TLP:WHITE

February 2024

Executive Summary for CISOs: Current and Emerging Healthcare Cyber Threat Landscape

This report is a collaboration between Health-ISAC and the American Hospital Association (AHA)

TLP:WHITE This report may be shared without restriction. For Health-ISAC members—be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™ SHARING SINCE 2010 Collaborating for Resilience in Healthcare

American Hospital Association™

health-isac.org

Contents

Introduction

Some call it the wall of shame – the U.S. Government website that lists healthcare industry data breaches since 2009 – breaches which have put millions of patients' Protected Health Information (PHI) at risk. The site, run by the Department of Health and Human Services Office for Civil Rights (OCR), reports breaches affecting the PHI of 500 or more individuals. When Health-ISAC reviewed the data in mid-2023, the site listed 5,558 events totaling nearly 438 million breached PHI records. **That averages to more than 86,000 PHI records exposed every single day for the past 13 ½ years.** What's even more troubling is that the number of incidents reported is increasing at an alarming rate. In just the last three years alone, 2,209 incidents were reported, whereas a total of 3,349 incidents were reported in the first 10 ½ years of reporting.

The breach disclosures highlighted here are just an indicator. It's one piece of the very complex reality of cybersecurity in the healthcare sector.

This executive summary is intended to give Board of Directors, Chief Information Security Officers, Chief Security Officers and cybersecurity and physical security executives in healthcare an overview of threat trends to improve their understanding of, and ability to protect against, the current and projected threat landscape. The report also includes cybersecurity market trends that leadership can use for strategic decision making.

The Executive Summary Report here is a condensed version of a more comprehensive report created by analysts from Health-ISAC and is based on experiences provided by Health-ISAC member organizations, threat intelligence providers, open-source research and interviews conducted with key leaders in the sector to give the most diverse and experienced perspective possible.

Annual Member Survey Insights

Survey Background

In a November 2023 survey, executives and cybersecurity professionals (n=396) across the health sector completed a survey and ranked their top five "greatest cybersecurity concerns" facing their organizations for both 2023 and 2024. The survey included cyber (e.g., CISO) and non-cyber executives (e.g., CFO), multiple healthcare subsectors (e.g., Providers, Pharma, Payers, Medical Device Manufacturers, Health IT) as well as healthcare organizations of varying size and IT/IS budget. Survey responses were received from members of:

- Health-ISAC
- American Hospital Association (AHA)
- Health Sector Coordinating Council (HSCC)
- College of Healthcare Information Management Executives (CHIME)
- Association for the Advancement of Medical Instrumentation (AAMI)

Survey Findings

Key Insights

- Professionals in the Healthcare Sector expressed the same top three concerns from 2023 to 2024, though third-party risk replaced compromised credentials in the top five cyber threats for 2024.
- Healthcare organizations, regardless of budget, are most concerned about ransomware attacks going into 2024.
- Organizations with large cybersecurity budgets were most concerned with ransomware deployments while organizations with small cybersecurity budgets were most concerned about spearphishing in 2023.

The Top Five Cyber Threats looking ahead towards 2024 reported by executives are:

1. Phishing/Spear Phishing Attacks
2. Ransomware Deployments
3. Data Breaches
4. Third Party/Partner Breaches
5. Social Engineering

"In recent years, we as a healthcare cybersecurity community have come together to develop and share best practices, exchange cyber threat intelligence across the sector and with government and to focus on preparing for the clinical impact of the ever increasing and damaging ransomware attacks. It is clear to healthcare technical and non-technical leaders alike that cyber risk is an enterprise risk issue, which poses a risk not only to the security and privacy patient data, but to patient care and safety.

Yet, despite our collective best efforts and close partnership with federal agencies, 2023 may turn out to be the worst year yet in terms of the frequency, severity and impact of cyber-attacks targeting healthcare. According to data obtained from HHS's Office of Civil Rights, there were approximately 550 hacks of protected health information impacting *108 million individuals* in 2023. The only other year which approximates that number was in 2015, when a single hack against a major healthcare insurer resulted in the theft of the healthcare records of 80 million individuals. Absent that event, no other year even comes close to the number of individuals impacted by the loss of PHI in 2023 — which is 2.5 times the number of individuals impacted in 2022 and 2021, and almost quadruple the number in 2020.

