Cybersecurity in Healthcare

Combating Challenges through Public Private Partnership

By Mia Heck and Sydney McCormick

September 2024



Rainey Center



EXECUTIVE SUMMARY

The healthcare industry has experienced a dramatic increase in cybersecurity threats.

Recent high-profile attacks, including incidents involving healthcare technology company Change Healthcare and hospital system Ascension, have raised awareness of the sector's vulnerabilities and lack of preparedness to combat bad actors. These system breaches have resulted in significant delays in patient care, financial losses, operational handicaps and large-scale exposure of sensitive personal health information. Unlike other critical infrastructure sectors, healthcare lacks uniform cybersecurity standards, leading to inconsistent security measures and increased vulnerability.

The growing occurrence of cyber-attacks on the U.S. healthcare system has prompted policymakers to consider what our state and federal governments can and should do to mitigate threats. At the federal level, policies under consideration in both the executive and legislative branches reflect the growing risk and importance of cybersecurity in safeguarding patient data and ensuring the integrity of healthcare services. Many proposed policies are centered on reporting and informing affected individuals of data breaches, but lack in preventive efforts that could protect systems and personal health information. This report outlines some of the key challenges, along with some recommendations for policymakers as they weigh the growing threat and possible path forward to help protect this facet of critical infrastructure in the U.S.

What is Cybersecurity?

The National Coordinator for Critical Infrastructure Security and Resilience (CISA) defines cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."



INTRODUCTION & BACKGROUND

The U.S. healthcare industry has become a prime target for cybercriminals, as standard practices that are in place to address cybersecurity do not address the unique challenges that persist in healthcare.

Between 2018 and 2022, the U.S. Department of Health and Human Services (HHS) Office of Civil Rights tracked a 278 percent increase[1] in ransomware

1 U.S. Department of Health and Human Services (2023) https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html#:~:text=According%20to%20the%20HHS%20Office,the%20nation%27s%20defenses%20against%20cyberattacks

attacks, and a 256 percent increase involving large data breaches and hacking on healthcare entities. The consequences of these breaches range from delays in patient care, cash flow issues for medical facilities, leaks of sensitive information, frozen pharmacy payments, and threats to patient access to emergency care.

As the designated authority for the Healthcare and Public Health (HPH) sector, the U.S. Department of Health and Human Services (HHS) currently lacks mandated minimum cybersecurity standards[2] for healthcare entities. Preventative measures have been overlooked for years. While a lack of standards offers flexibility to organizations to choose and oversee their internal systems, that lack has resulted in inconsistent and inadequate cybersecurity practices, ultimately jeopardizing patient data, access to care, and risk to patient care and safety.

The absence of technical standards has left the U.S. healthcare system with challenges that must be addressed. Specifically, the patchwork of state requirements to protect personal health information and health data systems between state and federal levels is a challenge to comply with for organizations that operate regionally or nationally. This creates increased vulnerabilities as healthcare entities implement varying security measures based on their interpretation of regulations and available resources. As the current lack of guidance heightens the threat of cyber-attacks on private healthcare organizations, the industry and regulatory bodies continue to be in a reactive posture, rather than focusing on measures that could prevent data breaches and large-scale attacks. Hospitals are particularly vulnerable, as they often operate on break-even or inconsistent margins,[3] causing them to put off updating operating systems and forgo other critical organizational updates that could possibly prevent operational failures. There is also a great disparity in the types of systems hospitals use, with many of them dependent on end-of-life operating systems with known vulnerabilities.[4] Cybercriminals understand these realities and are continuously looking to exploit them at our expense.

Some healthcare entities face a difficult cost-benefit analysis. In the short term, paying a ransom could be more economical than investing in preventive cybersecurity measures. However, this approach fails to consider the long-term consequences of data leaks and operational disruptions. The sensitive nature of personal health information (PHI) and its potential misuse create additional hurdles to implementing strong security measures, as organizations try to balance patient privacy with the need for data accessibility and sharing.

