

2026 Global Health Sector Threat Landscape

TLP:WHITE This report may be shared without restriction.



Contents

Introduction	1
Annual Member Survey Insights	3
Survey Background.....	3
Survey Findings	4
Key Insights	5
Part I: The Current Threat Landscape	6
Physical Security	6
Physical Security / Violence Legislation – U.S. and Global.....	6
Man-Made and Natural Threats to Security.....	6
Cybercriminal Activity.....	8
Hacktivist Attacks Against the Health Sector.....	8
Data Breaches – Episource	8
Significant Takedowns.....	9
Raccoon0365 Disruption.....	9
Ransomware Gangs Attacking Health Sector	10
Qilin	10
INC Ransomware	10
SAFEPAY	10
Sinobi.....	11
WorldLeaks	11
Ransomware Trends in the Health Sector	12
Emerging and Receding Ransomware Groups	12
Ransomware Insights	12
Nation-State Activity.....	13
DPRK Remote IT Worker Campaigns	13
Geopolitical Activity	14
Israel-Iran War.....	14
Hybrid Warfare.....	14
Medical Device Cybersecurity	14
Contec CMS 8000 Patient Monitor	14
Legacy Devices	15
DICOM/PACS Exposure	15

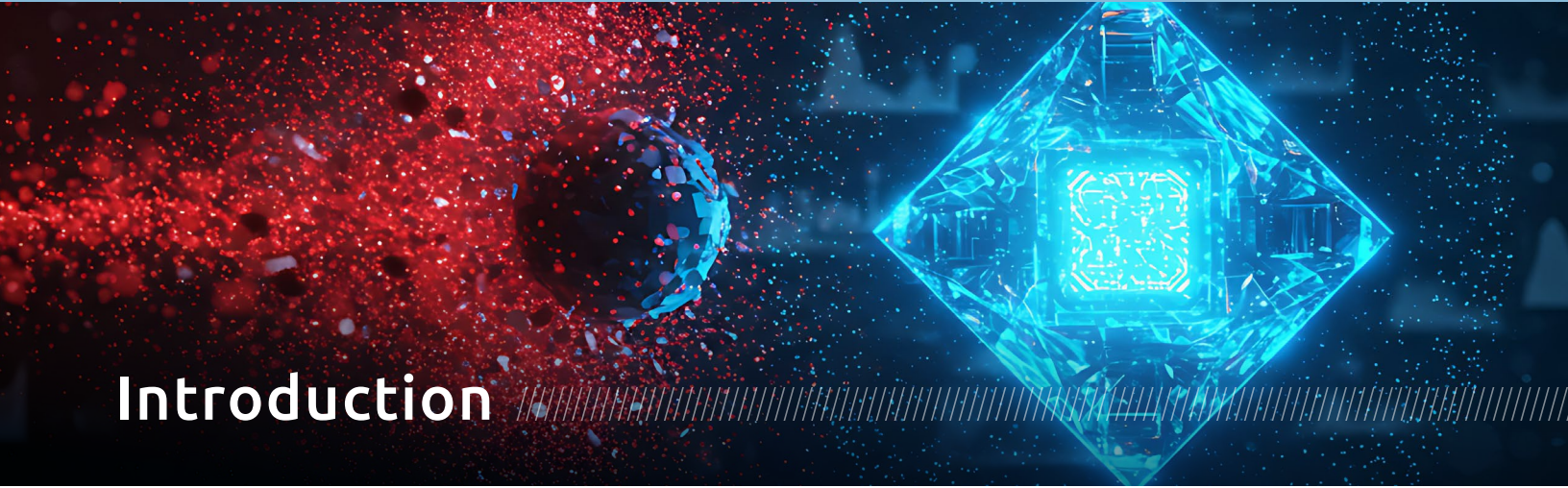
Part II: Tactics, Techniques, and Procedures 16

Social Engineering	16
ClickFix and FileFix.....	16
QR Code Phishing.....	17
Cleo Compromise Victim Bundling	17
Malicious Activity Observed by Members.....	18
XWorm.....	18
NetSupportRAT	18
njRAT.....	18
SocGholish.....	18
AsyncRAT.....	18
Breakdown of 2025 MITRE ATT&CK Data	19
Notable Vulnerabilities	19
Microsoft SharePoint ToolShell	19
Cisco ASA 5500-X Series	19
Popular Targeted Alerts	20
Dangling DNS	20
Citrix Netscaler ADC and Citrix Gateway	20
BeyondTrust	21
CEO Doxxing.....	21
Remote Desktop Protocol Exposures	21

Part III: Future Cybersecurity Outlook 22

Business Resilience	22
Business Resiliency Looking into 2026	23

Conclusion 24



Introduction

2025 was defined by a critical escalation in the volume, complexity, and systemic risk facing the global health ecosystem. As the digital transformation of the health sector—from advanced medical devices to telehealth platforms—continued to accelerate, it expanded the attack surface, confirming that the health industry remains a primary, high-value target for cybercriminals and nation-state actors alike.

The primary threat facing the health sector remains **ransomware**, with prolific groups like Qilin, INC Ransom, and the rapidly growing SAFEPAY dominating the threat landscape. However, the most concerning trend is the continued pivot and acceleration by threat actors to **supply chain exploitation**. Major security incidents throughout the year repeatedly demonstrated that a provider's security is only as strong as its weakest vendor link, leading to widespread compromises that impacted millions of patient records and forced a significant industry-wide reevaluation of third-party risk management.

Attack methodologies also evolved, requiring more advanced defenses. The proliferation of sophisticated social engineering techniques used in malware, such as **ClickFix** and **FileFix**, along with the emergence of **QR code phishing (quishing)**, showcased an increasing reliance on methods that bypass traditional perimeter defenses by exploiting human trust. The evolving attack methodologies were often successfully countered, as demonstrated by the intervention of illegitimate **Cobalt Strike** usage and the successful takedown of the **Raccoon0365** phishing-as-a-service infrastructure.



Compounding these cyber challenges is the unique duality of the health sector: the urgent need to secure life-critical operational technology and the exposure to geopolitical events. The security risks posed by **legacy medical devices**, particularly those approaching end-of-life, demanded immediate compensating controls to protect patient safety. Furthermore, 2025 saw the continued impact of **nation-state cyber activity**, from widespread remote IT worker fraud campaigns to hybrid warfare tactics that leveraged cybercriminal elements against geopolitical adversaries.

As we look toward 2026, the focus must shift from incident response to sustained **Business Resilience**. The lessons learned from massive disruptive events—such as the widespread impact from the faulty **CrowdStrike update** in July 2024 —underscore the necessity for robust planning that goes beyond traditional cybersecurity and addresses operational continuity in the face of widespread third-party failure.

This report is structured to provide an in-depth analysis of these dynamics, offering clear insight into:

- **Part I: The Current Threat Landscape:** A deep dive into the most active cybercriminal groups, significant law enforcement takedowns, nation-state activity, and critical issues in medical device security.
- **Part II: Notable Tactics, Techniques, and Procedures (TTPs):** A breakdown of the most effective initial access and evasion techniques used by adversaries.
- **Part III: Future Cybersecurity Outlook:** Strategic guidance on enhancing business resilience and preparing for the emerging risks of 2026.