Most concerning is the dramatic increase in ransomware attacks targeting healthcare. HHS has reported a nearly 300% increase in these ransomware attacks in recent years. We have seen and felt the impact firsthand — ambulance diversions, canceled elective surgeries, unavailability of electronic medical records and delayed cancer treatments. Clearly, ransomware attacks that result in the delay and disruption of healthcare delivery are not financially motivated crimes, as these foreign hackers would have us believe; they are, in fact, ***threat-to-life crimes***.

We as a healthcare cybersecurity community must continue to exchange cyber threat intelligence and collaborate to define effective defensive measures and increase resiliency. No doubt, this will help us identify cyber threats, defend against them — and ultimately prepare for impact.

That's why we at American Hospital Association are proud of our ongoing partnership with Health-ISAC, including assisting in the preparation of this cyber threat executive summary report for CISOs. In healthcare, we are all stronger together in the face of this common international threat. Our mutual respect and collaboration will help defend our global healthcare community and our patients against these heinous attacks."

John Riggi, National Advisor for Cybersecurity and Risk
American Hospital Association

Part I: Recent Attacks Against Healthcare

Hacktivism

Hacktivism is the act of civilians attacking critical infrastructure in a political response to geopolitical conflicts. Some examples of hacktivism that impacted the healthcare sector in 2023 include:

- **Pro-Russian hacktivist group Killnet** – attacked hospitals in the United States and European Union in response to continued Western military support to Ukraine.
- **Pro-Islamic hacktivist group, Anonymous Sudan** – attacked Western hospitals in response to a public burning of the Quran in Sweden.
- **Pro-Palestinian hacktivist groups** – attempted to cause chaos in Israel by getting a missile-tracking app to falsely claim a nuclear missile had been launched toward Israel.[1]

Physical Security

Healthcare facilities have been experiencing staffing deficiencies. Staff have reported feeling overworked from increased patient frequencies, and inflation rates. Disagreements over vaccination requirements saw large numbers of staff leave of their own free will or because they were let go.

The end of the Public Health Emergency (PHE) in the United States caused disruptions in healthcare coverage and increased government focus on rooting out instances of healthcare fraud. Under the PHE there was very little oversight into who was accepted into government healthcare programs such as Medicare and Medicaid to provide access to COVID treatment as widespread as possible.

Workplace violence has seen a steady increase since the onset of the COVID pandemic.[2] Controversy over the effectiveness and requirement to receive the COVID vaccine, combined with increased healthcare costs, has created an environment of distrust in medical personnel.

[1] *How hackers piled onto the Israeli-hamas conflict*. POLITICO. (n.d.). https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593

[2] Yang, J., & Mufson, C. (2023, September 17). *What's behind an alarming rise in violent incidents in health care facilities*. PBS. https://www.pbs.org/newshour/show/whats-behind-an-alarming-rise-in-violent-incidents-in-health-care-facilities

Part II: The Current Threat Landscape

Artificial Intelligence (AI)

Generative AI, or GenAI took the spotlight in 2023, representing incredible and new benefit to organizations in improved healthcare. Despite the benefits, hasty adoption of AI can lead to unnecessary risks in the corporoate environment.

Some ways premature adoption of GenAI can be harmful to healthcare organizations are:

- Ambiguous data storage policies
- Use of sensitive data as training data
- AI hallucinations, the act of the AI suggesting false information as truth

Some ways GenAI can present external threats to healthcare organizations include:

- Creation of convincing phishing emails using the linguistic ability of GenAI
- Threat actors increasing the sophistication of malware using AI-generated code
- More convincing disinformation campaigns targeting healthcare using AI-generated images and audio

Notable Ransomware as a Service (RaaS) Groups

Ransomware-as-a-Service (RaaS) is a business model where cyber-criminal organizations create and maintain the infrastructure to operate ransomware attacks. Cybercriminals can then purchase access to these platforms and use the ransomware group's code and tools to carry out their own attacks, paying a cut of any profits earned to the group. These patrons of the RaaS service are known as affiliates.

The thing that makes these RaaS groups so menacing is the fact that they are opportunistic, and often operate with no regard for the organizations they victimize, leading to the targeting and further victimization of hospitals and other healthcare entities.

Healthcare represents a unique opportunity for these RaaS affiliates because they know the incentive for a healthcare provider to pay the ransom extends beyond money, involving the prevention of harm to patients.