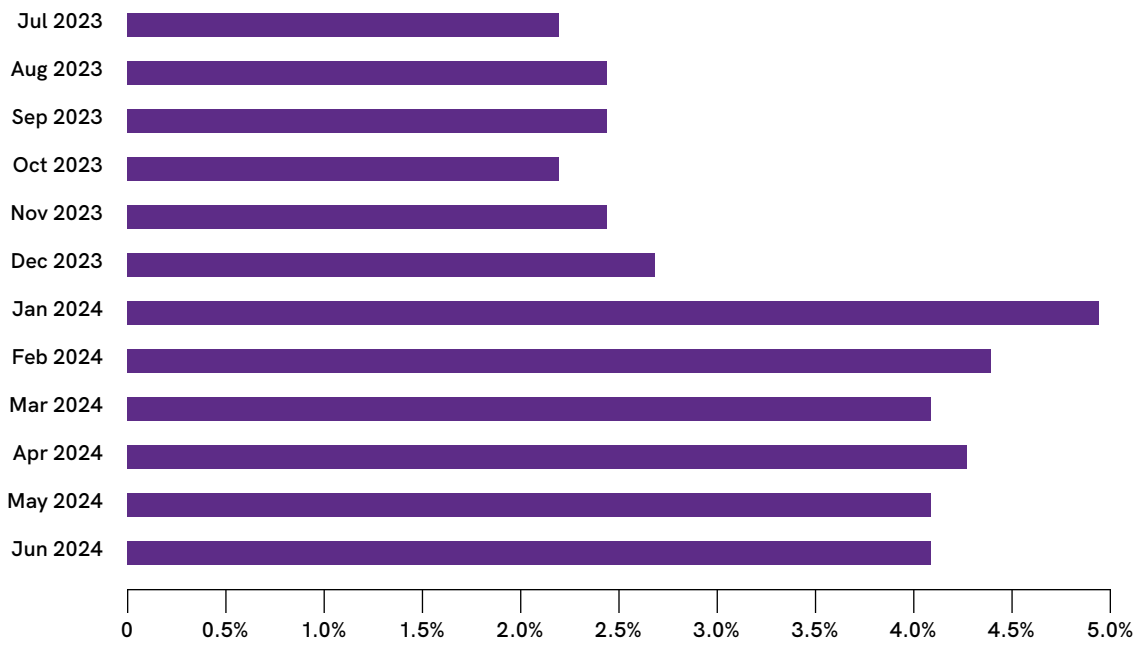
---

2 U.S. Senate Committee on Finance (2024) https://www.finance.senate.gov/chairmans-news/following-unitedhealth-group-ransomware-attack-wyden-urges-hhs-to-require-mandatory-cybersecurity-defenses-for-large-health-care-companies

3 American Hospital Association Blog (2023) by Bharath Krishnamurthy https://www.aha.org/news/blog/2023-08-01-margin-misconceptions-what-do-break-even-hospital-margins-mean-patient-care

4 HHS 405d Hospital Cyber Resiliency Initiative Landscape Analysis by Erik Decker, Robert Wood, Dr. Syed Mohiuddin, Douglas Nock and Akshay Venugopalan (2023) https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

U.S. Hospitals Operating Margin



Hospitals are particularly vulnerable to cyber-attacks, as they often operate on break-even or inconsistent margins, causing them to put off updating operating systems.

+ Limited flexibility for critical investments due to narrow margins
+ Cybersecurity Investment—increasingly important as cyber threats grow more sophisticated



Recent Cybersecurity Attacks on U.S. Healthcare

Many healthcare organizations have become reliant on multiple integrated electronic systems that facilitate their day-to-day business operations, creating different sets of vulnerabilities within their systems. The following examples illustrate how different types and sizes of healthcare entities have become targets of cyber-attacks, that have significantly delayed and disrupted care services and put many individuals and patients at risk for data privacy breaches.

In February 2024, Change Healthcare,[5] a major healthcare payment processing company, was hit by a ransomware attack. Change Healthcare processes 15 billion medical claims annually, accounting for almost 40% of all claims made

5 Congressional Research Service (CRS) Reports (2024) IN12230 https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

in the U.S. annually. The fallout was severe, disrupting prescription fulfillment, freezing pharmacy payments, and medical facilities faced major cash flow issues. Even more alarming, sensitive health information was leaked onto the dark web. UnitedHealth ended up paying a $22 million ransom.

Just a few months later, in May 2024, Ascension,[6] one of the largest hospital systems in the U.S., was hit by a ransomware attack that crippled operations across 142 hospitals. The attack forced affected hospitals to implement emergency protocols and revert to paper-based charting systems, significantly delaying patient care and raising safety concerns. As Ascension focused on remediation efforts, it endured substantial financial losses and grappled with class-action lawsuits, significantly tarnishing their reputation.