By sharing intelligence and adopting a collaborative defense strategy, the health sector can build the collective resilience necessary to protect patients, staff, and critical services in the years ahead.



Annual Member Survey Insights

Survey Background

In November 2025, Health-ISAC conducted a survey of nearly 250 executives and cybersecurity professionals across the health sector. The survey included cyber (e.g., CISO) and non-cyber (e.g., CFO) executives across multiple health subsectors (e.g., providers, pharmaceutical companies, payers, medical device manufacturers, health IT) as well as healthcare organizations of varying sizes and IT/IS budgets.

Survey responses were received from members of:

- Health-ISAC
- The Association for the Advancement of Medical Instrumentation® (AAMI)
- Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG)

Health Security Professionals were asked to rank the five greatest cybersecurity concerns facing their organizations for 2025 and 2026 and Medical Device Manufacturers were also asked the top three challenges in developing secure medical devices for 2025 and 2026.

The detailed survey results are available for members in the Health-ISAC Threat Intelligence Portal (HTIP).

<https://health-isac.cyware.com/webapp/user/doc-library/43dd7f6d-be19-4d26-b235-aa203e4b0a37>



Survey Findings

Health Sector Security Professionals ranked the top five cyber threats facing their organizations in 2025 as follows:

- | | |
|---------------------------------|----------------------|
| 1. Ransomware Deployments | 4. Data Breaches |
| 2. Phishing Attacks | 5. Zero-Day Exploits |
| 3. Third Party/Partner Breaches | |

Health Sector Security Professionals ranked the top five cyber threats facing their organizations, looking ahead toward 2026, as follows:

- | | |
|---------------------------|----------------------------|
| 1. AI-Enabled Attacks | 4. Zero-Day Exploits |
| 2. Ransomware Deployments | 5. Phishing/Spear Phishing |
| 3. Third Party Breaches | |

Medical Device Manufacturers reported the top three challenges in developing secure medical devices such as:

- | |
|---|
| 1. Integrating security into the design and development process |
| 2. Providing regular and secure updating and patching for medical devices |
| 3. Designing for the ongoing security of medical devices over their long operational lifespan |

Conversely, the top three impacts on Healthcare Delivery Organizations were reported as:

- | |
|---|
| 1. Disruption in the normal operation of medical technology |
| 2. Unauthorized access, theft, or exposure of patients' personal health information (PHI) |
| 3. Disruption of overall hospital operations, including administrative processes, scheduling, and communication |



Key Insights

////////////////////////////////////

- The most significant consequences of cyberattacks on patient care were found to be the same in 2025 as those reported in 2024.
- Executives and cybersecurity practitioners reported the same concerns going into 2026, indicating a level of synergy across all levels of health sector cybersecurity.
- Member organizations with smaller cybersecurity budgets were more concerned by phishing in 2025, while those with larger budgets were more concerned by ransomware deployments.



Part I: The Current Threat Landscape

Physical Security

Throughout 2025, the health sector has maintained an increased focus on workplace violence and the safety of staff. Most recent reporting by the Bureau of Labor Statistics in 2023 states that healthcare was the industry where staff had the highest likelihood of experiencing violence in the workplace.¹ This, combined with the assassination of a health insurance executive at the end of 2024, has caused an increased focus on physical security and executive protection measures, driving increased budget allocations to the safety of all employees.

Physical Security / Violence Legislation – U.S. and Global

From a regulatory perspective in the United States, the Save Healthcare Workers Act (H.R. 3178/S.1600) was reintroduced to Congress for a third time on May 5, 2025. The legislation aims to make assault on a healthcare worker a felony offense. Another regulation aimed at increasing healthcare worker safety was The Workplace Violence Prevention for Health Care and Social Service Workers Act (H.R. 2531/S.1232), which was introduced to Congress for the fourth time on April 01, 2025. This act, if passed, would establish a federal standard for preventing workplace violence in healthcare environments. Working outside of the legislative process, health sector organizations have been implementing their own policies and using recommendations from the Occupational Safety and Health Administration to reduce workplace violence.²

Man-Made and Natural Threats to Security

The 2025 wildfire season in North America was marked by multiple major fires. It was the second-worst fire season on record in Canada in terms of total area burned.³

The Atlantic hurricane season saw minimal activity, with fewer storms making landfall compared to recent years. The Pacific typhoon season also saw fewer overall storms, although Super Typhoon Fung-Wong caused severe damage in the Philippines in mid-November.⁴

1 <https://www.bls.gov/iif/factsheets/workplace-violence-2021-2022.htm>

2 <https://www.bls.gov/iif/factsheets/workplace-violence-2021-2022.htm>

3 <https://www.cbc.ca/news/climate/wildfire-season-2025-1.7606371>

4 <https://www.cbsnews.com/news/super-typhoon-fung-wong-philippines/>

There were multiple significant viral outbreaks throughout the year, the largest of which was the resurgence of Chikungunya. According to the World Health Organization, there were potentially 445,271 cases and 155 deaths globally across 40 countries.⁵

The 2025 outbreak of measles in the United States was the largest since 2000. It started in west Texas and quickly spread, with multiple cases appearing around the country.⁶

Avian Influenza has remained a global concern through 2025, as concerns of viral adaptation that makes the disease become human-to-human transmissible continue. The Centers for Disease Control and Prevention reported 70 cases in the United States, with one death. The World Health Organization reported 18 cases with eight deaths across the Western Pacific Region.⁷

The "50501" movement (short for "50 protests, 50 states, 1 movement") has been responsible for national protests on 10 different days across the United States, each growing in attendance and participation. The movement was founded with the intent of resisting perceived anti-democratic politics.⁸ The protests have had a large footprint and drawn in many participants. As they grow, there is an increased potential for disruptions to emergency medical services and business travel. The protests can also disrupt day-to-day operations in the healthcare industry, as they can pull staff and patients away who wish to participate. International activity related to the 50501 movement has manifested as coordinated solidarity demonstrations outside the US, primarily concentrated in Western Europe and key Asian capitals. These protests create localized physical security risks by restricting the freedom of movement around US government facilities, potentially delaying secure logistics and complicating emergency response protocols of personnel in the area.

Many nations have moved to categorize healthcare staff as a "protected class" or have increased penalties specifically for crimes committed against them. Here are several examples Health-ISAC is tracking around the world:

1. United Kingdom — Assaults on Emergency Workers

(Offences) Act 2018: This is perhaps the most direct parallel to the U.S. legislation. This Act doubled the maximum sentence for common assault against "emergency workers" (including NHS staff, paramedics, and police) from six months to 12 months in prison (later increased to two years via the Police, Crime, Sentencing and Courts Act 2022). The Act also created a specific offense of "assaulting an emergency worker," making the profession of the victim an aggravating factor that mandates a tougher sentence.

2. India — Epidemic Diseases (Amendment) Act 2020:

Following a surge in violence against doctors during the COVID-19 pandemic, India enacted significant federal protections. The amendment makes any act of violence against healthcare personnel a cognizable and non-bailable offense. Perpetrators can face imprisonment ranging from three months to five years and heavy fines. In cases of "grievous hurt," the prison term can extend up to seven years. It also mandates that the offender pay twice the market value of any property damaged (such as hospital equipment).