Below are the top 5 ransomware operators targeting healthcare in 2023:

1. **Lockbit 3.0** – attacked 68 healthcare organizations in 2023
2. **ALPHV/BlackCat** – attacked 61 healthcare organizations in 2023
3. **Cl0p** – attacked 40 healthcare organizations in 2023
4. **BianLian** – attacked 24 healthcare organizations in 2023
5. **8Base** – attacked 21 healthcare organizations in 2023

Enforcement Action Against BlackCat/ALPHVM

The US Department of Justice announced on December 19, 2023, the launch of a disruption campaign against a ransomware group that targeted the computer networks of more than 1,000 victims, including networks that supported critical infrastructure. The Blackcat ransomware group, also known as ALPHV or Noberus, became the second-most prolific ransomware-as-a-service variant in the world during the past 18 months, based on the hundreds of millions of dollars in ransoms paid by victims. Multiple foreign law enforcement agencies are also conducting investigations into the ransomware group.

The FBI developed a decryption tool that was used by more than 500 BlackCat ransomware affected victims to restore their systems. The agency worked with dozens of victims in the U.S. and internationally to implement the tool, and has saved victims from approximately $68 million in ransom demands.

Nation State Activity

Nation-state attacks refer to attacks carried out by state-sponsored threat actors. These attacks are often very sophisticated and difficult to defend against.

Nation-state attacks are often carried out against healthcare research and development (R&D) organizations in the form of cyberespionage operations aimed at stealing intellectual property to bolster the healthcare of the country sanctioning the attack. These attacks are often successful, due to their use of custom malware and zero-day exploits. Some examples of nation-state attacks against healthcare in 2023 are as follows:

- **YoroTrooper** – YoroTrooper was a prominent cyber espionage campaign targeting European and The Commonwealth of Independent States (CIS)* governments, including a critical EU health agency with the objective of obtaining intellectual capital.[3]
- **Jaguar Tooth** – a Russian nation-state cyberespionage campaign using Jaguar Tooth, custom malware created by Russian nation state actors to compromise Cisco IOS routers and steal intellectual property from the victim networks.[4]

Geopolitical Activity

US President Joe Biden signed an executive order[5] on August 9, 2023, that prohibited US advanced chip manufacturing in China, citing national security concerns. This act was met with export bans from China, straining tensions further, leading the two nations to prioritize trade with politically allied countries. Because of this, a renewed interest was placed on bolstering regional economic partnerships. Widening the schism between the East and West, placing the healthcare supply chain at risk of raw material shortages in 2024.

Notable Threats to Operational Technology in Healthcare

Four key cybersecurity challenges facing companies operating in Operational Technology (OT) or Industrial Control Systems (ICS) environments are:

- Exploitation of Older Vulnerabilities
- Backdoor Deployment
- Ransomware Attacks
- Hacktivist Attacks with Physical Consequences

[3] Malhotra, A. (2023, April 4). *Talos uncovers espionage campaigns targeting CIS countries, embassies and EU Health Care Agency*. Cisco Talos Blog. https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

[4] APT28 exploits known vulnerability to carry out reconnaissance ... - cisa. (n.d.-b). https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers.pdf

[5] The United States Government. (2023, August 9). *Executive order on addressing United States investments in certain national security technologies and products in countries of concern.* The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/

Part III: Notable Threats and Vulnerabilities Observed in Healthcare

This section of the report explores common threats and vulnerabilities observed by the Health-ISAC Threat Operations Center being used by threat actors to attack healthcare in 2023.

Attacks Against Healthcare

In 2023, Health-ISAC observed an increase in anti-analysis mechanisms in the malware targeting healthcare. This malware was seen being delivered to healthcare organizations through more sophisticated methods like malspam email campaigns to increase the likelihood of installation on victim systems.

Malware Used Against Healthcare

- In 2023, Health-ISAC consistently observed two strains of malware targeting healthcare organizations, IcedID[6] and Qbot[7] Once installed, both steal sensitive information and allow threat actors to carry out additional attacks such as ransomware.