In 2023, Prospect Medical Holdings[7] faced a significant cyber-attack, disrupting operations across multiple states. To continue to provide care, Prospect was forced to revert to using paper health records. This incident required FBI intervention. Other smaller-scale data breaches have also occurred, such as the 2022 incident at Logan Health Medical Center[8] compromising the personal information of up to 213,543 individuals, and the 2021 Broward Health data breach[9] which affected over 1.35 million individuals due to unauthorized access via a third-party provider.

In 2021, OrthoVirginia,[10] a provider of expert orthopedic and therapy care, experienced a disabling of their critical data systems, leading to an eighteen-month remediation process. OrthoVirginia eventually restored its operations, and then implemented cybersecurity measures to strengthen its defenses against future threats.

The 2015 Anthem medical data breach[11] exposed the information of nearly 79 million individuals. As a result, Anthem, a large health benefits company, encountered substantial legal and financial repercussions, agreeing to pay $16 million to the U.S. Department of Health and Human Services' Office for Civil Rights to resolve potential HIPAA violations[12] and to institute significant corrective actions. Further, in 2020, Anthem secured a $39.5 million multi-state settlement mandating the adoption of a comprehensive security program.

---

6 Ascension. (2024). *Cybersecurity event*. Retrieved from https://about.ascension.org/cybersecurity-event

7 New York Times (2023). Carballo, Rebecca, Ransomware Attack Disrupts Health Care Services in at Least Three States https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html

8 HIPAA Journal. (2022, February 24). *Logan Health Medical Center cyberattack affects more than 213,000 patients*. Retrieved from https://www.hipaajournal.com/logan-health-medical-center-cyberattack-affects-more-than-213000-patients/

9 HIPAA Journal. (2022, January 4). *Broward Health notifies over 1.3 million individuals about October 2021 data breach*. Retrieved from https://www.hipaajournal.com/broward-health-notifies-over-1-3-million-individuals-about-october-2021-data-breach/

10 Clearwater. (2021). *Clearwater and OrthoVirginia*. Retrieved from https://clearwatersecurity.com/case-studies/clearwater-and-orthovirginia/

11

12 Medicare Learning Network (2023) https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf



Federal Authority Cybersecurity in Healthcare

The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018[13] requires a framework to protect against critical infrastructure risks to be coordinated through codified Sector Risk Management Agencies (SRMA) required by Sec. 9002(b) of the FY 2021 National Defense Authorization Act (NDAA). CISA is a central authority that, through their delegation, coordinates all other critical infrastructure sectors with information to help them combat cyber-attacks.

Pursuant to the Homeland Security Act of 2002, and as amended by Presidential

13 Public Law 115-278 Cybersecurity and Infrastructure Security Agency Act of 2018 (2018), https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf

Policy Directive (PPD) 21[14] HHS serves as the Sector Risk Management Agency[15] (SRMA) for the Healthcare and Public Health sector in the U.S. In this role, HHS' function is to provide technical assistance, share information, and provide training and other assistance and resources with public and private entities so they may be best positioned to protect patients and mitigate risk from cyber threats. Within that function, the CISA, HHS, the Health Sector Coordinating Council (HSCC), and the Cybersecurity Working Group (CWG) work together to provide tools, technical expertise, and training to organizations in the Healthcare and Public Health sector.

While the federal framework to oversee cybersecurity functions is coordinated and based on industry, there are no mandatory technical requirements currently in place for healthcare organizations to adopt that will protect them - or their patients - from cyber-attacks. While training, education, and implementing security practices within organizational networks are critical to protecting against harmful actors, these proposals will not prevent or protect patients or organizations from large-scale breaches of protected health or payment information.

Federal Legislative and Regulatory Proposals

There are trends in legislative proposals in the 118th Congress (2023-2024) for cybersecurity in healthcare. Many require the protection of personal information and reports on protocol updates, however, few are centered around preventing cyber-attacks or system hacking. Here is a sample of current legislation:

U.S. Senator Marco Rubio (R-FL) has introduced legislation S. 3773[16] that would require the HHS Inspector General to evaluate cybersecurity practices that HHS has in place through '…penetration tests and other testing procedures…' that could compromise mission-critical information or expose patient information for Medicare beneficiaries and/or impact patient safety. The bill was introduced prior to the debilitating Change Healthcare cyber-attack, in February 2024. At the time of publication of this report, the aforementioned bill has three co-sponsors and has been referred to the Senate Committee on Health, Education, Labor and Pensions (HELP). The legislation would also require the Office of Inspector General of HHS to evaluate the department's cybersecurity practices every two years.

