Smaller hospital systems and specialty clinics often lack the same level of security preparedness, staff size or budget and have weaker cyber defenses. Attackers are

continuing to push the envelope and change the playing field when it comes to healthcare data breaches and attacks. The move from large hospital systems and payers to smaller entities that have a deficit in their Cyber defenses shows a massive change in victims and approach. As we continue into 2022, we anticipate attackers to continue to focus on smaller entities for ease of attack, but also for evasion of media attention and escalation with law enforcement.” This concept was reinforced by Healthcare Dive, stating, “Cyberattacks are pivoting to target smaller healthcare companies and specialty clinics without the resources to protect themselves, instead of larger health systems that – despite being treasure troves of personal and medical data – generally have more sophisticated security.” The overall national risk for healthcare is compounded when we consider that the majority of smaller hospitals are connected to larger systems, so when cybercriminals attack the small facility, it is often the “path of least resistance” into much larger healthcare networks.

Increased Time to Recovery and Escalating Average Cost of Breach

The length of time required to recover from a breach increased, and the cost for recovery climbed to \$10.10 million in 2022, with CommonSpirit reporting more than \$150 million in recovery costs [Healthcare and cybersecurity in the U.S. - Statistics & Facts | Statista](#). Both of these statistics are especially significant to smaller organizations, when considering an Expert Insight survey that showed the average recovery time is 33% longer for small organizations, and the cost per hour of system outage is 55% higher for this group than for hospitals over 1000 beds. [Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know | Expert Insights](#)

Current Challenges Faced by Small and Rural Organizations

Budget Constraints

Rural healthcare facilities are facing unprecedented economic challenges, which could quickly lead to a sharp decline in the number of hospitals available to our rural communities. When we consider the barriers to strong cyber programs, a Becker's Health IT article from December 2022 indicated that inadequate budgets are the number one issue keeping healthcare organizations from achieving more effective cybersecurity protections. This is especially true for small and rural facilities, with many facing severely strained budgets and danger of closure. Michael Topchik, national leader for Chartis, indicated this month that 43% of rural hospitals are operating in the red ([Nearly Half of Rural Hospitals Are Operating in the Red, Study Says \(dailyonder.com\)](#)), and a recent AHA Report outlines the closer of 136 rural hospitals between 2010 and 2021, with 19 in 2020 alone. The report indicated that in addition to lower patient volumes, rural hospitals often treat patient populations that are older, sicker and poorer compared to the national average. For example, a higher percentage of patients in rural areas are uninsured and 26% of uninsured, rural patients delayed seeking care due to cost. The Crisis in Rural Healthcare report indicates that, "More than 600 additional rural hospitals - nearly 30% of all rural hospitals in the country - are at risk of closing in the near future."

A few of the prevalent contributing factors to the economic distress of these rural healthcare providers include the severe shortage of clinical staff leading to significant

wage hikes, the increased need for scarce behavioral health services, a shortage of long-term care beds creating extended stays which are reimbursed at lower levels, and a sharp increase in supply chain and technology costs. Rural hospitals also tend to have lower overall reimbursement rates, which is projected to worsen as the end to the PHE takes effect, with as many as 15 million Medicaid patients anticipated to lose coverage ([The End of the PHE: How Providers Can Cope With the Impact of up to 15 Million Medicaid Enrollees Losing Coverage \(beckershospitalreview.com\)](#)). With the large number of competing priorities within these small health systems, it is difficult, if not impossible, to focus on cyber defenses. Budgets are strained, and with cybersecurity not seen as a priority for small and rural hospitals, cyber initiatives are often some of the first items cut from operational and capital budgets.

Security Staffing

Cybersecurity staff resources nationally are in high demand, and this shortage of cybersecurity skilled professionals is not ending anytime soon. According to the 2022 ISC2 report, "Despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce." ([ISC2-Cybersecurity-Workforce-Study.ashx](#)). I have had the opportunity to interact with small and rural hospitals across the counter, and most facilities have little to no trained security personnel on staff. Every member of the organization wears multiple hats and is spread extremely thin. The IT teams are generally very small (2-8 FTEs) and they can barely keep up with day-to-day help desk tickets. This small group of staff often needs to support more than 200 different information systems,

hundreds of interfaces, servers, laptops, desktops, printers, mobile devices, phone systems, internet connections, access control, biomedical devices, imaging devices, and all the other technical components that keep hospitals running. It becomes quickly apparent why cybersecurity initiatives take a back seat to the day-to-day business of keeping the facilities running. A basic security measure like 24/7 monitoring of systems is “pie-in-the-sky” for these organizations. Despite all the guidance, recommendations and services provided over the past few years by HSCC, 405(d), H-ISAC, CISA and other organizations, I have found that the vast majority of small and rural hospitals are unaware of these resources, and too overwhelmed to take advantage of these valuable tools. They are treading water, only addressing issues that are necessary to keep the clinical operations functioning or are mandatory.

Small hospitals especially struggle to recruit and retain security staff, with current salaries for these high-demand professionals beyond the already strained budgets. Many facilities attempt to train staff from within, but often these staff members quickly leave for other higher-paying jobs outside the organizations.

Technical Debt

Small and rural hospitals also typically have an abundance of technical debt, with many outdated systems that they cannot afford to keep updated, including hardware and software that is beyond end-of-life. While COVID greatly expanded the digital footprint of most hospitals, with new systems to meet the needs for telehealth and remote workforce implemented at warp speed, often very little consideration was

given to security. These factors contribute to the increased attack surface for small hospitals when compared with larger facilities.

Cyber Insurance Coverage

In recent years, it has become increasingly difficult for small rural hospitals to rely on cyber insurance coverage to assist them in recovering financially from an attack. Insurance companies have become much more selective in extending coverage, making it difficult for smaller organizations to meet their stringent requirements. If hospitals do qualify for coverage, often rates are 35-75% higher than larger entities, with lower limits, and more exclusions. Relying on cyber insurance to offset these risks is quickly evaporating as an option.

Summary

The topics listed above are not anywhere near exhaustive, but these items, in my opinion, combine to create a significant increased risk for cyberattacks for this segment of the healthcare sector, with the risk anticipated to continue to grow as the threats increase.

Dangers of Exposing Healthcare Sensitive Data to Adversaries

Protected Healthcare Information (PHI) is a concern well beyond HIPAA mandates. For a patient, their data is highly sensitive, and a leak can be extremely damaging. Healthcare data is extremely rich including Protected Health Information (PHI), Personally Identifiable Information (PII) and Payment Card Industry (PCI) data. When attackers can extort all three of these types of information, it is evident why healthcare data remains the information most targeted by cybercriminals across all critical infrastructure sectors. Healthcare records remain the most valuable information on the dark web (<https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>). But beyond the impact to healthcare organizations of reputational harm, loss of staff, difficulty in recruiting future staff, insurmountable recovery costs, legal penalties, and both civil and criminal lawsuits, the far-reaching ramification to patients of a security breach can be devastating. Exposure of health information can lead to individual reputational harm, identity theft, extortion, monetary loss, and patient safety risks.

Impact to Communities When Healthcare Organizations Experience Cyberattacks

Diversion of Patients

The impact on rural communities during a cyberattack is hard to overstate. While attacks in urban areas are also impactful, populated areas provide other healthcare options for patients close by, lessening the potential for patient safety issues. In most rural areas, the next closest healthcare facility may be 45 miles away or more. This can make the diversion of patients infeasible. With recent attacks causing outages measured in weeks, and sometimes months, the impact on patient safety is easy to comprehend when travel times can take up to an hour or more. This delay can directly influence negative outcomes for many healthcare issues such as stroke, heart attack, sepsis, or even the delivery of a child. When patients are diverted, nearby facilities can become overwhelmed beyond capacity, creating a cascading crisis throughout the community. This is supported by a University of Washington study showing the closure of urban hospitals had no impact on their surrounding communities, but the closure of rural hospitals had a mortality rate increase of 5.9%, primarily due to increased travel times for patients ([Rural hospital closings cause mortality rates to rise, study finds \(nbcnews.com\)](#)).

Hospital's Reliance on Electronic Health Records

Since the HITECH Act of 2009, more than 97% of hospitals in the US have adopted Electronic Health Records. They have integrated these systems and workflows into every aspect of safe, efficient, effective patient care and are highly dependent on

these systems to maintain the high-quality standards of care that patients deserve.

When these systems are not available, hospitals are significantly hindered, which can lead to a sharp increase in the likelihood of patient harm.

The effect on patient safety when systems are offline is very evident. A report from a recent cyber incident detailed a litany of issues that prevented staff from caring for patients. Some of the most sobering effects were that patient safety checks within the EHR (Electronic Health Record) were not available, paper documentation significantly slowed processes for workers, with no registration system, patients “slipped through the cracks,” ambulances quickly became backed up as crews waited to hand off patients, lab results were delayed for hours (routine lab tests taking up to 13 hours and STAT tests up to 5 hours), and medication delivery safeguards were not available. Additionally, communication between departments was slow and manual, clinical staff had no access to patient history (many patients do not know their medications or allergies), personnel could not access contact information for family members or advanced directives, leading to staff not knowing whether to resuscitate a patient. The manual paper charting workarounds were woefully insufficient, with illegible handwriting in paper charts and many staff that had never been trained in how to document care on paper. Ultimately, an ED nurse at this facility called 911 to ask if fire department support could be dispatched to support the Emergency Department because they were so overwhelmed.

All of these items contributed to the decreased level of patient care at this facility, and any one of them could lead to significant patient safety issues.

Community Health and Financial Impacts

While the patient safety concerns may be more easily understood, the closure of a hospital can place additional strain on other healthcare services within the community or in surrounding communities. Neighboring hospitals can be overwhelmed if diversion occurs, facilities that are connected via virtual private networks will need to be vigilant to avoid becoming a subsidiary victim, clinics or other health systems that typically receive results could see significant delays, and communication can become challenging, both between the hospital and their patients and between other healthcare providers.

In addition to the recovery costs for these organizations, it is common for hospitals to see lower reimbursement due to decreased volume and inability to capture costs. Reputational harm can also have significant impact on finances, with legal penalties, civil lawsuits, and other recovery costs potentially all contributing to a hospital's inability to recover from a cyber event given their already strained budgets.

Summary

Diversion of patients causing excessive delays in care, our national overall reliance on electronic health records to safely care for patients, and the overall community and financial impact are all very real, well-documented results of the growing cyberattacks on our nation's health sector. While the example above used may appear extreme, it can very easily be replicated in any of the 1796 rural hospitals across the country that are not prepared for these events.