Vulnerabilities Exploited in Healthcare

Below are the most notable vulnerabilities exploited by threat actors to gain access to healthcare networks in 2023:

- **MOVEit Transfer Critical Vulnerability** – A vulnerability in the MOVEit Managed File Transfer application was used by the Cl0p ransomware gang to steal proprietary information from thousands of organizations globally.
- **Adobe ColdFusion** – The Adobe ColdFusion vulnerability allowed attackers to remotely execute code with elevated privileges.
- **Citrix NetScaler ADC and NetScaler Gateway Vulnerabilities** – CVE-2023-3519 and CVE-2023-4966 (Citrix Bleed), were actively exploited by multiple threat actors throughout the year. With Citrix being one of the commonly used software in the healthcare sector, Health-ISAC's Threat Operations Center sent 249 targeted alerts to member organizations, notifying them about vulnerable Citrix systems on their networks. On December 1, 2023, AHA broadcast a national alert to all hospitals because it was believed this vulnerability was being exploited to execute numerous ransomware attacks against healthcare.

Social Engineering Attacks

Health-ISAC observed social engineering efforts primarily targeting helpdesk personnel in healthcare. There was an observed increase in phishing emails using QR codes to disguise malicious links to increase the likelihood of victim interaction.

[6] *IcedID: Analysis and detection - vmware security blog - vmware. (n.d.-c).* https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html

[7] Protecting the sick: Cyberattacks targeting the healthcare ... - blackberry. (n.d.-e). https://blogs.blackberry.com/en/2023/04/protecting-the-sick-cyberattacks-targeting-the-healthcare-industry

Part IV: Future Cybersecurity Outlook

Weaknesses in critical infrastructure security were felt by governments across the globe. From congressional think tanks in the US to the EU cybersecurity agency, assertions of insufficient cybersecurity measures for critical infrastructure and healthcare were made. These documents and directives helped create an atmosphere of increased cybersecurity prioritization on a global scale in 2023.

- **US Call to Revise Presidential Policy Directive 21 (PPD-21) to Fit 2023** – A report arguing that the current measures to secure critical infrastructure are insufficient at the national level, advocating for more information sharing.[8]
- **EU NIS2 Directive** – An updated version of EU cybersecurity rules meant to respond to the evolving cyber threat landscape by bolstering EU member States' preparedness and cooperation regarding critical infrastructure security.[9]
- **European Healthcare Cyber Threat Landscape** – The EU Agency for Cybersecurity (ENISA) has released its first cyber threat landscape report for the healthcare sector[10] revealing ransomware as the primary threat to the healthcare sector.

[8] Ackerman, D. (2023, June 7). *Revising public-private collaboration to protect U.S. Critical Infrastructure*. FDD. https://www.fdd.org/analysis/2023/06/07/revising-public-private-collaboration-to-protect-us-critical-infrastructure/

[9] *The NIS2 directive: A high common level of cybersecurity in the EU: Think tank: European parliament.* Think Tank | European Parliament. (n.d.). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[10] Health threat landscape. ENISA. (2023, July 17). https://www.enisa.europa.eu/publications/health-threat-landscape

Part V: CISO Exclusive Market Summary

Brand new for the 2024 Annual Threat Report is the CISO Exclusive Market Summary for cybersecurity products in healthcare. The cybersecurity trends compiled here are based on the purchasing decisions of C-Suite executives across all industries.

Key Takeaways:

- GenAI presents both opportunities and risks: Embrace its potential with caution, prioritizing data security, governance, and responsible application.
- Invest in integrated solutions: Look for platforms that offer SOAR capabilities to improve efficiency and mitigate risk.
- Modernize defenses: Move beyond legacy systems like AV and EDR, adopting XDR for comprehensive detection and response.
- Prioritize data protection: Clearly define data ownership and responsibilities, ensuring robust asset management and access control.
- Embrace cloud-based solutions: Leverage agentless vulnerability scanning and centralized CSPM for greater visibility and efficiency.
- Secure the API: As API complexity increases, invest in dedicated security tools and disciplines to minimize weaknesses and data exposures.
- Consider SASE/CASB/DLP and CAASM: Explore these new architectures and tools, but be mindful of potential implementation complexities.
- Continuously evaluate and adapt: The cybersecurity landscape is dynamic. Stay informed, test your defenses, and evolve your strategies to stay ahead of threats.

By understanding these trends and prioritizing strategic investments, healthcare organizations can build a robust cyber defense posture, protecting sensitive data, ensuring patient safety, and fostering trust in the digital age.