3. Australia — State-Level "Health Worker" Protections:

New South Wales introduced new laws in 2022 making it a specific crime to assault a healthcare worker. Penalties range from 12 months to 14 years in prison, depending on the severity of the harm. Queensland has similar "assaults on public officers" laws that carry increased penalties (up to seven or 14 years) specifically for those who bite, spit on, or assault healthcare staff.

4. France — Loi n° 2021-502: France has implemented specific criminal provisions to protect medical personnel, particularly those in emergency services. The law allows for increased criminal penalties when an assault is committed against a person "performing a public service mission," which explicitly includes hospital and emergency staff.

5. Armenia — 2025 Criminal Code Proposals: As of mid-2025, Armenia is debating a draft law very similar to the current U.S. bill. The Law proposes criminalizing the "obstruction of professional duties" of healthcare workers. If the obstruction involves threats or violence, the prison term can be up to two years.

⁵ <https://www.sciencealert.com/outbreak-of-chikungunya-virus-poses-global-risk-warns-who>

⁶ <https://www.who.int/emergencies/disease-outbreak-news/item/2025-DON561>

⁷ <https://www.cdc.gov/bird-flu/h5-monitoring/index.html>

⁸ <https://www.newsweek.com/50-states-anti-trump-protest-nationwide-50501-explainer-2026115>

Cybercriminal Activity

Hackivist Attacks Against the Health Sector

Hacktivism involves using hacking techniques to promote a political or social cause. Hacktivist groups often leverage Distributed Denial of Service (DDoS) attacks to achieve their goals.

Attackers are increasingly targeting business associates and third-party vendors that provide critical services (like medical billing, software, or IT support) to healthcare providers.

In June 2025, a Hacktivist group operating on Telegram within a channel dubbed ServerKillers orchestrated a temporary disruption of websites associated with Medical Centers in Israel in response to Israel's strikes on Iran.

The ServerKillers team is described as part of the larger Killnet Collective that has targeted health sector organizations in previous years. The Killnet Collective is self-described as including UserSec, Coup Team, DarkStorm Team, ServerKillers, D0rGe1st, and PalachPro.

The pro-Iran hacktivist group Cyber Islamic Resistance also attacked Israeli health sector entities in response to military action against Iran. In July 2025, the group attacked nine Israeli health organizations, including mental health hospitals, emergency rooms, and children's hospitals.^{9 10}

Data Breaches – Episource

Data breaches were identified as the fourth most severe concern for global health sector cybersecurity professionals in 2025.

A ransomware-driven intrusion between January and February 2025 exposed data from over 5.4 million individuals. The data breach originated from a single vendor, Episource, a provider of risk adjustment services, software, and solutions for health plans and provider groups. The breach resulted in a cascading effect that impacted numerous providers and millions of patients.¹¹

A New Era of Digital Warfare: Understanding and Mitigating Modern DDoS and RDoS Attacks

**Health sector security professionals
operate at the front line of service
continuity and patient safety.**

Learn strategic and
tactical
recommendations
your organization
can implement
today to limit severe
business
interruption.



Distributed Denial-of-Service (DDoS) attacks have increased in magnitude as more devices come online and organizations increase remote access for their staff. In September 2025, Health-ISAC published a white paper that covers the motivations behind DDoS attacks, provides several historical examples and details several strategic and tactical recommendations IT and information security professionals can use to limit impacts from these disruptive attacks.

Link: <https://health-isac.org/a-new-era-of-digital-warfare-understanding-and-mitigating-modern-ddos-and-rdos-attacks/>

⁹ <https://twitter.com/FalconFeedsio/status/1947009260543791524>

¹⁰ <https://twitter.com/FalconFeedsio/status/1946905848795546105>

¹¹ <https://www.hipaajournal.com/episource-data-breach/>

Significant Takedowns

Cybercriminal Cobalt Strike Usage Down 80%

Cobalt Strike is a legitimate penetration testing framework used by red team operators to emulate adversaries. It offers command and control capabilities that allow red team operators to emulate cybercriminals and nation-state threat actors. However, its capabilities drew interest from cybercriminals, and illegitimate instances of the Cobalt Strike framework were used in countless cyber attacks on the global health sector. In 2023, Fortra, Health-ISAC, and Microsoft led an effort to identify and disrupt instances of Cobalt Strike being abused by threat actors.

In the first quarter of 2025, Fortra announced abuse by threat actors had dropped by 80%, thanks largely to the joint Cobalt Strike disruption effort started in 2023. The blog went on to state that new instances of Cobalt Strike operated by threat actors are being detected faster and usually taken down within one or two weeks.¹²



80%
Reduction

In the first quarter of 2025, Fortra announced abuse by threat actors had dropped by 80%.

Raccoon0365 Disruption

Raccoon0365 is a phishing-as-a-service kit used in cyberattacks to steal user credentials (usernames and passwords) plus one-time login tokens, specifically targeting Microsoft Office 365 accounts through a sophisticated phishing kit. After its launch in July 2024, the kit quickly became the fastest-growing tool used by cybercriminals to victimize thousands of organizations globally.

While Raccoon0365 services are used to target all industries, its phishing kits have been used to target more than 25 health sector organizations.¹³ As phishing emails are often a precursor to the installation of malware and ransomware, usage of the Raccoon0365 phishing kits could have severe consequences for hospitals and put patient safety at risk. When hospitals get hit by ransomware, patient services are delayed, critical care is postponed or canceled, lab results are compromised, and sensitive data is breached, causing major financial losses and disruptions that directly impact patients' lives.

Starting in 2024, Microsoft's Digital Crimes Unit (DCU) collaborated with Health-ISAC to take down the Raccoon0365 phishing service. The partnership led to a civil lawsuit and a court order granted in September 2025 by the Southern District of New York that allowed Microsoft to seize the criminal infrastructure used by the attackers. The DCU seized 338 websites associated with Raccoon0365, disrupting the operation's technical infrastructure and cutting off criminals' access to victims.

The naming of a specific defendant and the referral of this case to law enforcement in September 2025, plus the subsequent arrest of the Raccoon0365 operator and two of his accomplices, sends a strong message that cybercriminals cannot operate with impunity.

This joint effort is considered a significant win for the health sector. It demonstrates the importance of collaboration and threat intelligence sharing when protecting sensitive data and essential health services.

This example shows that cybercriminals do not need sophisticated IT skills to cause widespread harm. Tools like Raccoon0365 make cybercrime accessible to virtually anyone, putting patients at risk.

¹² <https://www.cobaltstrike.com/blog/update-stopping-cybercriminsignificantls-from-abusing-cobalt-strike>

¹³ <https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/>



Ransomware Gangs Attacking Health Sector

The threat actor profiles listed below correspond to the five most active ransomware gangs Health-ISAC observed globally with the highest number of health sector victims for calendar year 2025. In total, Health-ISAC tracked 455 ransomware events across the health sector.

More threat actor profiles are available on the Health-ISAC Threat Intelligence Portal (HTIP) under the “Knowledge Base.” Threat actor profiles are actively updated and maintained by Health-ISAC analysts, ensuring members get the most relevant information possible.