Recommendations For Assistance to Improve Cybersecurity Postures for Small and Rural HospitalsRecommendation 1: Minimum Security Standards

In small and rural hospitals, there are always many competing priorities for time and money. Without minimum standards, these facilities will not prioritize cybersecurity over the seemingly more pressing needs in currently strained budgets. However, whichever cybersecurity minimum standards are imposed, they must be reasonable, achievable, and continually evolving as security needs develop. Consideration must be given to the limitations of small and rural hospitals, and the potential negative impact new requirements could have on these organizations.

My recommendation would be to start with the following requirements, based on the items outlined in the Health Industry Cybersecurity Practices (HICP) document. These could be grouped into five basic categories, as outlined below.

1. Email Security & Protection (This is the biggest risk)
 - a. Strong filtering / blocking systems with best practice controls implemented (like blocking macros, not allowing .exe files, geo-blocking, etc.)
 - b. Security awareness training (including phishing simulation, regular training, etc.)
 2. Access Management (Sites must know & manage who is on the network!)
 - a. Role-based security
 - b. Strong Password Management
 - c. Multifactor Authentication
-

-
- d. Provisioning/Deprovisioning best practices
 - 3. Asset Management – (Sites must know & manage what is on the network!)
 - a. Inventory management
 - b. Asset tracking
 - c. End Point Protection
 - 4. Network Management – (Sites must manage the gateway and keep things patched to prevent holes)
 - a. Firewall configuration best practices
 - b. Regular patch management
 - c. Change/Configuration Management best practices
 - d. Data protection and loss prevention
 - 5. Incident Response – (Must have a plan for when they get hit)
 - a. Documented IRP plan
 - b. Regular exercises
 - c. Disaster recovery plan

Recommendation 2: Funding/Incentives

The minimum standards outlined above can be reasonably expected of all facilities, but not without assistance from the federal government for small and rural facilities. Assistance should be made available in a variety of ways. The pros and cons of each option are outlined below:

Subsidies:

Subsidies are very effective for smaller hospitals. We have seen the positive effect of the USAC Health Connect Fund which allowed for small and rural healthcare organizations to reduce the costs of internet and telephony services by 65% since 2012. This is a very active fund, and most rural facilities (and clinics) are taking advantage of the cost reduction available for these services. Currently, this fund is restricted to items that affect the core and wide area network (WAN) only, but it does include some limited equipment and network management items. An effective way to quickly implement subsidies would be to increase the scope of the existing Health Connect Fund to include cybersecurity initiatives that are aligned with any minimum standards imposed. This could greatly reduce the cost of services of implementing cyber standards, and the funding would be repeatable year over year to continue to grow cyber programs as the needs change. Alternatively, if USAC cannot support this fund's expansion, implementing a similar subsidy fund through HHS or FEMA to address cybersecurity needs would have a positive impact, too.

Grants:

While grants can be very effective, it should be noted that most small organizations do not have grant writers on staff, and do not have the capacity to respond to complex grant applications or maintain the detailed tracking of information that many grants require. Existing grants under Homeland Security for cybersecurity are targeted at specific groups, such as state and local, tribal, law enforcement, or houses of worship. This makes it difficult for small and rural facilities to be competitive for these funds. If grants are an option under consideration, they need to be specific to

small and rural healthcare organizations (which is the biggest risk sector), be allowed over a period of three to five years to ensure adequate time for implementation of security given resource constraints, have a low application burden (similar to COVID funding where the funds were dispersed with proof of utilization coming later or the return of the funds), and have a reasonable threshold of ongoing administrative requirements.

Meaningful Security (Similar to Meaningful Use)

The Meaningful Use program was proven to be very effective in moving hospitals to electronic health records. However, the program was administratively burdensome for many small organizations. If a “Meaningful Security” program were used to incentivize hospitals to build their security programs, it would need to be specifically targeted to small and rural facilities, since this is the group that is most in need of assistance. Also, consideration would need to be given to how cybersecurity partners would become eligible under the program (similar to the CEHRT program for MU). One drawback to this type of incentive is the delay in getting this funding to facilities due to the administrative work it required to develop and implement the program. Many facilities could close before this becomes available.

Enhanced CMS Payments:

Another option to assist small and rural hospitals would be to enhance CMS payments to offset the costs of cyber programs, with a requirement for the submission of evidence to indicate that the excess funds were spent appropriately.

This may take additional time to design and implement, as there would need to be a clear definition eligible items, vetting (or certification) of software and services that qualify, a determination of how to qualify (ensuring that the neediest of our hospitals are able to take advantage of the funding), and other administrative decision points.

Recommendation 3: Coordination of Government Efforts

There are several agencies within the government trying to solve the cybersecurity challenges our nation is facing. While these efforts are greatly appreciated, the lack of clarity on who is ultimately leading healthcare cybersecurity can be unnecessarily confusing for small organizations. While the guidance and services available to date from a variety of organizations, such as HSCC, 405(d), ASPR, H-ISAC, CISA, and other organizations are a positive step, my interactions with smaller organizations have shown that the majority of small and rural hospitals are not aware of the recommendations, guidance, or service offerings. Additionally, even when these options are presented, small hospitals do not have time to consider engaging or implementing the resources as they do not have the staff or the knowledge to move forward. Without minimum requirements and incentives, these great tools could be overlooked by the organizations that need them most.

It should also be noted that many of the services currently available do not take into consideration the “healthcare-specific” nuances of cybersecurity. While CISA has many great services available, when engaged, it quickly becomes apparent that resources at CISA may not understand how healthcare systems operate, and how this

affects their ability to quickly implement security controls. For example, in many industries it is standard to apply system patches as soon as they become available. But in healthcare, due to the potential negative impact to patient care, patches are slow to become available and must be thoroughly tested prior to application, with a detailed change management plan. Many times, patching involves vendor associated costs that must be budgeted due to ensure the correct level of expertise required for the complex interfaces and equipment involved.

The recommendation here is to have one agency (preferably HHS) take the clear lead on all healthcare-specific cybersecurity needs and engage other agencies to ensure they are well versed on healthcare cybersecurity nuances. Alternatively, if CISA, Homeland Security, USAC, FCC and other areas are engaged in healthcare cybersecurity, they need to collaborate with HHS to ensure there is a comprehensive understanding of healthcare-specific cybersecurity management.

Recommendation 4: Allow Declaration of Emergency for Cyber Attacks on Healthcare

Cyber-attacks are a leading cause of hospitals not being able to effectively provide care to patients. The challenges that current exist with cyber insurance leave many organizations at risk of not being able to recover from a cyber event. Cyber-attacks should be handled like other hazards, allowing facilities to take advantage of resources available under a declaration of emergency. Establishing a FEMA cyber disaster relief program would provide victims of these attacks access to emergency-related assistance. This would not conflict with current cyber insurance coverage,

rather enhance the coverage and would allow for faster recovery and increased financial stability for health systems.

Conclusion

Currently, the cyber attackers are winning the battle. The Cybersecurity Act of 2015 is now approaching eight years old. While there have been many advancements made with respect to published documents, services, and guidance, we have continued to lose ground to these cyber criminals. There must be a bipartisan plan to address this cybersecurity crisis immediately. We can no longer delay without further jeopardizing our healthcare system, especially the small and rural hospitals that are already in crisis.



Testimony of

Greg Garcia
Executive Director

of the

Healthcare and Public Health Sector Coordinating Council

Cybersecurity Working Group

Before the

United States Senate

Committee on Homeland Security and Government Affairs

March 16, 2023



Introduction

Chairman Peters, Ranking Member Paul, and members of the Committee, my name is Greg Garcia. I am the Executive Director of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG), an industry-led advisory council of more than 350 healthcare organizations and government agencies working in partnership under the auspices of the DHS Critical Infrastructure Partnership Advisory Council (CIPAC) framework and Presidential Policy Directive 21. Our mission is to identify and mitigate cybersecurity threats and vulnerabilities to the delivery and support of healthcare. At the heart of this work is a recognition that patient safety must be a guiding principle of healthcare cybersecurity.

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

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector

March 16, 2023

2



We appreciate the Committee’s holding this timely hearing, as the HSCC is indeed conducting a “checkup on the cybersecurity risks to the healthcare sector.” Today, I will cover four areas that will help inform both the diagnosis and prescription for healthcare cybersecurity:

First, I will provide a brief overview of recent trends in cyber threats, vulnerabilities and incidents facing the healthcare sector;

Second, I will offer some observations about how the healthcare industry is changing in ways that could aggravate those threats and related incidents;

Third, I will review how the industry has organized and partnered with the government over the past five years to address these concerns and how we are mobilizing to get ahead of them over the next five years; and

Fourth, I will offer examples of how our government agencies and Congress may support the health industry’s efforts to augment our security and resilience against ongoing cyber threats.

Cyber Threats, Vulnerabilities and Incidents

The “healthcare cybersecurity” reference was generally not heard ten years ago. But since 2017, when ransomware and other forms of cyberattack disabled the health system in the UK and many other U.S. providers and multinational companies, the epidemic of cyber threats against the health sector has only proliferated.

Today, because of the rise in digital healthcare, technological advances, and the efficiencies of connecting devices and data, the cyber “attack surface” in healthcare – and the adversaries intent on exploiting them – have expanded.

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



Threat actors are motivated to attack, including monetizing ransomware and stolen health data; operational disruption; intellectual property theft; revenge; or geopolitical leverage. The focus has traditionally been on data and privacy, but if healthcare delivery organizations (HDOs) or their suppliers cannot deliver services, as has been seen in numerous ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

Incidents and Impacts

Data Breaches

The Office for Civil Rights in the Department of Health and Human Services, which enforces Health Insurance Portability and Accountability Act (HIPAA) data breach reporting, reported:

- Healthcare data breaches of 500 or more records (name, address, medical and financial records) increased from 329 to 715 between 2017 and 2021, with the number of individuals affected ranging between 20 million and 50 million;
- In 2022, there were 707 data breaches, more than half of which occurred against third party service providers that handle protected health information; and
- Of the 52 million data records exposed in 2022, 43.9 or 84% were caused by hacking.

And according to an IBM Cost of a Data Breach 2022 report:

- For the 12th consecutive year, the Health Provider and Pharmaceutical subsectors recorded the first and third highest costs for data breaches, followed by Financial Services, Technology and Energy;

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



- The average breach cost in healthcare increased by nearly \$1M and is now \$10.1M; and
- Costs overall have increased by over 40% in the last two years.