Listed below are some of the trends Health-ISAC sees for 2024 and beyond:

Technology Area / Topic	What's Hot
• Generative Artificial Intelligence (GenAI) • Large Language Models (LLMs) • ChatGPT • Google Bard	ChatGPT and Google Bard have been all the rage in 2023. The technological revolution possible through fast advancements in GenAI, coupled with the enormous potential benefits the technology could yield, have captured everyone's attention. But, with all the positive possibilities, new data security challenges are introduced including governance, intellectual property rights, responsible application of AI technology, and model transparency. Plus, the use of Gen AI could also introduce vulnerabilities or weaknesses that could be exploited by adversaries. Those that have been in IT and IT Security a decade ago may look to the lessons learned from the evolution of migration to cloud. Top Global Banks are denying access and forcing a business case with no PII sharing, an approach that aligns with their extremely cloud careful approach. Health-ISAC encourages organizations to take a conservative approach on the adoption of GenAI and CISOs be mindful as everyone is still learning the promises and perils of what GenAI has to offer. Questions CISOs should be asking their teams, business partners, third party vendors, etc: • Are you allowing public access? Blocking public sites? • Are you building private LLMs in the cloud? • Do you have target use cases like Call Center? AI powered chat? Cloud-based productivity tools? • Are you requiring a make money/save money business case to use generative AI? • Are you allowing sharing of Personally Identifiable Information (PII)? • Have you established a governance process? • Have you established sanctioned site access? Safe list? • How much data science do you have in LLM today? Outside of LLM? • Are you looking at the model protection vendors? • Have you Applied the NIST Trustworthy model? NIST Trustworthy and Responsible AI • Restricting access and sharing PII and PHI? Combination of tokenization and encryption? • Have you built a front end to the Chat GPT interface to mitigate the risk? • Have you built a sandbox to isolate the risk as the gateway to consume LLM services? • Is sensitive data in a company enclave or environment to protect it? • What is the maturity of your training program? • Are you enforcing DLP policies? • Will you be investing in Red Team Services to test the GenAI implementations? • Are you using Digital Signatures?
Threat Intelligence Platforms (TIPs)	TIPS that offer integrated automation and security orchestration (SOAR). TIPS should provide ways to automatically ingest, process, analyze and/or report data so as to improve analyst efficiencies and effectiveness and help reduce risk in an organization.
Application Security Tools	Healthcare management and In-house software development operations have demanded developers to turn out code faster and subsequently this is putting more pressure on AppSec tools to turn around code analysis faster
Antivirus (AV) and Endpoint Detection and Response (EDR)	AV and EDR solutions are not meeting the needs of organizations. AV and EDR systems are being replaced by more modern and comprehensive Extended Detection and Response (XDR) solutions.
Next-Gen Backup and Disaster Recovery	Investment into next-generation backup and disaster recovery products is increasing as the technology is an important part of disaster recovery and ransomware remediation strategies.

Technology Area / Topic	What's Hot
Email Gateway Security	Email gateway security technology solutions are still providing effective anti-spam and malware prevention at scale for the enterprise.
Security Information and Event Management (SIEM)	SIEM solutions are being sold as part of a bundled product package. Individual SIEM offerings are deemed too expensive and singularly focused when purchased as a single product. The bundling could lead to fewer efficiencies and distractions for cybersecurity teams.
Cloud Security Posture Management (CSPM)	Cybersecurity executives have expressed a need for security orchestration capabilities in Cloud Security Posture Management (CSPM) solutions that automate cloud security management, configuration management, and infrastructure management.
Cloud-based (agent-less) vulnerability scanning solutions	Cloud based scanning services (agentless scanning services) provide visibility to assess the total enterprise digital landscape quickly. As organizations move to cloud-based scanning services (agentless scanning service), cybersecurity teams can realize new efficiencies, but must coordinate across all supporting teams to work together in a new orchestrated process.
Application Programming Interface (API) Security	As the deployment of new applications continue to be in high demand by business lines, Application Programming Interface (API) security is becoming increasingly important. Organizations are fielding more complex applications and vulnerabilities emerge that are not simply protected by enterprise firewalls. API Security disciplines and vendor solutions are emerging to address these issues.
Zero Trust SASE / CASB DLP & Cloud Broker	Zero Trust and Secure By Design models offer new perspectives and ways to implement and deploy systems safely and securely. While the philosophies of Zero Trust Secure Access Service Edge (SASE) versus Cloud Access Security Broker (CASB), Data Loss Protection (DLP) and Cloud Brokers, Secure By Design, etc., all offer strategic advantages to security, complexities will be introduced in field implementations, leading to unexpected weaknesses and vulnerabilities. Some questions you should be asking your staff, partners and vendors: Can you get all security services from one vendor? Are there weaknesses in a single vendor approach? What do you do to provide security for infrastructure services in the cloud?
Cyber Asset Attack Surface Management (CAASM)	In enterprise environments with large Operational Technology (OT) implementations, CAASM solutions are being used to provide more reliable asset inventories and visibility to vulnerable systems. CAASM is especially useful in environments where network access control (NAC) cannot be used to isolate end devices.
Data Protection	The role of Data Protection Owner is not well-defined in healthcare organizations and found across multiple teams including Internal Audit, Corporate Legal, CIOs and Cybersecurity. CISOs need to ensure asset management, data security, data availability, and access control responsibilities are clearly assigned. Governance around GenAI will create even more data protection issues as well.