Most Active Ransomware Gangs	Number of Health Sector Entities Attacked
Qilin	77
INC Ransom	50
SAFEPAY	23
Sinobi	21
World Leaks	18

Qilin

The Russian-speaking ransomware-as-a-service (RaaS) group Qilin has been active since 2022¹⁴ and has been steadily gaining steam as a renowned ransomware threat. Its activity against the health sector soared in 2025. The group had nearly triple the number of health sector victims in 2025 than it had in 2024 (23 victims in 2024 vs 77 in 2025); Qilin has been named as the group attacking the health sector the most since Lockbit was disrupted by international law enforcement at the beginning of 2024.



INC Ransomware

INC Ransomware, an RaaS operator, has been active since 2023. It uses vulnerability exploitation, supply chain compromise and social engineering to gain access to target networks¹⁵ and has posed a significant threat to the health sector in both 2024 and 2025. In 2024, the group was named the second most disruptive group to the health sector. Despite having the same ranking in 2024, the total victim count in 2025 increased by 11, indicating that the group may be growing.



SAFEPAY

SAFEPAY is a relatively new ransomware group. Unlike the two RaaS groups named previously, SAFEPAY operates as a single sophisticated cybercriminal outfit. The group is known to use social engineering and stolen credentials to gain access to target networks.¹⁶ Its first activity was observed in September 2024. Since then, its attacks on the health sector grew from just 3 victims in 2024 to 21 victims in 2025, making the third most disruptive ransomware group targeting the health sector, and the group with the sharpest year-over-year percentage increase in victim count, increasing over sixfold from 2024 to 2025.



14 <https://analyst1.com/threat-actors/qilin-threat-actor-profile/>
15 <https://blackpointcyber.com/threat-profile/inc-ransom-ransomware/>
16 <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/>

Sinobi

Sinobi is also a new actor. First observed in the summer of 2025, Sinobi has aggressively targeted the health sector for the past six months. The group uses stolen credentials and exploits public-facing applications.¹⁷ In the second half of 2025 alone, Sinobi had 21 victims; they appear to be operating as an RaaS platform, creating the infrastructure and tooling that affiliates use during their attacks. In the absence of significant law enforcement action, Sinobi's RaaS affiliates are likely to keep aggressively targeting the health sector.

21

Attacks on Health
Sector Entities

WorldLeaks

WorldLeaks is suspected to be a rebrand of the group Hunters International, emerging just two months after the announcement that Hunters International was shutting down due to fear of law enforcement action. Notably, WorldLeaks has adopted a single extortion strategy, prioritizing data theft rather than encryption. The group then uses the threat of publication to coerce victims to pay a ransom.¹⁸ WorldLeaks was first observed in 2025, making it the second group on this list that is less than a year old. In the short time the group has been active, it has accrued 18 health sector victims, making it the fifth most disruptive ransomware threat to the health sector, as tracked by Health-ISAC in 2025.

18

Attacks on Health
Sector Entities



17 <https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-sinobi>

18 <https://sosransomware.com/en/ransomware-groups/worldleaks-the-healthcare-sector-the-most-suggesting-they-may-be-scaling-back-between-pure-extortion-and-traditional-ransomware-whats-the-difference/>

Ransomware Trends in the Health Sector

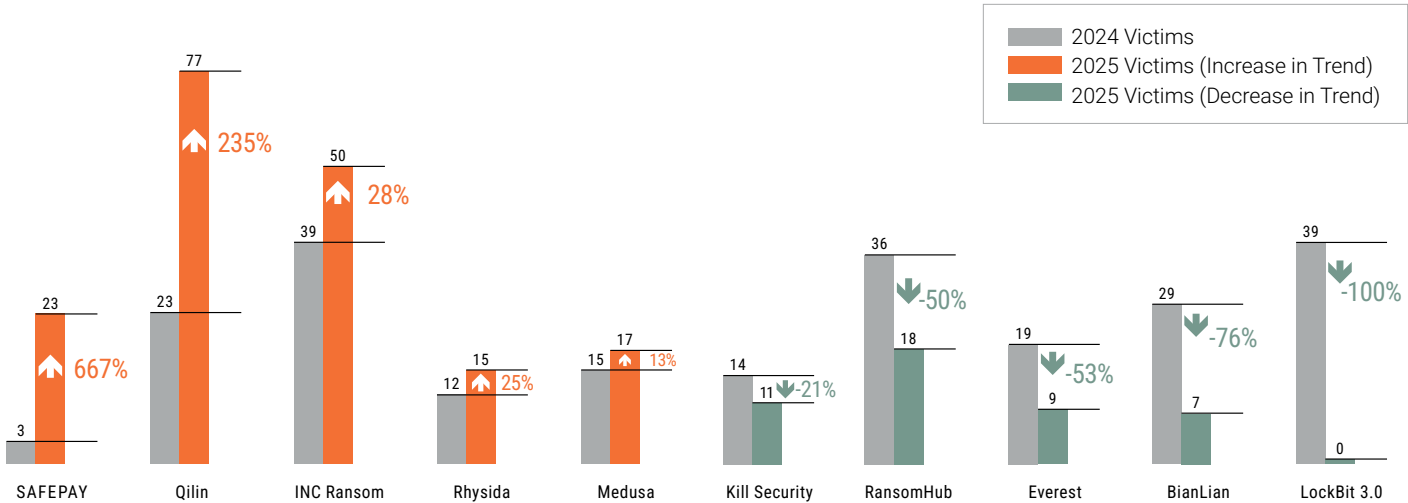
Health-ISAC has been compiling ransomware incident data across all sectors globally since 2020. Health-ISAC derived the following insights when examining the changes in the health sector ransomware landscape from 2024 to 2025.

Emerging and Receding Ransomware Groups:

Following is a list of the top 10 ransomware groups by victim count over the past two years, organized to identify which groups have experienced the largest percentage change in victim count from 2024 to 2025. The chart illustrates which groups are strengthening their operations and which are slowing down. This list excludes ransomware groups that first emerged in 2025.

SAFEPAY, Qilin, and INC Ransomware have the highest percentage increase in victim count year-over-year, suggesting they may be expanding operations against the health sector. Conversely, Everest, BianLian, and Lockbit have reduced their health sector victim count, suggesting they may be scaling back operations against health sector organizations moving forward.

Ransomware Actor Activity Comparison (2024 vs. 2025)



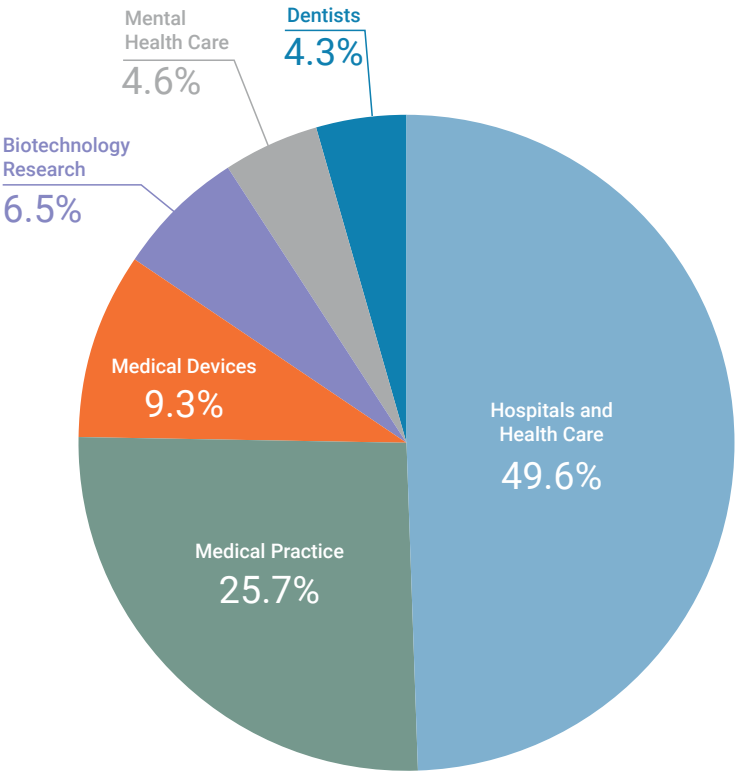
Ransomware Insights:

- **SAFEPAY** has the highest percentage increase from 2024 to 2025, suggesting the group has massively increased its operations against the health sector in the last year. If this trend continues, SAFEPAY may become a significant threat in 2026.
- **LockBit** was the top group attacking the health sector in 2022, 2023, and 2024, but no incidents were observed in 2025. This suggests that the gang’s operations were severely damaged following the law enforcement action taken against them in 2024.
- **WorldLeaks** emerged in 2025 Q2 and has accrued 18 victims in that short time frame. If they maintain aggressiveness toward the sector, they could evolve into a serious threat in 2026.
- **Sinobi** is a ransomware group that has shown the most aggressive targeting of the health sector in 2025. First observed attacking the sector in 2025 Q3, the group has accrued a victim count of 2117 in just two fiscal quarters. If this trend continues, Sinobi will be a persistent threat as we enter 2026.



Health Sector Victimology

The following chart represents categories of the health sector impacted by ransomware in 2025:



Nation-State Activity

DPRK Remote IT Worker Campaigns

North Korea has waged a concerted nation-state run operation to secure remote IT jobs to generate revenue for its national weapons development programs. First uncovered at the tail end of 2024, this campaign has continued into 2025. New research from Okta suggests that this campaign is expanding outside of the US and increasing in scope.¹⁹

The Health-ISAC Threat Intelligence Committee (TIC), comprised of security professionals across the health sector who share threat intelligence through Health-ISAC, continually reported in 2025 that this activity has been an ongoing problem for nearly every organization, with fake remote IT workers unfortunately being hired by various firms. The North Korean campaign has been a persistent topic discussed at the TIC's Monthly Threat meetings and among members of the Health-ISAC CISO Council as well. Member organizations strive to identify fraudulent remote workers during the recruiting and hiring process. Organizations are also taking steps to improve insider threat programs to identify fraudulent remote workers who are already on the payroll.

¹⁹ <https://www.okta.com/newsroom/articles/north-korea-s-it-workers-expand-beyond-us-big-tech/>



Geopolitical Activity

Israel-Iran War

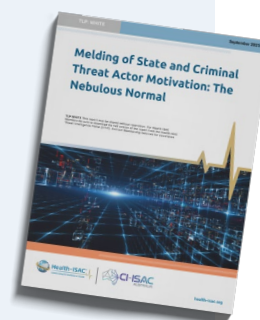
On June 13, 2025, Israel launched Operation Rising Lion, a strategic military operation meant to degrade Iran's nuclear capabilities. These strikes kicked off a 12-day war between the two countries. During this war, various hacktivist groups began targeting the health sector in Israel as part of a larger campaign to target Israeli critical infrastructure. Some groups were reportedly using leaked ransomware payloads to launch one-way ransomware attacks—a ransomware attack where the attacker never planned to decrypt the data, instead using malware to make the data unusable and destroy it.²⁰

Hybrid Warfare

In 2025, Health-ISAC and CI-ISAC (Australia) launched an inquiry into tactics used by nation-state threat actors to launch hybrid warfare attacks. Hybrid tactics, named after the term hybrid warfare, fall just short of kinetic warfare and often incorporate gray zone tactics to obscure nation-state involvement. An example of this is the direct or indirect empowering of regional cybercriminal elements to attack geopolitical enemies. In September 2025, Health-ISAC and CI-ISAC released a joint publication titled *Melding of State and Criminal Threat Actor Motivation: The Nebulous Normal Whitepaper*, which examined the collaboration between nation-state intelligence agencies and cybercriminal elements.²¹

Melding of State and Criminal Threat Actor Motivation: The Nebulous Normal

Link: <https://health-isac.org/melding-of-state-and-criminal-threat-actor-motivation-the-nebulous-normal-whitepaper/>



Medical Device Cybersecurity

Contec CMS 8000 Patient Monitor

On January 30, 2025, CISA issued advisory ICSMA-25-030-01, warning of severe vulnerabilities in Contec CMS8000 patient monitors, including out-of-bounds write, hard-coded backdoor access, and privacy leakage. The FDA released a concurrent safety alert, noting that these monitors, including relabeled versions such as the Epsimed MN-120, can be remotely controlled by unauthorized users, risking patient data and device function.

Claroty's Team82 attributed the presence of the hard-coded IP address in the Contec CMS8000 Patient Monitor, 202.114.4.[.]119, to insecure design, not malicious intent. This IP address appears in manuals from multiple manufacturers, including Drager, Mindray, Edan, and Epsimed, suggesting shared design origins. Cylera linked the IP address to Tsinghua University in Beijing, China.^{22 23}

Originally introduced around 2005 and approved in 2011, the CMS8000 is not a life-sustaining device, but it plays a vital role in monitoring high-risk patients, especially in intensive care units (ICUs) and critical care units (CCUs). The FDA recommends two actions to secure the device. First, discontinue use of remote monitoring services, and block the 202.114.4.0/24 IP address range. Health-ISAC recommends healthcare providers review central monitor configurations, segment networks containing medical devices, apply firmware updates where possible, and conduct device security assessments.

20 <https://dailydarkweb.net/aptiran-allegedly-hits-israeli-critical-infrastructure-with-ransomware/>

21 <https://health-isac.org/melding-of-state-and-criminal-threat-actor-motivation-the-nebulous-normal-whitepaper/>

22 <https://claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated>

23 <https://cylera.com/blog/contec-patient-vital-signs-monitor-chinehat-that-se-backdoor-bad-design/>

Legacy Devices

Legacy medical devices, which include healthcare products like infusion pumps or imaging machines, now pose a critical and immediate threat to patient safety, healthcare operations, and even national security. Many devices remain in use for decades due to high replacement costs and their continued necessity for patient care. On April 1, 2025, the United States House Energy & Commerce Oversight & Investigations Subcommittee highlighted the issue of legacy devices during a hearing titled "Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices." It also highlighted the regulatory gap that existing legacy devices are not subject to the same cybersecurity requirements as newer devices.²⁴

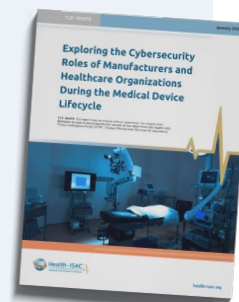
Devices often outlast the service life of their operating systems, allowing for the increased likelihood of unpatched vulnerabilities once software support ends. Since Windows 10 reached end-of-life on October 14, 2025, many devices running the operating system will require support through compensating controls.