Ransomware and other disruptive cyberattacks

Widely reported incidents experienced over the past few years by health systems such as Scripps Health, University of Vermont Health Network, and CommonSpirit involved some combination of disruptions affecting patient safety, business operations and clinical workflow, such as:

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

**Business Risks**

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

- Damaged reputation
- Lost patient trust
- Lawsuits
- Regulatory penalties
- Strained employee morale and burnout, and
- Reduced stock value.

Common Methods of Attack

The Health Information Sharing and Analysis Center (Health-ISAC) – the operational defense collective of the health sector - surveyed its members asking them to rank order the Top 5 “greatest cybersecurity concerns” facing their organizations for both 2021 and 2022. The survey included cyber and non-cyber executives, multiple healthcare subsectors (e.g., Providers, Pharmaceutical Manufacturers, Payers, Medical Device Manufacturers, and Health Information Technology), and healthcare organizations of varying sizes and budgets. The Top 5 threats, which were the same for both 2021 and 2022 were:

1. Ransomware Deployment, by which the adversary can inject networks with malware that encrypts - or renders inoperable - networked devices and software applications



and data and demands a ransom in exchange for returning the data and operations to the health provider;

2. Phishing/Spear-Phishing Attacks, by which the adversary sends bogus emails that trick employees, clinicians, or influential senior executives into divulging information, clicking on malicious links, or opening corrupted attachments that release malware into the network;
3. Third-Party/Partner Breach, by which business partners or third party software that support clinical or business operations become infected, in turn infecting networked clinical and business operations of the healthcare entity;
4. Data Breach, which involves the theft and exposure of protected health information that can include name, address, social security number, insurance and financial information, and patient data; and
5. Insider Threat, by which employees inadvertently, carelessly, or maliciously allow malware or other adversarial actions into the health system network.

The Related Scourge of Misinformation and Disinformation

Pandemic-themed disinformation and misinformation tactics in phishing and other social engineering subterfuge often resulted over the past three years of the pandemic in compromised systems, stolen data and identity theft, resulting in degradation of trust in the industry. Many of the peddlers of spam and malware have engaged in or allowed their tools to be used to disseminate deliberately false information. While misinformation might cause

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



discomfort and arguments in other areas, disinformation in the healthcare area could lead to the loss of lives. COVID was a sad example in which even the most vulnerable citizens succumbed to misinformation and paid a tragic price.

Current and Future Dynamics in the Healthcare System

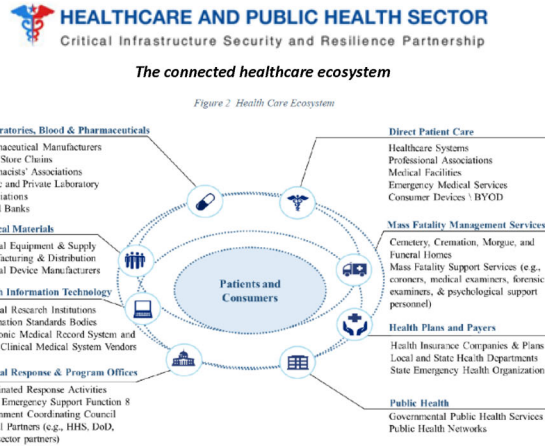
The health sector is highly interconnected:

- Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and payment for those services;
- Many healthcare facilities, such as hospitals, operate in environments that are accessible to the public, which adds to the vulnerability;
- The average patient bed has 15 supporting medical devices, and a 500-bed hospital could have 7,500 devices, many of which are over 8-10 years old and connect to a network that may not be protected or segmented from other systems or databases;
- Thousands of hospital-deployed medical devices are supplied by many different manufacturers with various levels of security and patching protocols. Devices often have unencrypted hard drives or common passwords set by the manufacturer that cannot be changed;
- Accompanying this range of manufacturers are many differing support models, timing for developing patches and methods for their deployment. This adds time, cost and complexity to hospitals' ability to manage effectively;

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



- Hospitals utilize many devices with outdated operating systems that are not supported by the manufacturers. Expensive equipment such as Magnetic Resonance Imaging (MRI) machines are not easily replaced as they run 24 hours a day, seven days a week, 365 days a year. Implementing compensating controls, or taking them offline for patches, updates or replacements is complicated. Further complicating HDO replacement programs are budget constraints and small operating margins;
- When supply chains are tightened or non-existent for various reasons, or pandemics or natural or man-made regional disasters occur, stretched supplies and staff become additional factors; and
- Coupled with a diverse base within the sector, complex siloed departments, a lack of skilled cyber staff, cyber security situational awareness, knowledge and training for the medical staff and CEO and Board levels, and lack of cyber security strategy including a risk management approach, the health, and public health sector face an enormous challenge.



An Organized Partnered Response

Policy Foundation. U.S. national policy (Presidential Decision Directive 63, Homeland Security Presidential Directive 7, Presidential Policy Directive 21) designates 16 essential industries as “critical infrastructure,” including healthcare, financial services, energy, telecommunications, water, transportation, and more. These critical sectors are represented by industry-organized “sector coordinating councils (SCCs).” These SCCs and their government counterparts form a national public-private partnership coordinated overall by the U.S. Department of Homeland Security through the National Infrastructure Protection Plan (NIPP).

The Sector Coordinating Councils (SCCs) are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities.

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



The SCCs coordinate and collaborate with sector risk management agencies (SRMAs) and related Government Coordinating Councils (GCCs) to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.

SCCs serve as the sector's voice and facilitate the government's collaboration with the sector for critical infrastructure security and resilience activities. In addition, the SCCs are encouraged to establish voluntary practices to ensure that sector perspectives are included. Other primary functions of an SCC may include the following:

- Serve as a strategic communications and coordination mechanism between owners, operators, trade associations, suppliers, and the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support appropriate information-sharing capabilities and mechanisms in sectors where no information-sharing structure exists;
- Encourage representative sector membership;
- Participate in planning efforts with designated SRMAs (the designated SRMA for healthcare is the U.S. Department of Health and Human Services) related to longer term strategic plans;
- Facilitate inclusive organization and coordination of the sector's policy development regarding critical infrastructure security and resilience planning and preparedness,



exercises and training, public awareness, and associated implementation activities and requirements;

- Identify, develop, and share information with the sector (both public and private sector members) concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans; and
- Provide input to the government on sector research and development efforts and requirements.

For the government's part, SRMAs have enumerated partnership responsibilities promulgated under §9002 of the FY 2021 National Defense Authorization Act, to include:

1. Provide specialized sector-specific expertise to Critical Infrastructure (CI) owners and operators in the sector or subsector;
2. Support the sector or subsector's programs and associated activities;
3. Carry out responsibilities in coordination with DHS, other relevant departments and agencies, independent regulatory agencies, and state local tribal and territorial entities as appropriate, and in collaboration with the sector's CI owners and operators; and
4. Utilize specialized expertise in the sector to support sector risk management in coordination with the CISA Director, including establishing and carrying out programs to help owners and operators identify, understand, and mitigate threats, vulnerabilities, and risks to their systems and assets, recommending security measures to mitigate risks,



assessing sector risk, coordinating with the sector, facilitating information sharing, and supporting incident management.

Critical Infrastructure Partnership Advisory Council Framework. Critical infrastructure SCC-GCC partnerships operate under a CISA-coordinated framework called “*Critical Infrastructure Partnership Advisory Council (CIPAC)*” which exempts ongoing SCC-GCC engagements involving planning and decision making from standard public disclosure rules associated with federal advisory committees under the Federal Advisory Committee Act. This is due to the imperative of protecting sensitive critical infrastructure threat, vulnerability, and mitigation information from public disclosure that could encourage the malicious targeting of data and operations and jeopardize public safety and economic and national security.

Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group. The HSCC serves as an advisory council to the sector, HHS, CISA, and other government agencies, with a formally-designated critical infrastructure protection function distinct from the advocacy and member services roles of traditional industry associations. The HSCC, Health-ISAC, HHS, FDA, and CISA work jointly to identify and mitigate systemic threats to critical healthcare infrastructure, such as pandemics, major weather events, terrorism, active shooters, and cyber-attacks. The mission is to identify cyber and physical risks to the security and resiliency of the sector, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response.

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



The HSCC Cybersecurity Working Group is a volunteer council of ~380-organizations that operate under a charter-based governance structure with an elected Chair, Vice Chair and Executive Committee. Membership is open to any organization that is a) a covered entity or business associate under HIPAA; b) a health plan or payer; c) regulated by FDA as a medical device or pharmaceutical company; d) a health IT company subject to health data interoperability rules HHS Office of the National Coordinator; e) a public health organization and f) any healthcare industry association or professional society. A small allotment of an “Advisor” members – consulting, law, and security companies - is permitted to participate and support CWG initiatives pro bono.

When working with our government partners, the industry-led Cybersecurity Working Group becomes the *Joint* Cybersecurity Working Group, which identifies and develops preparedness measures against cybersecurity threats to the security and resiliency of the healthcare sector.

The HSCC Cybersecurity Working Group is currently organized into 15 function-specific, outcome-oriented task groups composed of 30 to 130 organizations across the health industry spectrum that meet regularly to develop best-practices for various healthcare cybersecurity disciplines. These disciplines include health provider cybersecurity hygiene; supply chain cyber risk management; workforce development; incident response; and medical technology security, among many others.



Last week the Cybersecurity Working Group published its 17th [best-practice guidance](#) since 2019, this one guiding healthcare organizations on how best to implement the widely recognized NIST Cybersecurity Framework. This was our second “Joint Seal” publication in partnership with HHS – a compelling indication of the importance of collaboration between industry and government, on the principle that market forces alone cannot solve our cybersecurity challenges, and regulation cannot solve those challenges. This publication also acknowledges the imperative of critical infrastructure protection articulated in the recent publication of the President’s National Cybersecurity Strategy. The NIST Cybersecurity Framework was developed principally as a cybersecurity management tool for critical infrastructure industries, so our Healthcare Implementation Guide for the NIST CSF specifically addresses that imperative.

Our first joint seal publication in 2019 was the [Health Industry Cybersecurity Practices \(HICP\): Managing Threats and Protecting Patients](#), which was the result of an HHS-industry partnership created by Congress in Section 405(d) of the 2015 Cybersecurity Information Sharing Act. Now four years after its publication, we have updated the HICP resource to reflect evolving threats and deterrent capabilities, which will be published jointly in the coming weeks as “HICP 2023.”