---

14 Presidential Policy Directive 21 (PPD-21) The White House (2013) https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

15 Cybersecurity and Infrastructure Agency (CISA) Sector Risk Management Agencies (2024) https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies

16 118th U.S. Congress Senate Bill 3773, Strengthening Cybersecurity in Healthcare Act (2024) https://www.congress.gov/bill/118th-congress/senate-bill/3773?q=%7B%22search%22%3A%22cybersecurity%22%7D&s=8&r=3

As of September 2024, the bipartisan H.R. 498[17]: The 988 Lifeline Cybersecurity Responsibility Act has passed the U.S. House of Representatives. This proposed legislation has required notifications for identifying vulnerabilities for providers that receive federal funding and serve the federally-funded, locally-operated 988 Suicide and Crisis Lifeline.

Another proposal is the Cybersecurity Improvement Act of 2024,[18] which mandates that Medicare-eligible payment organizations meet minimum cybersecurity standards, standards to be determined by the Secretary of the U.S. Department of Health and Human Services. The legislation aims to ensure that healthcare providers maintain robust cybersecurity measures to qualify for payments in the event of cybersecurity disruptions.

These federal proposals address some of the complexities at the nexus of federal oversight and the issues affecting healthcare organizations, however, none would protect patient data or prevent a cyber-attack on a private healthcare organization. Technical standards that can be applied as a roadmap for the private sector would be a better provision for industry to put in place.

State Legislative and Regulatory Policy Proposals

Without federal authorities providing uniform standards for the Health and Public Health sectors, states have gotten to work on policy proposals to help protect patients and healthcare organizations from cyber-attacks. According to the National Conference of State Legislatures,[19] in 2023 at least 40 states introduced or considered more than 500 bills or resolutions that deal significantly with cybersecurity. Thirty-nine states, Puerto Rico, and Washington, D.C. enacted at least 130 bills and adopted at least 10 resolutions in 2023. Of those, the most common enactments will:

+ Require government agencies to implement cybersecurity training for private organizations; set up and follow formal security policies, standards and practices; to have incident response plans in place; to provide mandatory training for employees; and to report security incidents, including ransomware attacks
+ Provide funding for cybersecurity programs and practices in state agencies, local governments and schools

---

17 118th U.S. Congress House Bill 498, 9-8-8 Lifeline Cybersecurity Responsibility Act (2023) https://www.congress.gov/bill/118th-congress/house-bill/498?q=%7B%22search%22%3A%22cybersecurity%22%7D&s=7&r=1

18 118th U.S. Congress Senate Bill 4054, Healthcare Cybersecurity Improvement Act (2024) https://www.congress.gov/bill/118th-congress/senate-bill/4054

19 National Conference of State Legislatures (NCSL) Cybersecurity Legislation (2023) https://www.ncsl.org/technology-and-communication/cybersecurity-2023-legislation

- Mandate security practices related to elections
- Establish or support programs or incentives for cybersecurity workforce training and education programs
- Provide provisions for critical infrastructure and limit the procurement of software and supplies from specified sources
- Limit the use of software and applications on government devices

Some notable state legislative policies include Illinois HB 4093[20]: The Protect Health Data Privacy Act. This legislation provides a framework to safeguard patient and personal information that regulated entities must maintain, including the regulated entity obtaining written consent from the patient before disclosing such information, unless in specified circumstances. The Illinois Protect Health Data Privacy Act (H.B. 4093) has only made it through the IL State House Committee and is not expected to be enacted this session, however, absent federal data privacy legislation,[21] state consumer protections specific to protecting patient data is necessary.

The Colorado HB 1130[22] amends the "Colorado Privacy Act" to include new protections for biometric data, such as requiring controllers, who determine the purposes and means of processing biometric data, to adopt a written policy that establishes a retention schedule, a breach response protocol, and guidelines for the permanent destruction of biometric identifiers by certain dates. This new law authorizes the Colorado Attorney General to implement rules for the bill.

