Electronic Medical Records Still a Top Target for Cyber Threat Actors

April 6, 2023

TLP:CLEAR, ID# *202304061300*

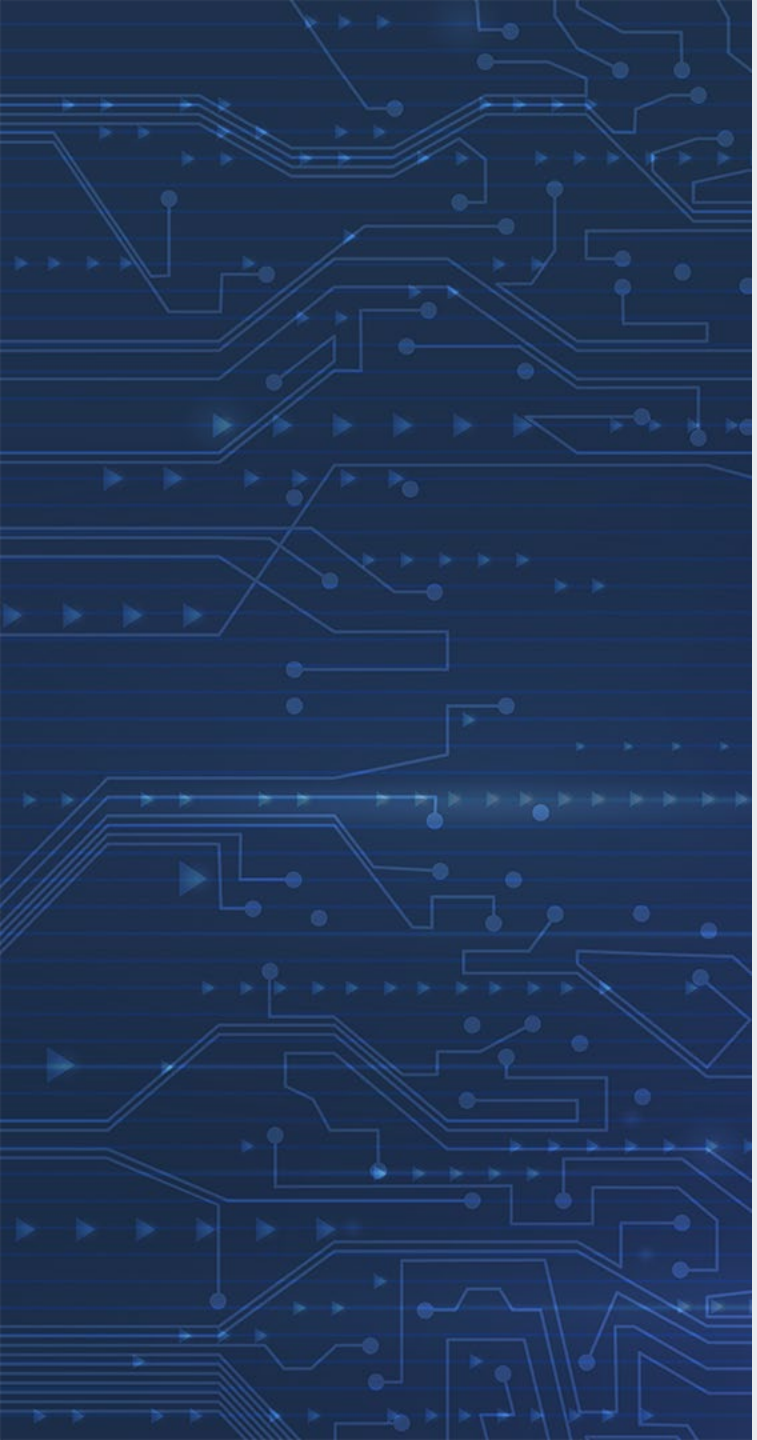
Agenda

- What Is an Electronic Medical/Health Record (EMR/EHR)?
- How Are EMR/EHRs Stored and Handled?
- Top EMRs/EHRs Used In Hospitals
- Benefits and Risks of Using EMRs/EHRs
- Health Sector Under Siege: Notable Data Breaches and Cyber Incidents
- Top Healthcare Data Breaches
- The Health Sector's Most Wanted: Threat Actor Profiles
- The Future of EMRs/EHRs
- Law & Order: Data Breach Penalties
- Protecting the Health Sector
- Recommendations

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Electronic Medical and Health Records

An In-Depth Look

What Is An Electronic Medical/Health Record?