And on March 1, the HSCC published a long-awaited resource laying out how medical device manufacturers and health delivery organizations can share the responsibility for [managing the](#)

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector

March 16, 2023

15



[cybersecurity of medical devices](#) as they age in the clinical environment beyond manufacture or software support and patch ability. This document, more than two years in negotiation between major hospitals and medical technology manufacturers, with assistance and support from FDA, exemplified the spirit of shared cybersecurity responsibility for patient safety that is the cornerstone principle of member engagement in the HSCC Cybersecurity Working Group.

Finally, this week and over the next several weeks, we will roll out a dynamic resource to address the issue of the “insider threat” discussed earlier, with the release of an 8-part video training series – available now on YouTube called “[Cybersecurity for the Clinician](#)”. This short series totaling 50 minutes will help clinicians – doctors, nurses, medical students, support staff, and many others understand the importance of helping to secure their small part of cyberspace and that it is not just the job of IT security teams. Again, accessible to anyone and any institution, this educational tool will offer continuing education credit as an incentive to click the play button and improve cybersecurity awareness and protection.

The resources mentioned above and all others we produce – by the sector for the sector - are offered as a public service free to sector stakeholders and the public via our website <https://healthsectorcouncil.org/hscs-publications>. Some additional publications include:

Operational Continuity after Cyber Incident; Securing Telehealth and Telemedicine; Model Contract Language for Medtech Cybersecurity; Medtech Vulnerability Communications Toolkit; Supply Chain Cybersecurity Toolkit; and Information Sharing Best Practices. We encourage and

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



expect all healthcare entities among the subsectors to review these tools and implement any and all elements as appropriate into their enterprise cybersecurity programs so that collectively the sector will be prepared before, during, and after the inevitable cyber incident.

It is important to note that many of these HSCC CWG publications directly address the many important recommendations contained in the 2017 report of the Health Care Industry Cybersecurity (HCIC) Task Force, which was established by Congress in Section 405(c) of 2015 Cybersecurity Information Sharing Act and was composed of industry and government experts in healthcare and cybersecurity. The HCIC Task Force Report characterized the healthcare industry's cybersecurity preparedness as being in "critical condition." It recommended a total of 15 action items that the industry and government needed to address to raise the level of cybersecurity preparedness in the sector. Those many HCIC Task Force recommendations motivated the functional CWG task group structure, which served as the circulatory system of the council and produced our many publications. We believe and urge that broad sector-wide implementation of those scalable practices will eventually raise the sector's preparedness diagnosis to "stable."

But in the business of cybersecurity, we are never done, only better. That is why the HSCC and HHS are embarking this year on a review of how we have addressed those recommendations over the past five years, how the healthcare industry will evolve over the next five years, what associated cybersecurity challenges will be presented to us by those trends, and how we should

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



collectively prepare, in industry and government. Around this time next year, we expect to have a strategy to share that follows up on the HCIC Task Force report and builds on it with forward-looking assessments and measures of improvement among sector objectives.

Finally, it is important to recognize that the engagement of health sector entities to join forces against evolving cyber threats has broadened and deepened through a membership increase in the Cybersecurity Working Group from 50 organizations in 2017 to 380 today, or a 660% increase. Likewise, the Health-ISAC membership has increased by 85% since 2015, now representing more than 70% of healthcare's GDP, with 8500 member personnel sharing information around the world. Collectively, we are motivated by the existential principles that a) Cyber safety is patient safety and b) as former National Cyber Director Chris Inglis aptly articulated, "They have to beat all of us to beat one of us."

Government Action on Healthcare Cybersecurity

The following section provides: 1) a brief overview of policy actions over recent years aimed specifically at healthcare cybersecurity and 2) an overview of options for government programs, incentives, and direct support for healthcare cybersecurity that industry stakeholders have been to discuss as possible recommendations beyond simply mandating technical controls.

Policy Developments

The following partial list of legislative, regulatory or executive actions taken over the past 2-3 years illustrates the range of potential policy shifts that healthcare organizations may consider

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



as part of their cyber and enterprise risk management strategies. Likewise, this overview may stimulate discussion between industry and government partners about how to synthesize disparate initiatives into a coherent national critical infrastructure protection strategy.

- [Omnibus Appropriations Act Section 3305](#), p. 1374 (December 2022): requires medical device manufacturers to ensure that their devices meet select minimum cybersecurity requirements, supported by device manufacturers and health delivery organizations;
- [National Cybersecurity Strategy, The White House](#) (March 2023): with an emphasis on protection of and minimum controls for critical infrastructure industries
- Policy options paper "[Cybersecurity is Patient Safety](#)" released by Senator Mark Warner (D-VA) (November 2022)
- Deputy National Security Advisor [public comments](#) (October 2022) that HHS "is beginning to work with partners at hospitals to put in place minimum cybersecurity guidelines, and then further work upcoming thereafter on devices and broader health care as well."
- [Cyber Incident Reporting for Critical Infrastructure Act of 2022 \(CIRCA\)](#) (March 2022): Require (p. 127) critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency within 72 hours of a substantial cyberattack or within 24 hours of a ransomware payment. Rulemaking process will take up to 3.5 years.
- [S. 3904 Healthcare Cybersecurity Act of 2022](#) (March 2022): - proposes closer collaboration between the Department of Health and Human Services and the

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



Cybersecurity and Infrastructure Security Agency, with the goal of strengthening cybersecurity in the health and public health sectors.

- **Securities and Exchange Commission [proposed rules](#)** (March 2022) aimed at bolstering the cybersecurity-related disclosures of regulated public companies that would require covered public companies to, among other things:
 - Report material cybersecurity incidents on Form 8-K within four business days of a materiality determination.
 - Routinely update investors on such incidents in quarterly and annual reports.
 - Analyze whether individually immaterial cybersecurity incidents are material in the aggregate and report those in quarterly and annual reports.
 - Make periodic disclosures regarding the company's cyber-related risk management policies and procedures.
 - Periodically disclose cyber-related governance information, including the board's oversight and management's implementation of cyber-related risk management policies and procedures.
 - Make periodic disclosures regarding board-level expertise in cybersecurity.
- **Federal Trade Commission [policy statement](#)** (September 2021) directing health apps and connected device companies to comply with the Health Breach Notification Rule. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media,



if there has been a breach of unsecured identifiable health information or face civil penalties for violations. The Rule also covers service providers to these entities.

- [Class action lawsuits](#) (June 2021) against Scripps Health in State and Fed Courts re ransomware effect on violation of California Confidentiality of Medical Information Act, Federal Trade Commission unfair trade practice regulations and the HIPAA privacy and security rules.
- [Government Accountability Office report](#) (June 2021) on the need for enhanced HHS Industry Partnership responsibilities.
- [HHS OIG Report](#) on Lack of CMS Cybersecurity Oversight of Networked Medical Devices in Hospitals (June 2021).
- [Executive 14028 Order on Improving the Nation's Cybersecurity](#) (May 2021): Section 4 encompasses medical technology security by specifying procurement requirements for Software Bills of Materials and agency guidance on purchasing systems with software defined as "critical software" for purposes of ensuring appropriate security before purchasing or deploying.
- [P.L. 116-321 \(HR 7898\) HITECH Act Amendment](#) (January 2021) requires OCR to consider mitigating fines and audit during a data breach enforcement if it determines that a breached entity has implemented recognized cybersecurity practices, such as NIST CSF and 405(d) Health Industry Cybersecurity Practices over the previous year.
- January 1, 2021: [FY '21 NDAA Section 9002](#) (p. 3383) – which codified Sector-Specific Agencies (SSAs), previously defined in Presidential Policy Directive 21 (PPD-21), as Sector

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



Risk Management Agencies (SRMAs), and defined how DHS and SRMAs should work with each other to protect critical infrastructure.

- [Cybersecurity Act of 2015](#) (pp. 104-108): §405c directed HHS to establish the Health Care Industry Cybersecurity Task Force and §405d directed HHS to convene an industry partnership program that eventually joined the HSCC Cybersecurity Working Group and produced the Health Industry Cybersecurity Practices.

Potential Government Support Programs

The following compilation of programmatic options have been or may be considered as potential recommendations for HHS, CISA, Congress or other Federal agencies to support healthcare cybersecurity. If designed, structured and implemented according to appropriate rulemaking or statutory authorities, these concepts could help reduce risk across the sector through incentive- or grant-based financial assistance and operational support to under-resourced health systems, particularly critical access and rural health providers.

Joint Preparedness Collaboration

- Augment the HHS 405(d) program. Resourced by HHS as a public-private partnership initiative codified by CISA 2015, 405(d) has a successful track record of partnership with industry. This model should continue with consideration for how it may be enhanced with continued industry-driven leadership;
- Healthcare Cybersecurity Workforce Development Program - HHS can administer a workforce development and cyber training program with assistance from NIST's *In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector*



National Initiative for Cybersecurity Education (NICE). Elements of this program could include access to free cyber training, assistance to providers under a Regional Extension Centers model, 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.

Financial Support and Incentives

- CMS reimbursement incentives: Similar to the cybersecurity investment incentive created in the HITECH Act amendment in PL 116-321, health systems may indicate implementation NIST CSF, HICP or other consensus-based, voluntary cybersecurity frameworks for a higher reimbursement;
- HHS grant programs to help under resourced health systems improve situational awareness by joining the Health-ISAC or other information and sharing and analysis organizations;
- Expand FCC Health Connect Fund of the Universal Service Administrative Company (USAC) from WAN/Core Network investment to network and application cybersecurity;
- Immediate One-Time Funding for Baseline Security Implementation for health systems under a certain threshold of current cybersecurity investment, tied to implementation of specific cybersecurity control frameworks such as NIST CSF and HICP;

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



- “Cash for Clunkers” for legacy hardware replacement, modeled after the program for consumers to replace used automobiles that do not meet current emissions standards. When coupled with FDA authorities to ensure medical devices have met pre-market security requirements this program would provide a mechanism for HDOs to replace legacy and insecure technology.