In June 2024, Texas Attorney General Ken Paxton proposed the Data Privacy and Security Act,[23] an initiative which will be a newly created office as part of the Texas Consumer Protection Division of the Office of Attorney General, a major data privacy and security initiative, creating a team within the Consumer Protection Division to enforce Texas privacy laws. This team is set to be one of the largest in the U.S. focused on privacy law enforcement with the intent to enforce laws such as the Data Privacy and Security Act, Identity Theft Enforcement and Protection Act, Data Broker Law, Biometric Identifier Act, Deceptive Trade Practices Act, and federal laws like the Children's Online Privacy Protection[24] Rule (COPPA) and HIPAA.

---

20 Illinois 103rd General Assembly House Bill 4093 (2023), https://www.ilga.gov/legislation/BillStatus.asp?DocNum=4093&GAID=17&DocTypeID=HB&SessionID=112&GA=103

21 International Association of Privacy Professionals (IAPP) 118th Congress U.S. Federal Privacy Legislation Tracker, (2024) https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf

22 Colorado 74th General Assembly House Bill 24-1130 (2024) https://leg.colorado.gov/bills/hb24-1130

23 Texas Attorney General Data Privacy and Security Initiative (2024) https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive

24 U.S. Federal Trade Commission (FTC) Children's Online Privacy Protection Rule of 1998 15 U.S.C. 6501–6505



Policy Recommendations

For healthcare organizations, basic enterprise-wide system protections should be put in place to protect organizations from data breaches. However, due to the cost and increasingly fragmented data exchange systems between payers and providers, the U.S. healthcare remains in a state of high vulnerability to attacks on personal health information and from malicious actors.

Whether to have mandated technical requirements for all healthcare entities, or provide more specific requirements tied to different types of entities, such as health insurers, hospitals and other medical providers, is a question to be answered. Is it Congresses job to ensure there are technical standards in place for the Health and Public Health sectors in the U.S.? With the associated cost of the 2024 Change Healthcare cyber-attack reaching $2.45 billion dollars[25] and

25 Becker's Health IT, Laura Dyrda, "Change Healthcare's cyberattack costs soar, may hit $2.45 billion", https://www.beckershospitalreview.com/cybersecurity/change-healthcare-cyberattack-costs-soar-may-hit-2-45b.html#:~:text=UnitedHealth%20Group%20expects%20costs%20associated,at%20%241.6%20billion%20this%20year

affecting the personal health information of up to 1 in 3 Americans,[26] it might be. However, a one-size-fits-all mandated approach would not work for the rapidly advancing world of technology.

We recommend HHS provide standard best practices to health payers and providers that are easy to understand and frequently communicated to ensure up-to-date guidance and compliance on these matters. Standard best practices, along with frequent communication - including regarding elevated risk factors—will assist the private sector in how they situate their operating systems away from a reactive, and into a preventative posture in the cybersecurity space. Tools to better position healthcare organizations, along with oversight and enforcement measures will provide a positive foundation between federal authorities and private and non-profit organizations so they may work together to combat bad actors looking to breach the U.S. healthcare system.

In 2023, two reports outlining Health Industry and Cybersecurity Practices[27] (HICP), one specific to small healthcare organizations and one with best practices for medium-to-large healthcare organizations were published. These reports chronicle the realities for IT vendors, what to look for in endpoint protection systems, and vulnerability management and incident responses to consider in healthcare. While not mandated, this information is significant and necessary, as entities navigate organizational threats that seem to increase every day.

The National Institute of Standards and Technology (NIST) within the Department of Commerce also offers practical resources that organizations can use as a starting point to help protect their systems and train employees to be educated on ransomware[28] and phishing[29] attacks. One-pagers outlining how to educate an organization's tech team and all employees on these practices, can protect sensitive information no matter what sector someone operates in.

---

26 HIPAA Journal. (2024). Adler, Steve, Change Healthcare Reports Ransomware Data Breach to HHS https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

27 U.S. Department of Health and Human Services 405d Health Industry Cybersecurity Practices (2023) https://405d.hhs.gov/cornerstone/hicp

28 U.S. Department of Commerce (DoC) National Institute of Standards and Technology (NIST) Preparing Your Organization for Ransomware Attacks (2021) https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf

29 U.S. Department of Commerce (Doc) National Institute of Standards and Technology (NIST) Protecting your Small Business from Phishing (2024) https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

COMPARATIVE ANALYSIS

Healthcare vs. Finance Industry: What can we learn?