Healthcare delivery organizations (HDOs) will need to identify devices still operating after Windows end-of-life and develop a strategic replacement or upgrade plan for these systems. While device upgrades are often costly and not feasible due to their role in providing critical care, facilities should implement compensating controls. This includes network segmentation and monitoring, as well as preparing to transition to modular medical devices that are not dependent on a specific, fixed operating system.

On February 4, 2025, Health-ISAC released the whitepaper, *Exploring the Cybersecurity Roles of Manufacturers and Healthcare Organizations During the Medical Lifecycle*, which details the shared responsibilities between HDOs and medical device manufacturers in end-of-support and end-of-life.²⁵

Exploring the Cybersecurity Roles of Manufacturers and Healthcare Organizations During the Medical Lifecycle

Link: <https://health-isac.org/exploring-the-cybersecurity-roles-of-manufacturers-and-healthcare-organizations-during-the-medical-device-lifecycle/>



DICOM/PACS Exposure

Vulnerabilities in DICOM (Digital Imaging and Communications in Medicine) and PACS (Picture Archiving and Communication Systems) represent a growing threat. These technologies are now used beyond radiology, and are now commonplace in dental, ophthalmic, and pathology workflows, broadening the attack surface. Of the 45 Health-ISAC medical device advisories issued in 2025, 19 specifically addressed DICOM/PACS vulnerabilities.²⁶

Smaller clinics and private practices are particularly vulnerable, often lacking dedicated cybersecurity staff to properly firewall and secure their systems against internet exposure. On October 23, 2025, Health-ISAC released a PACS Tip Sheet, which offers recommendations applicable to any internet-facing DICOM/PACS technology.²⁷

²⁴ <https://www.congress.gov/event/119th-congress/house-event/118077>

²⁵ <https://health-isac.org/exploring-the-cybersecurity-roles-of-manufacturers-and-healthcare-organizations-during-the-medical-device-lifecycle/>

²⁶ <https://www.dreamsoft4u.com/blog/what-is-the-difference-between-dicom-and-pacs>

²⁷ https://www.linkedin.com/posts/phil-englert-2642724_health-isac-protecting-pacs-tip-sheet-activity-7385033795650928640-gLlx



Part II: Tactics, Techniques, and Procedures

Social Engineering

ClickFix and FileFix

The ClickFix and FileFix malicious actor campaigns represent a new generation of advanced social engineering tactics that successfully exploit user trust and bypass traditional security defenses. Both methods rely on deceiving users into executing malicious commands by imitating technical issues, such as CAPTCHA errors or system updates.

ClickFix, first seen in 2024, uses phishing emails, malvertising, and SEO poisoning to redirect users to fake error pages. The core deception involves tricking users into copying and pasting malicious code directly into their system, a technique successfully leveraged by groups like APT28 and MuddyWater to deploy potent malware, including SMOKE SABER, Lumma Stealer, and ransomware. These attacks have specifically targeted the health sector, using fraudulent update notifications to steal credentials and gain unauthorized access to target systems.

FileFix, a variant that emerged in 2025, maintains the same goal but uses a slightly different, more evasive approach. It utilizes multilingual phishing sites and anti-analysis techniques to evade detection. Instead of copy-pasting, FileFix exploits a browser's legitimate file upload feature to trick users into executing commands via the File Explorer's address bar. This method has been used to deliver StealC malware, often abusing trusted platforms like Bitbucket to complicate detection further.²⁸

Given the growing sophistication of these threats, organizations must prioritize phishing awareness training, implement robust email and web filtering, and deploy endpoint detection solutions.

²⁸ <https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/>



QR Code Phishing

QR phishing, or “quishing,” is an emerging threat where threat actors embed malicious URLs in QR codes to steal credentials or deliver malware. After scanning a malicious QR code, users are often directed to fake login pages or prompted to harmful files.

In the health sector, these campaigns exploit the assumed trust of QR codes inherited from the widespread use in patient services, such as health sector applications or lab results. When these attacks are successful, they can be particularly impactful because the majority of the interaction occurs on a personal mobile device when a user scans the QR code using a mobile device camera. Personal devices often lack robust endpoint security when compared to enterprise-managed devices. These attacks can lead to unauthorized access to sensitive systems, patient data breaches, and even ransomware deployments.

To mitigate this risk, healthcare organizations should educate staff on the dangers of scanning unknown QR codes, implement mobile device management (MDM) solutions, and use security tools capable of analyzing QR code content before access. Sharing intelligence through platforms like Health-ISAC can also strengthen defenses against these evolving threats.

Cleo Compromise Victim Bundling

The health sector's cybersecurity landscape in 2025 was characterized by an escalating level of attack sophistication, combined with systemic challenges inherent to the industry's rapid digital transformation. Ransomware attacks remained the most damaging and common threat, often resulting in significant compromises of patient data and operational disruptions to patient care. This persistent threat forced a significant regulatory and defensive shift across the industry.

In 2025, criminals shifted their focus to health sector businesses and third-party vendors, who handle everything from medical billing to managed file transfers. Such entities often represent a less-defended gateway to multiple large health sector providers.

The Cleo compromise is one such example. A major cyberattack campaign by the ClOp ransomware group in late 2024 and early 2025 exploited vulnerabilities in the Cleo Managed File Transfer (MFT) software. The ClOp group—known for large-scale, automated attacks—was able to compromise hundreds of organizations quickly by leveraging a single, widespread vulnerability in Cleo's platform. The threat group essentially bundled many victims into one mass extortion campaign by exploiting a common piece of software used by their victims.

Attacks by groups like ClOp, INC Ransomware, and Qilin were responsible for compromising millions of patient records.

This focus on the supply chain highlights that a provider's security is only as strong as its weakest vendor link, making Third-Party Risk Management a critical and costly priority.

Malicious Activity Observed by Members

Top 5 Malicious Observations Shared by the Health-ISAC Membership

Attribution
XWorm
NetSupportRAT
njRAT
SocGholish
AsyncRAT

XWorm

XWorm is a remote access trojan (RAT) that is designed to harvest information from target systems. It is sold as commodity malware under a malware-as-a-service cybercriminal model. Upon installation, the malware begins to harvest sensitive data. The malware can exfiltrate local files and hijack social media accounts.²⁹

NetSupportRAT

NetSupportRAT is malware packaged to look like the legitimate remote management tool NetSupport Manager. Unlike the legitimate version, NetSupportRAT operates in stealth mode, providing threat actors access to data on the victim’s machine without them knowing.³⁰

njRAT

njRAT is used to remotely control target computers. Written in the .NET framework, the malware has been around since 2013. It has the capability to turn on webcams, harvest credentials, and steal cryptocurrency. Due to its long tenure in the cyber underground, there is an abundance of tutorials and documentation on how to use njRAT available on popular social media sites, making njRAT especially appealing to less experienced cybercriminals.³¹

SocGholish

SocGholish is a malware loader that is primarily used for initial access by threat actors. It is usually served through drive-by compromise and most commonly observed masquerading as fake software updates. The malware was first observed in 2017.³²

AsyncRAT

AsyncRAT stands for Asynchronous Remote Access Trojan and is a malware family that is used to target Windows systems. Once present on a system, AsyncRAT can broker connections with external command and control (C2) servers and conduct a variety of actions on the host machine, including credential theft and loading additional malware.³³