Threat and Vulnerability Sharing

- Boost funding for HHS Health Sector Cyber Coordination Center (HC3) to be a primary knowledge sharing and analysis resource within HHS to support healthcare cybersecurity in coordination with CISA;
- Continue development of innovative CISA support programs, such as the Automated Indicator Sharing (AIS) program or Cybersecurity Information Sharing and Collaboration Program (CISCP), that can be tailored, in close consultation with HHS, to healthcare entities;
- Timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should as a matter of protocol consult ahead of publication with designated industry sector leaders with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence. This would ensure that both industry and government leaders are generally aligned before publication to the

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures;

- Tailor a healthcare liaison classified information sharing program with industry-designated representatives of the HPH Sector, CISA, HC3, and other law enforcement agencies, so that the HPH representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the Sector;
- CISA should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities under CIRCIA 2022, as summarized in the previous section. Implementation should include consideration of waivers from victim reporting requirements while the incident response is underway in the early stages of discovery and operational triage;
- Protect health delivery organizations from class action lawsuits if they can demonstrate they implement NIST CSF, HICP, or other recognized cybersecurity practices and voluntarily share information about a critical cybersecurity incident with Health-ISAC, CISA, HHS/HC3, FBI, and/or state regulators. This could incentivize more robust adoption and implementation of security controls, promote voluntary information sharing, and protect against disclosure of sensitive incident information being used against the hospital in a class-action lawsuit.



Incident Response Support

- Federal-sponsored incident response support for organizations that are experiencing security incidents and need assistance getting through and recovering from the breach;
- Federal-sponsored cyber incident insurance modeled after FEMA to compensate for the retraction of private insurance carriers from the cyber insurance market;
- Expanded innovative law enforcement disruption of threat groups to reduce ecosystem risk creating the most harm to hospitals.

Regulatory Reform

- Revise HIPAA to reference the use of minimum standards in NIST CSF, HICP, or other recognized security practices, rather than prescribing cybersecurity requirements in statute. These standards should be built in partnership with the HSCC and regulators such as (OCR, ONC, CMS, and FDA) and cross-mapped for overlap or conflict across the various regulatory regimes intersect. A holistic, coherent cyber policy strategy is essential for a healthcare environment where clinical operations, medical devices, electronic health record technology, patient data, and IT systems are all interconnected but subject to different regulatory structures and authorities.

Conclusion

Mr. Chairman, as a critical infrastructure industry, the health sector and its dedicated workforce are mobilizing against the ongoing and existential threat of cyber disruption. We also recognize we need to move faster to keep up with the evolving threats. But through continued and

In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector



expanded engagement in our collective purpose, broader awareness promotion, and forward-leaning government programs and support, we can move the needle and five years from now diagnose healthcare cybersecurity to be in a “stable condition.”

Thank you.



March 14, 2023

**Testimony of Stirling Martin
Before the United States Senate
Committee on Homeland Security and Governmental Affairs**

Distinguished members of the committee, thank you for the opportunity to provide my testimony today. My name is Stirling Martin, my formal training is as a computer scientist, and I am the Chief Security and Privacy Officer and Senior Vice President at Epic. Since 1979, we've created clinical, financial, and administrative software, including the patient portal, MyChart, for healthcare organizations in the U.S. and around the world. Our customers include academic medical centers, integrated health systems, critical access hospitals, and federally qualified health centers.

Our focus first and foremost is on helping patients. Personal health data is uniquely sensitive if compromised because it cannot be reset like passwords or changed like credit card information. A patient's health information can also be immensely personal, and even just the threat of exposure can create angst for an individual. If exposed, private healthcare data can be leveraged by malicious actors through identity theft and the potential for blackmail. In an extreme case, patient safety could be directly impacted if a bad actor were to manipulate healthcare data.

Within a community, cyberattacks can reduce access to care. In a rural community with only one healthcare facility, patients may need to delay preventative care or elective treatments until an incident is resolved. In a larger community, a cyberattack can have a cascading effect as patients may be diverted to an unfamiliar care team at another facility, and those facilities need to deal with an influx of additional patients.

We've been shoulder to shoulder with our customers as healthcare has become increasingly targeted by cyberattacks. For a health system, a cyberattack disrupts their patient care mission, and causes both reputational harm and financial burden. Organizations often take their systems offline as they mitigate the impact of a security incident. Doing so places stress on staff to provide high quality care without the IT systems that drive their workflows. As organizations may see fewer patients, the financial impact extends beyond the cost of incident response to lost revenue as well.



Organizations face several challenges in improving their security posture. First is staffing, and their ability to hire and retain high-demand security talent.

Second, security is a constant effort, and there are always more steps that can be taken to make systems more secure. In working with healthcare organizations across the country, we see both basic and highly sophisticated security programs in use, and yet there is no defined benchmark of what security practices are considered sufficient.

An additional challenge is the lack of cybersecurity information sharing among healthcare organizations, as well as the limited threat intelligence from government agencies and private industry.

These challenges are exacerbated as many healthcare organizations currently face unprecedented financial and staffing pressures. The costs to improve one's security posture through new technology or staff must be weighed against other needs such as recruiting and retaining nurses at the bedside.

There are a variety of ways the federal government could help healthcare organizations prevent and respond to cyberattacks.

Starting first with prevention, there is a dire shortage of security talent in the United States. To build a deeper bench of skilled IT security professionals, the federal government could develop security training programs and incentivize newly trained professionals working in healthcare. This could be similar to the Rural Community Loan Repayment program for physicians who agree to provide care to rural communities after medical school and residency.

Secondly, the industry needs a single set of prescriptive security practices, whether defined by federal agencies such as NIST or CISA, industry efforts such as HITRUST, or a collaboration such as the Healthcare Sector Coordinating Council. This will raise the overall security posture of healthcare organizations by encouraging them to meet those acceptable security practices. The government should take the further step of establishing a legal safe harbor for organizations that meet the defined benchmark if they fall victim to an incident. This would also encourage information sharing to remediate active issues more quickly and prevent similar issues in the future, and could be bolstered by government agencies sharing deeper threat intelligence.



Lastly, on incident response, similar to how FEMA responds to a natural disaster, at-the-elbow support from the government could help healthcare organizations remediate an attack. For example, an organization recovering from a ransomware attack may need assistance cleaning and redeploying the computers used by their staff. On-the-ground support could help reduce the time it takes to bring systems back online by patching devices or by delivering a strategic reserve of computers and network equipment that can be used immediately. This could reduce recovery time by hours or days, providing tremendous value to healthcare organizations and the patients they serve.

In closing, people often ask me what keeps me up at night. It's the reality that we have to be perfect 100% of the time, and the bad guys only need to be lucky once.

Thank you for the opportunity to share Epic's perspective on this important topic.

Testimony Clarification: HSGAC – “In Need of a Check Up: Examining the Cybersecurity Risks to the Healthcare Sector”

From Kate Pierce, 3/17/2023

Senator Peters Question:

Rural hospitals, which continue to struggle due to the stressors of a worldwide pandemic, are bound to provide care to a high concentration of patients with limited financial resources. Often these hospitals are located many miles apart and far from larger urban centers.

- Ms. Pierce, how can the federal government help ensure that small and rural hospitals are able to invest in cybersecurity while balancing needed investments in other parts of patient care?

Senator Warner stated it well when he said that Cybersecurity IS patient safety. Cybersecurity initiatives can't be considered in isolation – they have a direct and immediate impact on patient care. Security minimum standards need to be embedded into the day-to-day cost of providing care, similar to the way the cost of electronic health records is now an engrained part of hospital budgets. Small and rural facilities typically serve a very high percentage Medicare and Medicaid patients (often 70% or more of their patients). For Critical Access Hospitals, the Medicare rate is reimbursed at cost, but this can take 2 to 3 years or more for cost reports to be reconciled. For Medicaid patients, in most states the reimbursement rates are well below the actual cost of services. Medicaid reimbursement must be at cost for these hospitals.

An incentive program that is similar to Meaningful Use with a 5 to 7-year timeline could allow small and rural hospitals the funding to implement best practices and the increase in CMS reimbursement that would catch up over time would make this a sustainable model. This allows cybersecurity costs to become part of hospital budgets without jeopardizing our small and rural hospitals.

Alternatively, funding assistance could be in the form of subsidies for small & rural hospitals, similar to the USAC Health Connect Fund with renewable reimbursement year-over-year directed at cybersecurity programs.

Testimony Clarification: HSGAC – “In Need of a Check Up: Examining the Cybersecurity Risks to the Healthcare Sector”

Whichever option you choose urge you, however, not to delay any longer. Many small hospitals are in crisis.

Senator Padilla’s Question:

Today there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide Both public and private sector companies face challenges in recruiting, hiring and retaining these professionals, which negatively affects our collective cybersecurity. Growing talents is a priority under the recently released White House Cybersecurity Strategy.

Can you speak to the specific and unique challenges in the healthcare sector as far as identifying, recruiting and retaining IT security professionals. Do you have any recommendations for us today.

Clarification:

The use of Managed Security Service Providers (MSSPs) for small and rural hospitals allows these facilities to share highly trained security staff among many facilities without having to bear the entire cost of these services. These services can be engaged on a fractional basis and within specific areas of cybersecurity according to each facilities needs and can be used to enhance IT staff knowledge, support specific cyber initiatives, and provide expert guidance on the best way for organizations to manage the risks within their environments. For example, a small facility will most likely not be able to afford to staff a 24/7 Security Operations Center to monitor their networks. This is crucial since the time lapse between an attack and intervention can mean the difference between no outages or outages of several weeks or months. But when many facilities can share an operations center, the cost becomes more affordable.

With the extreme complexity and vast number of areas of expertise within cyber, the reality is that small hospitals would find it even more difficult to find cyber personal well versed in all areas of cyber. And, if they would find it very difficult to retain them. My recommendation would be to fund small facilities to hire fractional cyber talent from dedicated healthcare cyber security service firms to gain economies of scale for the services and ensure that their program is not negatively by security staffing turnover.



March 16, 2023

The Honorable Gary Peters
Chairman
Committee on Homeland Security &
Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Rand Paul
Ranking Member
Committee on Homeland Security &
Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Peters and Ranking Member Rand Paul:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 129,600 family physicians and medical students across the country, I write to express our appreciation for the Committee's attention on health care cybersecurity, including today's hearing titled, "In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector." The AAFP shares your concerns about the need to address growing cybersecurity threats impacting the sector, including primary care physicians, and we write to share our policy recommendations.

The migration to digital health and electronic storage of patient health data has improved the ability for patients to access their health information. The AAFP has long [supported](#) policies that guarantee the appropriate security of protected health information while working to improve patients' access to their data, as well as the ability to share patients' health information across the care team. We are strongly [supportive](#) of making data reliably interoperable while maintaining patient confidentiality and the fundamental right to privacy. A confidential relationship between physician and patient is essential for the free flow of information necessary for sound medical care, and confidentiality of patient health data should continue to be a priority outside of the physician-patient relationship.