The healthcare industry significantly trails the finance sector in cybersecurity regulations and enforcement, as evident in their differing resource allocation and strategic approaches. While healthcare organizations typically allocate a much smaller portion of their IT budgets to cybersecurity, financial institutions invest significantly more. This disparity reflects the fundamental difference in mindset between the two industries: healthcare adopts a reactive stance towards cyber threats, while the finance sector views cybersecurity as a critical, proactive necessity.

The finance industry's approach to cybersecurity offers valuable lessons for the public health and healthcare sector. In the late 1990s and early 2000s, collaboration between the largest financial institutions led to common cybersecurity standards when they formed the Financial Services Information Sharing and Analysis Center (FS-ISAC). Working in concert allowed for intelligence-sharing in the face of threats and fostered a strong, unified defense against them. The financial sector has seen adherence to strong regulatory requirements, such as compliance with the Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR). All these organizations have in place extensive frameworks, a dedicated incident response team with clear reporting protocols, and an ongoing schedule of risk assessment.

To bridge the gap, healthcare organizations should consider several steps. First, they need to increase their cybersecurity budget. Establishing a Healthcare Information Sharing and Analysis Center (H-ISAC) would facilitate the sharing of threat intelligence. Implementing robust frameworks would provide a structured approach to managing cybersecurity risks. Creating dedicated Cybersecurity Incident Response Teams (CSIRTs) with clear reporting protocols is crucial for promptly addressing cyber threats. Conducting regular risk assessments would help identify and mitigate vulnerabilities.

Common Types of Cyber Attacks

An organization's network system can be compromised in many ways. The most common are ransomware and hacking.

Ransomware
A type of malicious software where system access has been blocked until a sum of money is paid.

Malware (Malicious Software)
Used to attack a system—through a virus—which can infect a system and change how the computer works, or through worms designed to infect a computer's operating system. Malware can be sourced from documents, email attachments, advertisements, downloads, or network connections.

Password Attack
Commonly used and can be by obtaining a password, by shoulder surfing, or other means of maliciously obtaining passwords.

Email Attack
Used to access an organization's server through phishing or encouraging people to share their personal information through email communication, or spoofing, where the attacker poses as another organization alerting the individual of a problem with another existing account or subscription, prompting the sharing of personal information the person might not otherwise share.

Email Attachment
Once clicked on or downloaded, can be used to access a system network with the intent to harm. Attachments can be shared as files, photos, audio or video.

Distributed Denial of Service
When an attacker uses a botnet to flood a system's server so it will be overwhelmed, ultimately shutting that resource (website, application) down.



CONCLUSION

The disruption and delay of care caused by cyber-attacks is a threat to patient care and safety.

Many current policy proposals require the reporting of data breaches, however, few are centered around the prevention of system hacking or cyber-attacks. Hospitals, healthcare providers and health insurers should work with federal authorities and to receive and implement standard best practices to mitigate threats and protect their data systems. Federal authorities should monitor all possible threats, and frequently communicate threats to Health and Public Health organizations so they may choose software and internal protocols that will best integrate into their operations, avoid a one-size-fits-all approach to safeguarding patient data while mitigating the threat of cyber-attacks.

ABOUT THE AUTHORS

Mia Heck

Mia Heck is a Senior Fellow for Health Policy at the Joseph Rainey Center for Public Policy and government affairs consultant in Washington, DC. With nearly two decades of experience in policy, government service and strategic planning, Mia's career has been defined by a commitment to community-based care models and national government relations initiatives, driving ideas for policy reform across health and human services programs. Having previously served as a Schedule C appointment in the Presidential Administrations of George W. Bush and Donald J. Trump, Mia also served as the Director of Federal Health Policy at Change Healthcare. In this role she provided strategic guidance on critical policy issues impacting healthcare technology.

Sydney McCormick

Sydney McCormick is a student at Virginia Tech's Honors College, studying Clinical Neuroscience and Spanish on the premedical track. She has an interest in the intersection of healthcare and technology, with a focus on cybersecurity in the healthcare industry. Sydney recently completed a summer internship with the Joseph Rainey Center for Public Policy, furthering her understanding of public policy's impact on healthcare.





Rainey Center

(202) 350-1689
info@raineycenter.org
raineycenter.org