29 <https://any.run/malware-trends/xworm/>
30 <https://any.run/malware-trends/netsupport/>
31 <https://any.run/malware-trends/njrat/>
32 <https://attack.mitre.org/software/S1124/>
33 <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/asyncrat-malware-explained/>



Breakdown of 2025 MITRE ATT&CK Data

Top 5 MITRE ATT&CK Techniques Observed By Members

MITRE Code	MITRE ATT&CK Technique
T1059.001	Command and Scripting Interpreter: PowerShell
T1189	Drive-by Compromise
T1204.004	User Execution — Malicious Copy & Paste
T1566.002	Spearphishing Link
T1219	Remote Access Tools

Notable Vulnerabilities

Microsoft SharePoint ToolShell (CVE-2025-53770)

On July 19, 2025, Microsoft disclosed a Remote Code Execution (RCE) vulnerability tracked as CVE-2025-53770 affecting on-premises Microsoft SharePoint Servers. This vulnerability, tracked by some as ToolShell, allows unauthenticated attackers to execute arbitrary code. The vulnerability had a CVSS score of 9.8. At the time of the disclosure, threat actors were already exploiting the flaw as a zero-day, resulting in the compromise of hundreds of systems globally.

Once ToolShell was exploited, threat actors could begin data exfiltration and the deployment of persistent backdoors. Microsoft has observed active exploitation by three distinct groups linked to the Chinese government: Linen Typhoon, Violet Typhoon, and Strom-2603.

Cisco ASA 5500-X Series (Adaptive Security Appliance) (CVE-2025-53770)

On September 29, 2025, Health-ISAC received information that the recently reported critical vulnerabilities affecting Cisco ASA 5500-X Series devices were under active exploitation by malicious actors.

Cisco ASA and FTD devices are typically deployed at the network perimeter—the crucial boundary between a healthcare organization's internal network and the public internet. They function as firewalls and, most importantly, VPN gateways used for remote access.

By compromising the ASA, the attacker can gain access to a victim's internal network. The ASA/FTD device is then no longer a defense; it becomes the attacker's launchpad.

These vulnerabilities can be exploited by remote unauthenticated attackers with low privileges for Cisco ASA and FTD to execute arbitrary code or gain unauthorized access to restricted endpoints.

Health-ISAC published an advisory with additional details and recommended countermeasures.³⁴

³⁴ <https://health-isac.cyware.com/webapp/user/myfeeds/671361ad>



Popular Targeted Alerts

Health-ISAC sends “Targeted Alerts” to warn specific organizations of high risks specific to their network—including things like vulnerable servers, cybercriminals selling access to their networks, stolen intellectual property, and compromised credentials. In 2025, Health-ISAC’s Threat Operations Center shared more than 1,200 Targeted Alerts to health sector organizations, including both Health-ISAC members and non-members.

The top five vulnerabilities by targeted alert volume are as follows:

Vulnerabilities & Exposures	Targeted Alerts Distributed
Dangling DNS	407
Citrix NetScaler (CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424)	98
BeyondTrust (CVE-2024-12686, CVE-2024-12356)	77
CEO Doxxing	54
RDP	41

Dangling DNS

On June 9, 2025, Health-ISAC learned from our threat intelligence partner, BlueVoyant, that numerous member organizations were susceptible to Dangling DNS vulnerabilities. Dangling DNS records are legitimate DNS records that are no longer being used by the organization. When these records are not removed, it can lead to a significant cybersecurity risk.³⁵

Health-ISAC sent out a series of Targeted Alerts to impacted organizations, distributing 407 Targeted Alerts.

Citrix Netscaler ADC and Citrix Gateway (CVE-2025-7775, CVE-2025-7776, CVE-2025-8424)

On August 26, 2025, Citrix released a security bulletin to address three critical vulnerabilities in its NetScaler ADC and NetScaler Gateway products: CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424.

The most severe, CVE-2025-7775, was an actively exploited memory overflow vulnerability that can lead to remote code execution (RCE) and/or denial-of-service (DoS) attacks. The other two vulnerabilities allow for DoS and improper access control. Citrix strongly recommends that all users with affected appliances update to the recommended versions immediately to mitigate these risks.

Health-ISAC delivered 98 Targeted Alerts related to infrastructure potentially running vulnerable instances of Citrix for investigation and remediation.

³⁵ <https://www.paloaltonetworks.com/cyberpedia/what-is-a-dangling-dns>

BeyondTrust (CVE-2024-12686, CVE-2024-12356)

Two vulnerabilities in the BeyondTrust Remote Support product were exploited in December 2024, resulting in a breach of the platform that exposed sensitive customer data. Health-ISAC received a list of organizations in the health sector that were impacted by this breach and promptly took action, sending Targeted Alerts to each member.³⁶

Health-ISAC distributed 77 Targeted Alerts relating to these Beyond Trust vulnerabilities in 2025.

CEO Doxxing

On May 29, 2025, Health-ISAC issued a TLP:AMBER alert regarding a website that contained a list of executives from health sector organizations. The website was created in April 2025, with a name that is in reference to Luigi Mangione, the individual accused of shooting the UnitedHealthcare CEO. The website, `hxxps://play[.]luigiwasright[.]com`, contained details of over 1,000 company CEOs and executives, publicly available business information, possible personal or work mobile numbers, and LinkedIn accounts.³⁷

The webpage had an "About" section that stated the provided information was shared with the intent of giving individuals the power to contact those in power at the organizations, rather than speaking to a customer service representative. Although the intent may be to provide individuals with the ability to hold corporate leadership accountable, with the rise in negative public sentiment against health and insurance firms, there were physical security concerns related to the data being in one location and under the "Luigi Mangione" moniker.

This list does not likely pose a significant physical threat to the listed executives; however, it could result in a potential threat actor using the LinkedIn accounts and other sensitive information to target executives.

Additionally, while the information provided may not pose an immediate physical threat, the URL referencing Luigi Mangione implies support of physical violence against corporate leadership. The Alert was issued with the intent that organizations should ensure they are preparing executives who may be targeted, with remedial training on social engineering and recognizing vishing, phishing, and smishing.

Over 400 Targeted Alerts were sent out to health sector organizations that had executive leadership listed on the website. At the time when the alert was published, the `luigiwasright` website was no longer active.

Remote Desktop Protocol Exposures

Remote Desktop Protocol (RDP) is a popular service used for remotely accessing and controlling computers over the internet. The use of RDP poses a severe security risk to any health sector organization, as threat actors continuously scan the internet, looking for easy entry points.³⁸ Unsecured RDP connections are the primary initial access vector for a substantial portion of ransomware attacks.

Once RDP access is gained, the attacker gains the ability to remotely control a device as if they were physically sitting at the keyboard. This high-level access could allow them to steal vast amounts of protected health information (PHI) for extortion, deploy ransomware to encrypt critical electronic health records (EHRs), and move laterally to other systems.

Health-ISAC distributed 41 Targeted Alerts relating to exposed RDP services.