However, the rapid move to this electronic era of health care has unavoidably introduced the risk of cyberattacks for all health care organizations. The health care sector experienced the highest number of third-party cybersecurity breaches in 2022, accounting for more than one-third of all incidentsⁱ, and more than 45 million people were affected by cybersecurity attacks on health care professionals in 2021.ⁱⁱ Personal health data is particularly attractive to cyber criminals because it often contains both personal and financial data. It is often widespread across a patient's care network, which can include multiple clinicians and facilities, making it more vulnerable. The health care industry has had the highest average cost of a breach for 12 consecutive years and at this time, the average breach in health care costs \$10.1 million.ⁱⁱⁱ

The AAFP educates and encourages our members to work with their electronic health record (EHR) vendors, medical device vendors, and other partners to adopt data privacy and security practices, including cybersecurity protections. While privacy and security of patient health data is a priority for physician practices, not all of them have the resources, financial capacity, or technical knowledge needed to properly establish and implement best practices in cybersecurity. Many hospitals struggle to maintain appropriate resources, let alone small health care organizations, despite hackers likely

STRONG MEDICINE FOR AMERICA

President Tochi Iroku-Malze, MD Islip, NY	President-elect Steven Furr, MD Jackson, AL	Board Chair Sterling Ransone, MD Deltaville, VA	Directors Jennifer Brull, MD, Plainville, KS Mary Campagnolo, MD, Bordentown, NJ Todd Shaffer, MD, Lee's Summit, MO Gail Guerrero-Tucker, MD, Thatcher, AZ Sarah Nosal, MD, New York, NY Karen Smith, MD, Raeford, NC	Teresa Lovins, MD, Columbus, IN Kisha Davis, MD, MPH, North Potomac, MD Jay Lee, MD, MPH, Costa Mesa, CA Rupal Bhingradia, MD (New Physician Member), Jersey City, NJ Chase Mussard, MD (Resident Member), Portland, OR Richard Easterling (Student Member), Madison, MS
Speaker Russell Kohl, MD Stillwell, KS	Vice Speaker Daron Gersch, MD Avon, MN	Executive Vice President R. Shawn Martin Leawood, KS		

March 16, 2023
Page 2 of 7

having the same access to both. In any health care setting, health information technology (IT) vendors must be held accountable both to ensure cybersecurity protections and manage the consequences from any data breach or cyberattack on patient health and practice operations.

We applaud Congress for examining this threatening and dangerous issue. In November, the Academy provided robust [feedback](#) in response to a report issued by Senate Warner on this exact issue. Building upon that letter, we offer the following policy recommendations from the family medicine perspective to help inform today's hearing.

Federal Agency Engagement and Collaboration

Congress should encourage the Office of the National Coordinator for Health IT (ONC) to consider including cybersecurity framework best practices in health IT certification as one strategy to arrive at industry-wide adoption of standard best practices. If all EHR vendors are required to incorporate these practices into their technology, this would enable smaller physician practices who purchase and utilize their software and systems but lack their own IT resources to benefit from basic cybersecurity protections. In the meantime, the AAFP recommends Congress consider ways to encourage all health entities to adopt voluntary guidance from the National Institute for Standards and Technology (NIST), with technical assistance and support for effective implementation in real-world settings.

Overall, we urge Congress and the Department of Health and Human Services (HHS) to consider the role of ONC in any future cybersecurity policies. ONC has authority over all health IT coordination within HHS and has certification responsibility over health IT and EHRs, which would be responsible for complying with many of the proposed policies.

The Academy also thanks the Administration for Strategic Preparedness and Response (ASPR), in collaboration with NIST and other federal agencies, for their recent release of a [cybersecurity implementation](#) guide to help the public and private health care sectors prevent cybersecurity incidents. We know that interagency and cross-governmental collaboration will be integral to successfully advancing federal health care cybersecurity solutions, so **we strongly encourage Congress to continue working with ASPR, NIST, ONC and other related federal agencies to build on these resources.**

Health Insurance Portability and Accountability Act (HIPAA)

While privacy is the concept of the patient's ability to control, access, and regulate their personal health information, and security refers to the protection of this information, they are undeniably intertwined and therefore must be considered together as Congress takes steps to meaningfully address health care cybersecurity. First, most health data is now electronic and therefore security will also most always be how privacy is protected. Second, for decades, the challenges of inconsistent policy across federal and state privacy rules have made compliance very difficult. The Health Insurance Portability and Accountability Act (HIPAA) only protects health care data that is maintained by a covered entity or their business associates. This means that covered entities must have business associate agreements (BAAs) to ensure data is protected (i.e., HIPAA protections are extended to travel with the data). Health data captured or used outside of covered entities do not have any HIPAA protections.

Therefore, **the AAFP is particularly concerned about the privacy, security, use, and transfer of patient and consumer health data in the ecosystem outside of HIPAA where it is largely unprotected by federal laws or regulations.** We [believe](#) federal legislation is necessary to achieve

March 16, 2023
Page 3 of 7

a greater degree of data standardization and adherence to agreed-upon principles related to the privacy of health data.

Maintaining an up-to-date and robust cybersecurity footing can be an overwhelming task for some covered entities, especially small and medium physician practices. Any national data privacy legislation with new requirements must avoid imposing excessive administrative burden, liability for data breaches of third-party apps and application programming interfaces (APIs), or additional expenses to implement safeguards or contract with EHRs on physicians.

Even though a physician may not be subject to costly HIPAA breach penalties as a result of breaches of medical records due to vulnerabilities in third-party APIs and apps, they would still incur significant damage to their reputation and patient-physician trust, from a perceived mishandling of patient data. Additionally, relying on a patient's clinician to determine whether an app that the patient wishes to use or the clinician wishes to recommend has appropriate security (and privacy) places a [significant burden](#) on individuals and physician practices, who are likely unequipped to make this determination or provide patient education on app security.

While clinicians and health care organizations must follow the HIPAA Privacy Rule, which protects against disclosures of protected health information (PHI), other entities and data that do not qualify as PHI are not bound by the same rules. Large technology companies and data brokers could obtain and inappropriately use extremely detailed information about individuals, including internet search histories, communications, finances, and location data. These companies may also require the surveillance of personal information as a condition of use for apps individuals use to access their health data or improve their health.

Last Congress, the AAFP has [endorsed](#) the Health and Location Data Protection Act (S. 4408), which prohibits data brokers from selling and transferring customers' health and location data and requires the Federal Trade Commission to promulgate rules to implement and enforce these protections. We believe such measures should be a part of any comprehensive legislation to address consumer data privacy.

However, despite the limitations of HIPAA in this instance, Congress should consider the fact that HIPAA may not be the best legal mechanism to regulate cybersecurity and cyber threats. Modifying HIPAA regulations to address cyber threats may create unnecessary confusion and may limit the scope of protections. While web applications that contain patients' personal and health data may be secure themselves, the broader issue is often who has access to the data in the apps and what they might do with it, which includes selling it to hackers that pose cyber threats. **Congress must take action to protect personal and health data outside of HIPAA and ensure cybersecurity and privacy rules extend beyond the HIPAA regulatory framework.**

HIPAA regulations should align with those of the Federal Trade Commission (FTC), such as the Health Breach Notification Rule, by implementing consistent reporting of notifications. Ensuring consistency across requirements to report notifications in the event of a data breach of unsecured personal health information would be helpful to reduce the administrative burden of such requirements on physicians while ensuring data breaches are quickly reported and addressed. Congress should require HHS to monitor and report on notification trends and develop and publish best practices to assist health care organizations experiencing a data breach with rebuilding security and preventing future attacks.

March 16, 2023
Page 4 of 7

Workforce Development

There currently [exists](#) a significant worker shortage in the health care cybersecurity industry despite the rise in cyberattacks on health care organizations.¹⁴ **The AAFP strongly supports implementation of a workforce development program to incentivize cybersecurity professionals to work in rural, independent, and small practices, underserved communities, and communities with health professional shortages.** Such a program would help alleviate the financial and administrative burden on small physician practices by allowing for more outsourcing of cybersecurity compliance and ensuring they are able to access these professionals, despite potentially not having the resources or financial capacity to employ them or attract them from urban areas. The AAFP urges Congress to consider the appropriate federal agency to administer this program based on established expertise, capacity, and experience partnering with relevant health care, IT, and education stakeholders and to ensure adequate and sustainable funding to sustain the program.

The [Regional Extension Center \(REC\) program](#), established by ONC, is a good model for developing similar programs focused on cybersecurity and bolstering the cybersecurity workforce for areas and practices most in need. RECs represent a range of organizations that serve local communities throughout the country, providing on-the-ground technical assistance for individual and small medical practices to implement and maintain EHRs. Leveraging local expertise, RECs tailor and customize their support to each individual practice's needs and stay involved with the practice to provide consistent, long-term support. Training cybersecurity professionals to work in the health care industry is important, but it is perhaps more critical that these professionals are continually available to small and under-resourced physician practices. A REC-like program for cybersecurity could ensure primary care practices have access to trained professionals, provide technical assistance for implementing their own security protocols, and facilitate shared learning and dissemination of best practices.

To further address workforce, **the Academy also supports student loan forgiveness or repayment programs to incentivize cybersecurity professionals to spend several years serving health care organizations in rural or underserved communities and smaller health care organizations, especially safety net providers.** Similarly, loan forgiveness and repayment programs are a commonly used strategy to increase the primary care workforce in health professional shortage areas, including the [National Health Service Corps](#). A model like the National Health Service Corps coupled with a REC-like program could increase the cybersecurity workforce in the health care industry in rural and underserved areas of the country, in which many physician practices don't have the resources to hire cybersecurity staff. We suggest that such programs focus both on the size of a physician practice as well as its geographic location and the patient population it serves. It is critical that small, independent practices in rural as well as urban and suburban underserved communities have the same opportunity to benefit. We recommend there be a particular focus on programs that serve clinicians and practices in health care shortage areas.

It is efficacious to both increase the cybersecurity staff present at health care organizations in rural areas as well as make it easier for those entities to contract with third-party service providers for their cybersecurity needs. There is a need for on premises staffing, which can help educate existing staff on basic cybersecurity practices and support day-to-day operations, but there is also a need for access to remote experts as rural areas would likely be unable to recruit all the experts needed for on premises staffing. Congress should work with individual physician practices to determine their cybersecurity needs and provide resources to secure the appropriate staffing. Small, independent physician practices will have unique needs compared to large hospital systems.