Electronic medical records (EMRs) and electronic health records (EHRs) are often used interchangeably. An EMR allows the electronic entry, storage, and maintenance of digital medical data. EHRs contain patients' records from doctors and include demographics, test results, medical history, history of present illness (HPI), and medications. EMRs are part of EHRs and contain the following:

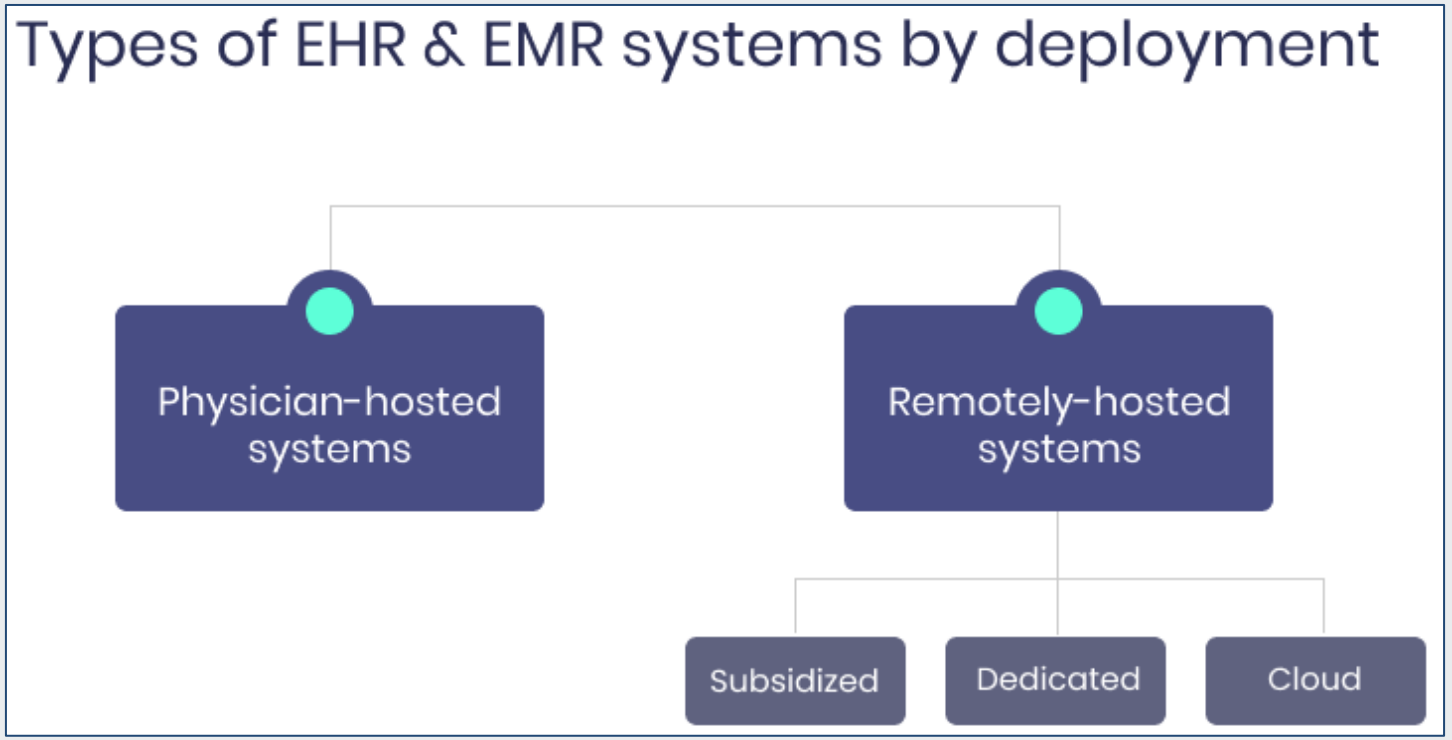
- Patient registration, billing, preventive screenings, or checkups
- Monitoring and improving overall quality of care
- Patient appointment and scheduling
- Tracking patient data over time

EMR	EHR
Designed to store patients' information in the form of charts digitally.	Records health data digitally.
Cannot share patients' data outside the practice.	Transfer data to concerned authorities according to CMS standards in real time.
Helps diagnose patients accurately.	Simplifies decision-making processes.
Restricts access to demographic data.	View lab results, imaging, insurance claims information, demographic data and more.