³⁶ <https://www.beyondtrust.com/trust-center/security-advisories/bt24-11>

³⁷ <https://www.securitymagazine.com/articles/101670-luigi-was-right-a-look-at-the-website-sharing-data-on-more-than-1-000-executives>

³⁸ <https://cybersecuritynews.com/microsoft-remote-desktop-protocol-services/>

Part III: Future Cybersecurity Outlook

Business Resilience

CrowdStrike Faulty Update and Supply Chain Risk

The CrowdStrike Faulty Update incident in July 2024 highlighted a significant supply chain risk within every critical infrastructure sector, including health. Previous research indicates that 750 US hospitals faced measurable disruptions, with over 20% of outages affecting patient care, while the estimated direct losses to the industry reached \$1.94 billion. These figures underscore the urgent need to invest in resilience strategies for the health sector.

In October 2025, Health-ISAC conducted a survey to gather additional insights from the 2024 CrowdStrike incident. Some of the key findings include:

- Approximately 69% of respondents indicated that their organization was affected by the CrowdStrike outage.
- Among the impacted services, electronic health records were the most affected, with 80% reporting issues, followed by patient-reported outcomes, such as drug development and direct patient care at 70%, as well as direct-to-consumer telehealth at 60%, and online portals and mobile applications, each at 40%.
- Most respondents noted that the disruptions lasted longer than one day, with 64% experiencing extended impacts. 9% reported that the disruptions lasted three days or longer.
- In response to the incident, 73% indicated they have reassessed their business resiliency strategy. For those who revisited their strategy, the components reviewed included recovery strategies (91%), the frequency of drills, simulations, and/or tabletop exercises (45%), supply chain management (36%), and data backup policies (18%).
- Currently, 60% of respondents express some degree of confidence in their organization's ability to maintain operations in the event of a similar incident. Meanwhile, 27% reported feeling not at all confident, while another 13% stated they are strongly confident.

The detailed survey results are available for members in the Health-ISAC Threat Intelligence Portal (HTIP).³⁹

39 <https://health-isac.cyware.com/webapp/user/myfeeds/f2235d14>



Business Resiliency Looking into 2026

Threats for the health sector in 2026 are expected to include supply chain challenges, financial pressures, and the governance risks of artificial intelligence (AI) and new technologies, among many others.

The rapid deployment of AI and digital health technologies will continue to introduce new risks. Concerns in 2026 are expected to escalate around algorithmic bias, potential misdiagnoses, and the reliability of AI-driven equipment. Without AI being properly governed and validated, there are potential patient safety and liability risks.

These threats, plus the post incident fallout from events like the faulty CrowdStrike update and the Change Healthcare incident from February 2024, will require ongoing strategic adaptation and robust resilience planning from health sector leaders. As technologies continue to evolve at a rapid rate, health sector leaders are encouraged to examine the potential risks of implementing advanced technology into internal workflows.

Additionally, we encourage readers to review the Health Industry Cybersecurity – Sector Mapping and Risk Toolkit (SMART) published by the Health Sector Coordinating Council Cybersecurity Working Group. The SMART Toolkit provides templates and a methodology to visualize, identify and measure systemic risk posed by third party technology, software and communications services essential to clinical, administrative and manufacturing workflows. The resource is intended for cybersecurity, supply chain, risk, operational and administrative executives across the health industry.⁴⁰

⁴⁰ <https://healthsectorcouncil.org/smart-toolkit/>



Conclusion

A Call to Action

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

In today's interconnected health sector, 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 the 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.

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.
- For technical guidance, please view Health and Human Services (HHS) and the Health Sector Coordinating Council's (HSCC) joint publication: [405\(d\) Health Industry Cybersecurity Practices \(HICP\)](#)
- 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 or Secure Chat and join the conversation.
- If you are unaware of these resources, please contact Health-ISAC Member Engagement, who will help you get access.

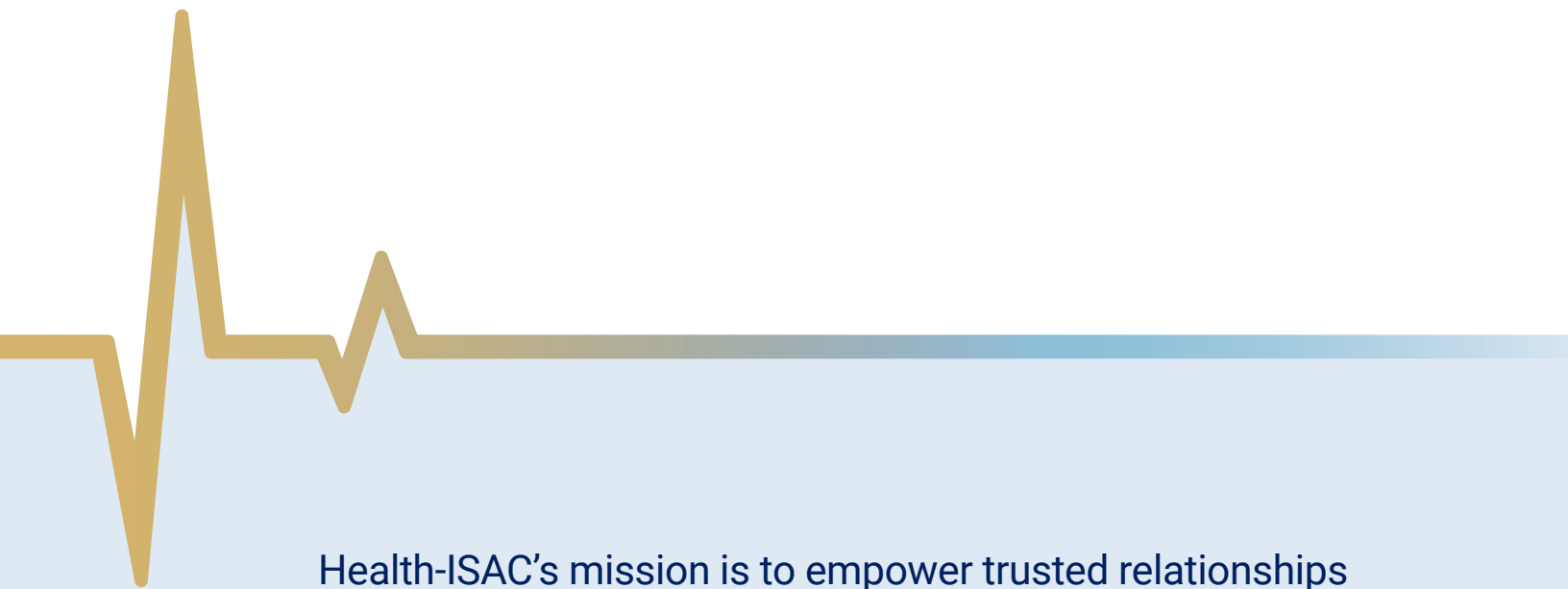
Together, we can build a stronger, more resilient health ecosystem where patient safety is always the top priority. Don't wait for the next attack. Be part of the solution. Share, collaborate, and secure the future of health sector.

If you have any comments or questions about this report, please reach out to Health-ISAC at contact@h-isac.org



Health-ISAC®
Collaborating for Resilience in Health

Health-ISAC, Inc.
12249 Science Drive, Suite 370
Orlando, FL 32826
Drève Richelle 161 M Box 57
1410 Waterloo, Belgium
Health-ISAC.org



Health-ISAC's mission is to empower trusted relationships in the global Health Sector 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 schedule a membership overview, visit <https://health-isac.org/join-h-isac/>