March 16, 2023
Page 5 of 7

Cybersecurity attacks and data breaches cause disruptions in workflow and interruptions in patient care, including delayed procedures and tests, which can lead to negative health consequences for patients.⁹ These incidents also have the potential to financially bankrupt physician practices from being forced to pay ransoms and investing in rebuilding security of their electronic networks. While technology-based security solutions like artificial intelligence and automation can help reduce the cost of data breaches, many organizations may not have the capacity or expertise to employ these strategies. **For these reasons, although cybersecurity talent is in high demand across all industries, Congress must prioritize increasing cybersecurity talent in the health care industry.**

Incentives and Requirements to Improve Cybersecurity Capabilities

The AAFP urges Congress to be very cautious in defining and requiring adoption of minimum cyber hygiene practices. We encourage the use of incentives for compliance rather than penalties for noncompliance because the ability to comply varies with the type, setting, and size of physician practices. What is considered a minimum cyber hygiene practice should be based on the risk it is mitigating but the minimum also must consider an organization's available resources. What is minimum for a hospital may not be the same as for a small, rural family medicine clinic. If establishing minimum cyber hygiene practices, Congress must prioritize the intent of quality improvement and assurance rather than a system to punish bad actors. Therefore, the program should support health care organizations to achieve and exceed the minimum hygiene practices and only for severe and repetitive breaches of hygiene should penalties be inflicted.

Insecure legacy systems, especially medical devices and imaging technology are a major cybersecurity risk. While there are no easy solutions, the Healthcare and Public Health Sector Coordinating Council's [Model Contract Language for Medtech Cybersecurity](#) (MC2) is a good start.

Many physician practices depend heavily on their EHR vendors and medical device vendors to support cybersecurity, and many do not have cybersecurity professionals in their practices due to cost and availability. Therefore, it is critical that certified EHR technology and the devices it supports are held to high cybersecurity standards and compliance with industry best practices. Vendors and owners of these legacy systems should hold the most responsibility. **To address the current issue of insecure legacy systems, Congress should consider ways to incentivize medical device companies to update their products without placing the burden of these updates on the physician practices.** These companies should be held liable for the risks posed by not addressing known insecure legacy systems of their devices and products.

The Academy was pleased to see provisions to help ensure cybersecurity of medical devices included in the Consolidated Appropriations Act of 2023. However, to further address this issue moving forward, we continue to urge Congress to pass the entire [Protecting and Transforming Cyber Health Care \(PATCH\) Act](#) (H.R. 7084 / S. 3983), which would require premarket applications for cyber devices (i.e., medical devices that include software or connect to the internet) to include information relating to cybersecurity, including plans to monitor for cybersecurity risks and address vulnerabilities through regular product updates. These plans should include ways to efficiently collaborate with physician practices throughout the product's lifecycle, including updates, without excessively disrupting the clinical workflow or patient care.

Cybersecurity-Associated Costs

The AAFP believes that cybersecurity expenses should be explicitly accounted for in payment, including Medicare, and incorporated into practice expense and other formulas the same way other basic expenses are. The Centers for Medicare and Medicaid Services (CMS) informed by the

March 16, 2023
Page 6 of 7

American Medical Association/Specialty Society RVS Update Committee (RUC) should propose Medicare payment changes to account for this and allow opportunity for stakeholder comment through the regular rulemaking process. Cybersecurity expenses involve investments in technology, as well as investments in staff, both of which specifically serve the purpose of protecting patient health data. Aside from investments in cybersecurity preparedness, remediation costs during and after data breaches can be crippling, especially for smaller physician practices.

The AAFP supports the concept of offering startup grants to help physician practices cover initial investments in and costs for cybersecurity technology and workforce talent. The AAFP supports the [Health Care Providers Safety Act](#) (H.R. 7814 / S. 4268), which would establish a grant program for health care organizations to enhance the physical and cyber security of their facilities, personnel, and patients.

It is critical for these startup grants to include sustainability plans to implement after the grant is applied, and these plans should consider the different capabilities and resources of differently sized physician practices. Additionally, technical assistance should be accounted for financially, both in the startup grants and in sustainability plans. The appropriate agency administering these grants should work with health care organizations to ensure that grants are appropriately sized, the allowable uses of funds are well-informed, and the grants are targeted to entities most in need.

Preparedness for and Recovery from Cyberattacks

Congress should not implement required training for all staff within a health care system or practice but should rather focus on providing organizations with educational resources on how and why to prepare for cyberattacks. Despite best efforts to implement training and awareness programs for their employees, many health care organizations report a lack of in-house expertise, staffing, and collaboration with other entities as barriers to having effective cybersecurity strategies. According to recent data, the most common cyberattacks on health care organizations include cloud compromise, ransomware, supply chain attacks, and business email compromise/phishing.¹¹ Congress should consider these factors when developing educational resources on training that include key cybersecurity practices and actionable steps.

Just like for medical care, having a stance focused on quality improvement and assurance rather than blame and penalties is critical to support the shared learning needed to secure our health IT infrastructure. For example, quality improvement measures for infection control procedures and precautions rather than penalties contribute to shared learning and improved patient safety. This model could be applied to information sharing and learning on cybersecurity vulnerabilities and responses to prevent threats and address them as they arise. The AAFP encourages Congress to work with the Agency for Healthcare Research and Quality on whether policies of [patient safety organizations](#) may serve as a good model for a similar effort in the health care cybersecurity industry. Congress should consider that entities willing to be vulnerable in disclosing their current practices are likely seeking assistance and resources to help address the flaws of their approaches, often due to a lack of resources. It is critical to understand the barriers small, lower resourced, and rural physician practices face, who may need considerable ramp up in expertise and resources to address any flaws. Therefore, it is critical to avoid penalties and instead tailor assistance to the practice and the practice setting.

Additionally, we often hear from our members that the cost of cyber insurance is out of reach for many and unattainable for many physician practices. A recent report found that cyber insurance premiums have jumped more than 10% since 2019, and many insurers have implemented stricter requirements for practices and health systems to meet to be coverage-eligible while also narrowing

March 16, 2023
Page 7 of 7

what their policies cover.^{vi} Therefore, **many physician practices do not have cyber insurance and could be bankrupt should they have a significant incident.** Congress should investigate ways to support and regulate cyber insurance to ensure smaller health care organizations can afford to be covered. Before moving forward with a reinsurance program, starting with regulation of cyber insurance is a good first step to understand what constitutes a quality cyber insurance plan. This may include minimum coverage provisions to be deemed adequate to protect against junk plans to ensure that coverage is meaningful and effective in situations where it would need to be used.

Thank you for the opportunity to offer policy recommendations on ways to address health care cybersecurity. The AAFP looks forward to working with the Committee to strengthen cybersecurity in the health care sector in an attainable and sustainable way for primary care physician practices to protect patient health data. Should you have any questions, please contact Natalie Williams, Manager of Legislative Affairs at nwilliams2@aafp.org.

Sincerely,



Sterling N. Ransone, Jr., MD, FAFAP
Board Chair, American Academy of Family Physicians

ⁱ Third Party Breach Report: Trends, Shifts, and Lessons Learned from 2022. Black Kite.

<https://blackkite.com/wp-content/uploads/2023/01/third-party-breach-report-2023.pdf>

ⁱⁱ Milstein J. 2022. Critical Insight Finds 35 Percent Increase in Attacks on Health Plans in 2021 End of Year Healthcare Data Breach Report. Critical Insight. <https://www.criticalinsight.com/resources/news/article/critical-insight-finds-35-percent-increase-in-attacks-on-health-plans-in-2021-end-of-year-healthcare-data-breach-report>

ⁱⁱⁱ Cost of a Data Breach Report 2022. IBM Security. <https://www.ibm.com/downloads/cas/3R8N1DZJ>

^{iv} Rodríguez S. 2022. Talent Remains in High Demand Amid Cybersecurity Workforce Shortage. Health IT Security. <https://healthitsecurity.com/news/talent-remains-in-high-demand-amid-cybersecurity-workforce-shortage>

^v Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.

^{vi} Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care.

2022. Ponemon Institute. <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>

^{vii} Reed T, "As cyber attacks on health care soar, so does the cost of cyber insurance," *Axios*. Mar 6, 2023.

**Post-Hearing Questions for the Record
Submitted to Scott Dresen
From Senator Thomas R. Carper**

**“In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector”
March 16, 2023**

Intelligence Sharing Between Federal Government and Health Sector

1. Given the increasing number of cyberattacks, there is no doubt that we must continue to strengthen our country’s cybersecurity defenses. As we have heard during other hearings held by this Committee, improving the ability to share information about emerging threats between the private sector and the federal government is critical to thwarting cyberattacks.
 - a. You noted in your remarks that health systems need more collaboration and intelligence sharing from federal agencies regarding threats to our systems to protect patients’ health care data. Could you tell us how you believe the federal government could more rapidly and efficiently share cyber threat information with the health care sector?

Response

The federal government can take several steps to share cyber threat information more rapidly and efficiently with the healthcare sector:

1. Develop a standardized information sharing process: The federal government can work with healthcare organizations to establish a standard process for sharing cyber threat information. This process should be easy to use, widely adopted, and free for participating healthcare organizations. It should also include clear guidelines for how threat information should be shared.
2. Enhance coordination and collaboration with the healthcare sector: The government should work closely with healthcare organizations to ensure that cyber threat information is shared in a coordinated and collaborative manner. This can involve establishing regular meetings and forums for sharing information, as well as developing relationships between government and healthcare stakeholders.
3. The federal government should work to enhance collaboration and information sharing between government agencies to improve threat intelligence accessible to all government agencies as well as improving threat intelligence shared with the healthcare sector.
4. Provide timely and actionable information: The federal government should ensure that the cyber threat information it shares with healthcare organizations is timely, accurate, and actionable. This can involve leveraging automated tools to collect and analyze threat data, as well as working with healthcare organizations to understand their specific needs and priorities.

5. Invest in cybersecurity education and training: The government can invest in cybersecurity education and training for healthcare organizations to help them better understand the threat landscape, develop the skills needed to protect their systems and data, and build a talent pipeline to address the growing demand for this skillset across all sectors that make recruitment by healthcare organizations more challenging.
6. Streamline regulatory compliance: The government can work to streamline regulatory compliance requirements for healthcare organizations, which can help reduce the burden of compliance and free up resources for cybersecurity activities.

Overall, by taking these steps, the federal government can help healthcare organizations better protect themselves from cyber threats and ensure that critical patient data remains secure.