Resources

Health-ISAC would like to thank Mike Schramm, CEO of Cloud Security Solutions, for his guidance and valuable input into the CISO Market Survey. Cloud Security Solutions serves as the eyes and ears of the industry providing Global 500 enterprise clients in the financial services and health care sectors the highest level of scrutiny in identifying and procuring the services of the most innovative cybersecurity startups. More information about CSS can be found *here*.

Conclusion

The 2024 Health-ISAC CISO Exclusive Market Summary paints a vivid picture of the evolving cybersecurity landscape in healthcare due to the rapid changes in technology and ever-increasing threats. While familiar threats like ransomware persist, newer challenges emerge, driven by technological advancements like generative AI and cloud migration.

As we look ahead into 2024, most organizations anticipate flat or slight increases in their cybersecurity budgets. Venture capitalists are slowing down investments which will lead to more consolidation in the cybersecurity startup space. Existing startups will have more pressure to deliver on sales, which could ultimately drive up prices for existing customers. Cybersecurity vendors must focus on delivering on their promise with successful deployments and increasing sales backed by proven, repeatable value.

Health-ISAC encourages CISOs and senior leaders to consider the information presented here – including the dynamic threat landscape and trends in the cybersecurity market – to develop a proactive and strategic approach that works in their environment.

A Call to Action

Protect your patients, elevate your defenses, and empower your team.

In today's interconnected healthcare ecosystem, no organization is alone in facing cyber threats. Information sharing and collaboration through Health-ISAC is the key to building a unified front against cybercrime, protecting sensitive patient data, and ensuring the well-being of those we serve.

By joining and actively participating in your Health-ISAC community, you gain:

- Foresight: Early warnings about emerging threats and proven mitigation strategies from your peers.
- Expertise: Crowdsourced knowledge from industry veterans to strengthen your defenses and elevate your team's skills.
- Resilience: Collaborative trust to navigate evolving threats with confidence and maintain a secure, reliable network.
- Innovation: Shared insights that fuel cutting-edge cybersecurity solutions for a safer future of healthcare.

Take action today:

- Visit the Health-ISAC *website* or contact your Health-ISAC Member Engagement representative to learn more about the community and membership benefits.
- Download Health-ISAC's white paper on Information Sharing Best Practices in healthcare, available *here*.
- Connect with your peers on the Health-ISAC member portal (*https://portal.h-isac.org/*) or Secure Chat (*https://healthisac.slack.com/*) and join the conversation.
- Health-ISAC members can obtain a copy of the expanded version of this report (Current and Emerging Healthcare Cyber Threat Landscape). Please contact Health-ISAC here for the report: *contact@h-isac.org*.

Together, we can build a stronger, more resilient healthcare ecosystem where patient safety is always the top priority. Don't wait for the next attack. Be part of the solution. Share, collaborate, and secure the future of healthcare.

Feedback and suggestions on this document are encouraged and welcome.
Please email *contact@h-isac.org*

Health-ISAC, Inc.
226 North Nova Road, Suite 391
Ormond Beach, Florida 32174

Drève Richelle 161 M Box 57
1410 Waterloo, Belgium

Health-ISAC.org

Health-ISAC's mission is to empower trusted relationships in the global healthcare industry to prevent, detect, and respond to cybersecurity and physical security events so that Members can focus on improving health and saving lives.

Together, we are stronger, better, and more resilient. We invite you to join us.

Memberships are purchased for your organization (not individuals), with unlimited seat licenses. To apply, visit *h-isac.org/h-isac-membership*