Post-Hearing Questions for the Record
Submitted to Kate Pierce
From Senator Thomas R. Carper

“In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector”
March 16, 2023

Lessons Learned

I often say that we should find out what works and do more of it. I suspect that we have learned a lot from recent cyber incidents, and we could apply these lessons learned moving forward.

I understand that Fortified Health Security serves as a cybersecurity partner to hundreds of health care systems across the United States. I imagine you have learned a lot of what is working and what isn't when it comes to cyber security in the health care industry.

Question

1.a. What lessons have been learned from the recent cyberattacks on the health care industry?

Response

Cyberattacks in health care have continued to increase in number and escalate in severity over the past ten years, creating an unprecedented threat to our nation's healthcare systems in 2023. Data breaches have soared with a recent threat report from HHS indicating that more than 385 million patient records have been exposed due to breaches from 2010-2022, with hacking/IT incidents (aka cybersecurity incidents) now far outpacing all other types of incidents combined. (See HHS document: [EMRs a Top Target for Cyber Threat Actors](#)). In addition, the average costs of a data breach in healthcare soared to over \$10.1 million in 2022, nearly twice the next critical infrastructure sector. The United States was targeted more than four times as frequently as any other country when it comes to ransomware attacks in 2023 thus far. In late April 2023, HHS published an extensive document that I had the pleasure of collaborating on called "[Hospital Cyber Resiliency Initiative Landscape Analysis](#)". This document does a tremendous job outlining the current state of health sector cybersecurity for the sector as a whole.

So, what have we learned from all this recent cyber activity?

Fortified has been called to assist with post-attack recovery at several facilities, and found some common trends:

- Small and rural facilities often struggle to implement even basic security controls, so these key deterrents to attacks are often not being implemented at all or may be implemented inconsistently and/or incompletely.
- Lack of skilled cybersecurity staffing to manage and monitor basic controls is contributing to the number and severity of these cyber-attacks.
- The inability of small and rural facilities to adequately fund their security programs is a significant contributor to the poor cyber hygiene within these organizations.
- Lack of governance structure or a security program
- Risk assessments often reveal high level risks, but these risks are not remediated due to lack of staffing and/or funding.
- Inconsistent guidance from various government agencies increases the difficulty of implementing proper security measures.
- Cyber insurance companies are increasingly requiring more security controls in order for hospitals to acquire cyber coverage, with the premiums skyrocketing, and the coverage decreasing, especially for small and rural facilities that may not be able to implement all the required elements.
- Requiring organizations to implement basic security controls, such as user access with multi-factor authentication, adequate system backups, logging and alert monitoring of systems 24/7, timely patching of network assets, and proper configuration of internet facing devices could go a long way in improving the security posture of healthcare organizations.
- Any requirements imposed must be coupled with funding and incentives to ensure our small and rural facilities remain open to serve our rural patients.

Question

1.b. What are some best cybersecurity practices shared across the health care sector?

Response

Since the Cybersecurity Information Sharing Act of 2015, a tremendous amount of progress has been made in healthcare with providing information sharing, recommendations, and guidance. Key resources from the Health Sector Coordinating Council Cybersecurity Working Groups (HSCC CWG), 405(d), HHS, CISA, Health-ISAC, ASPR, and other agencies have been extremely helpful in educating healthcare

professionals on proper cyber hygiene, sharing threat information, and making recommendations on network security.

Some best practices are outlined in the Health Industry Cybersecurity Practices (HICP – pronounced “hiccup”) document that was originally released in 2018 and updated in 2023. This document outlines the five main threats in cybersecurity for health systems, and the ten best practices, and is broken down into recommendations for medium and large facilities, and another volume for small organizations.

Other best practices include:

- Performing a regular risk assessment that identifies high, medium, and low risks followed by a remediation plan.
- Required security awareness training for staff which leads to an organizational security culture (employees are our greatest risk).
- Best-practice sharing across organizations.
- A proper governance structure for security programs, including board involvement.
- Adoption of either the HICP or NIST CSF (National Institute of Standards and Technology Common Security Framework) including:
 - Basic Email and Endpoint Protections (such as MFA, antivirus tools, etc.)
 - Supply Chain Risk Management (including Third Party Risk)
 - Remote Access Management
 - Critical Monitoring and Incident Response/Recovery Actions
 - Vulnerability Management and Mitigation

Post-Hearing Questions for the Record
Submitted to Greg Garcia
From Senator Thomas R. Carper

“In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector”
March 16, 2023

Communication between CISA, HHS, and Health Sector

1. We have had many hearings before this Committee on the significant cyber threats our country is facing. An issue I often focus on is whether or not victims of cyber incidents know who to turn to when a cyber incident occurs.

a. Can you please elaborate on how the federal government – specifically the Cybersecurity and Infrastructure Security Agency and the Department of Health and Human Services – is working with the many hospitals and health care providers across the U.S. to create effective and swift pathways for communication when a cyber-attack occurs?

A: I cannot speak for the government about their specific plans for coordinating with hospitals and health care providers in the aftermath of a cyber incident. I can observe, however, that:

- HHS and CISA are enhancing their coordination efforts for outreach to and assistance for health systems in need, leveraging CISA’s technical capabilities and HHS’s sector specific knowledge
- HHS reportedly is working to enhance the capabilities and resources of the Health Sector Cyber Coordination Center (HC3), which serves within HHS as an outward-facing knowledge and analysis center for health sector-specific cybersecurity information and practices
- More generally, we are seeing signs that HHS is organizing its SRMA responsibilities to be more proactive and response to the health sector in terms of preparedness, information sharing and incident response. The recent joint publication by HHS and the HSCC of Health Industry Cybersecurity Practices, the 405(d) Program’s Knowledge on Demand, and the Hospital Cybersecurity Resiliency Landscape Analysis, as well a NIST Cybersecurity Framework Implementation Guide and an upcoming joint playbook on Operational Continuity-Cyber Incident demonstrate a beefed-up and accelerated partnership between the private healthcare sector and HHS
- Health providers do often report confusion about who to report at the Federal level, while many leverage relationships with law enforcement and other government systems at the state, regional and local level.
- Some health systems are taking advantage of CISA-offered assistance, such as Cyber Information Sharing and Collaboration, the Automated Indicator Sharing Program, table top exercises and others that give health systems visibility into their vulnerabilities and recommended remediations.

b. How can this communication be improved?

A: Timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should as a matter of protocol under MOU consult ahead of publication with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence. This would ensure that both industry and government leaders are generally aligned before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

Within an organization during an incident response activity is chaotic as teams are trying to figure out the problem, its scale and impact, internal and external communications and how to mitigate. In addition, there are myriad stakeholders – regulators, press, clients, partners, etc. – who are trying to obtain information from these very same responders. Obviously, this component adds to the chaos. That is why having plans and relationships in place beforehand is so vital.

When it comes to cyber incident response, the focus has been on reporting incidents within certain timeframes versus collaborating and coordinating on response. Industry has been open that this approach/focus places emphasis on compliance and reporting and takes essential resources away from response activities.

In addition, there has been concentration on single organizational incidents instead of large-scale incidents that could have cascading impacts within the sector and across critical infrastructure.

The scope of the incident is also a factor. Is it limited to one organization? Does it impact others? Are there regional, national, or international impacts? The broader and more significant the impact then there is a greater need for coordination at various levels; national, state, local, cross-sector, public, private, for example.

Incident response is what the Information Sharing and Analysis Centers (ISACs) do and excel at. For decades they have served as collaboration, coordination and information sharing/situational awareness points for the sector and cross-sector as well as with government and law enforcement as applicable. ISACs can quickly assess impacts, provide industry perspective, and can scale as one interface during a threat or incident.

An example of this is the industry response to Petya/Not Petya. In June 2017 the attack was launched and immediately had severe, global impacts. There was a lot of misinformation pushed out at the time as entities scrambled to figure out what was going on. Within 48 hours a group of 60+ analysts and individuals from some 30+ Health-ISAC member organizations collaborated to identify, what the attack was, how the initial infection took place and spread and then developed a ‘vaccine’ to stop the spread. This was shared with sector partners and across the globe via the Health-ISAC website.

The Health-ISAC, whose operational mission complements the strategic and policy focus of the Health Sector Coordinating Council, has conducted an annual exercise in conjunction with government and law enforcement called the Hobby Exercise, which examines how the government, law enforcement and industry coordinate and collaborate during an incident. It looks at the gaps and areas for improvements and addresses them.

In summary, there are a number of possible improvements to industry-government coordination on threat intelligence sharing and incident response, enumerated below, some of which are variations on related themes:

- Place less focus on reporting/compliance, and place more emphasis on collaboration, coordination and sharing.
- Support and encourage scale and coordination through sector industry bodies like the Sector Coordinating Council and the ISAC, which are designed as part of the National Infrastructure Protection Plan (NIPP) to represent owners and operators of critical infrastructure.
- Encourage participation in sector exercises like Hobby and others as applicable that are focused on incident response.
- Tailor a classified information sharing program involving health sector-designated liaison representatives, CISA, HC3, and law enforcement agencies, so that the liaison representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the Sector.
- CISA should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities under CIRCIA 2022.
- Implementation should include consideration of waivers from victim reporting requirements while the incident response is underway in the early stages of discovery and operational triage.
- Provide federal-sponsored incident response support for organizations that are experiencing security incidents and need assistance getting through and recovering from the breach.
- Fund a federally-sponsored cyber incident insurance modeled after FEMA to compensate for the retraction of private insurance carriers from the cyber insurance market.
- Expand innovative law enforcement disruption initiatives against threat groups (e.g., botnet takedowns) to reduce ecosystem risk creating the most harm to hospitals.
- Incident reporting timeframes and methodologies should be standardized across government regulatory entities – e.g., CISA, SEC, OCR, etc. Health systems are burdened with multiple differing report forms and overlapping agency requirements for the same incident.
- The same civil, regulatory, FOIA and anti-trust protections provided under CISA 2015 for cyber threat information sharing with the federal government should be provided for: 1) victim organizations that have implemented recognized cybersecurity practices, as defined under PL 116-321 and 2) discussions with government to determine impact of attack on public health and safety. This in effect is a “safe harbor” incentive: if you report and you’re following NIST CSF/HICP then you’re “safe”.

- 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.
- HHS, CISA, and FBI should consider negotiating a pre-approved template for “request for technical assistance” from a health system struggling to respond to and remediate the effects of a cyber attack, such that the request can be processed quickly across the interagency to provide timely assistance to the victim organization. This would be modeled after a similar RTA negotiated between the financial sector and the government.

Thank you for the opportunity to comment.

##