Source: SelectHub

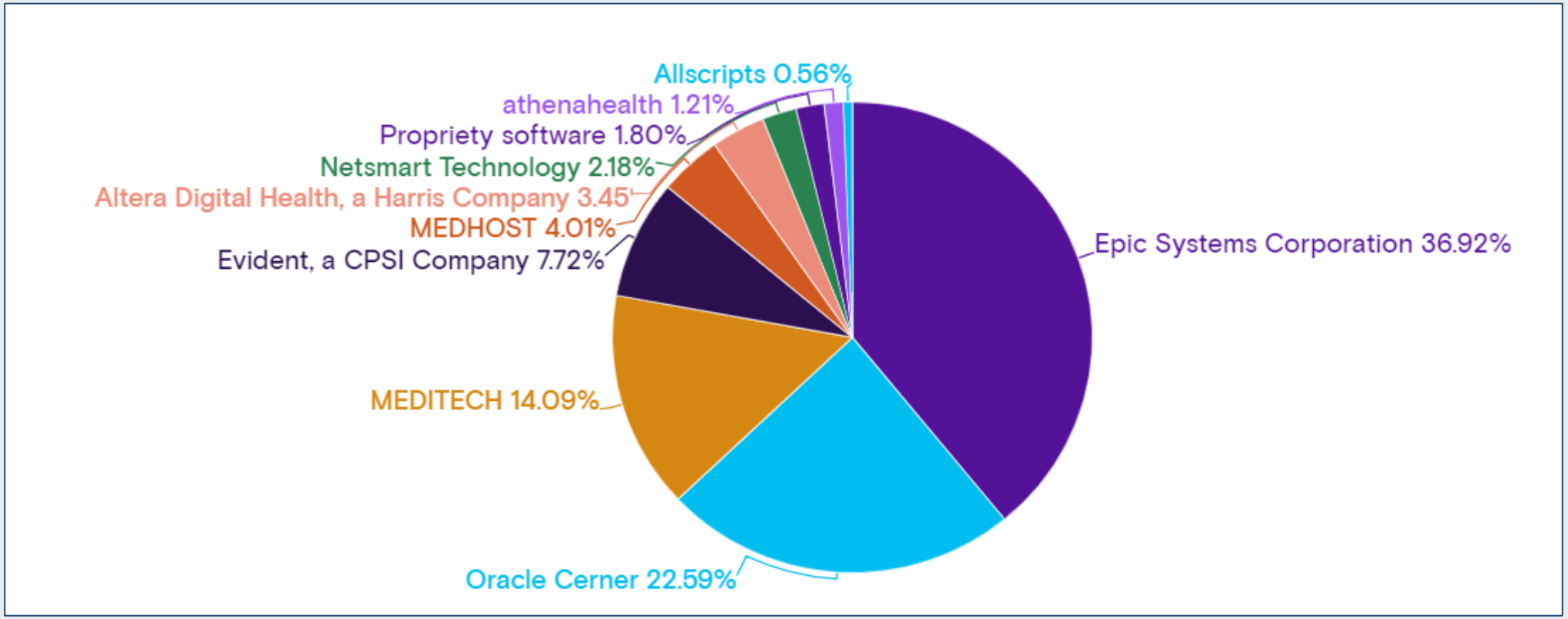
How are EMRs/EHRs Stored and Handled?

EMR/EHR data is stored on dedicated servers in specific, known physical locations.



Source: Empeek

Top 10 Inpatient EMRs/EHRs Used in Hospitals

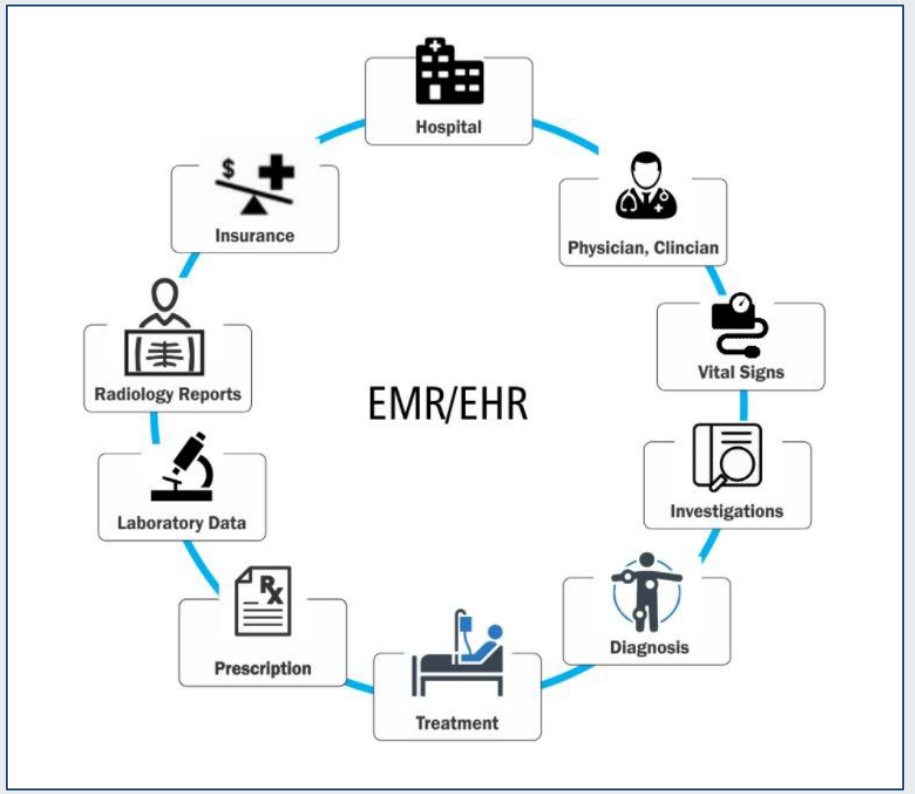


Top 10 Inpatient EHR Vendors by Market Share

Source: Definitive Healthcare (Data accurate as of June 20, 2022)

Top Threats Against Electronic Medical and Health Records

- Phishing attacks
- Fraud
- Data breaches and vulnerabilities
- Malware and ransomware attacks
- Encryption blind spots
- Cloud threats/Third-party risks
- Employees/Insider threats



Source: Integracon

Benefits and Risks

Using EMRs/EHRs in Healthcare

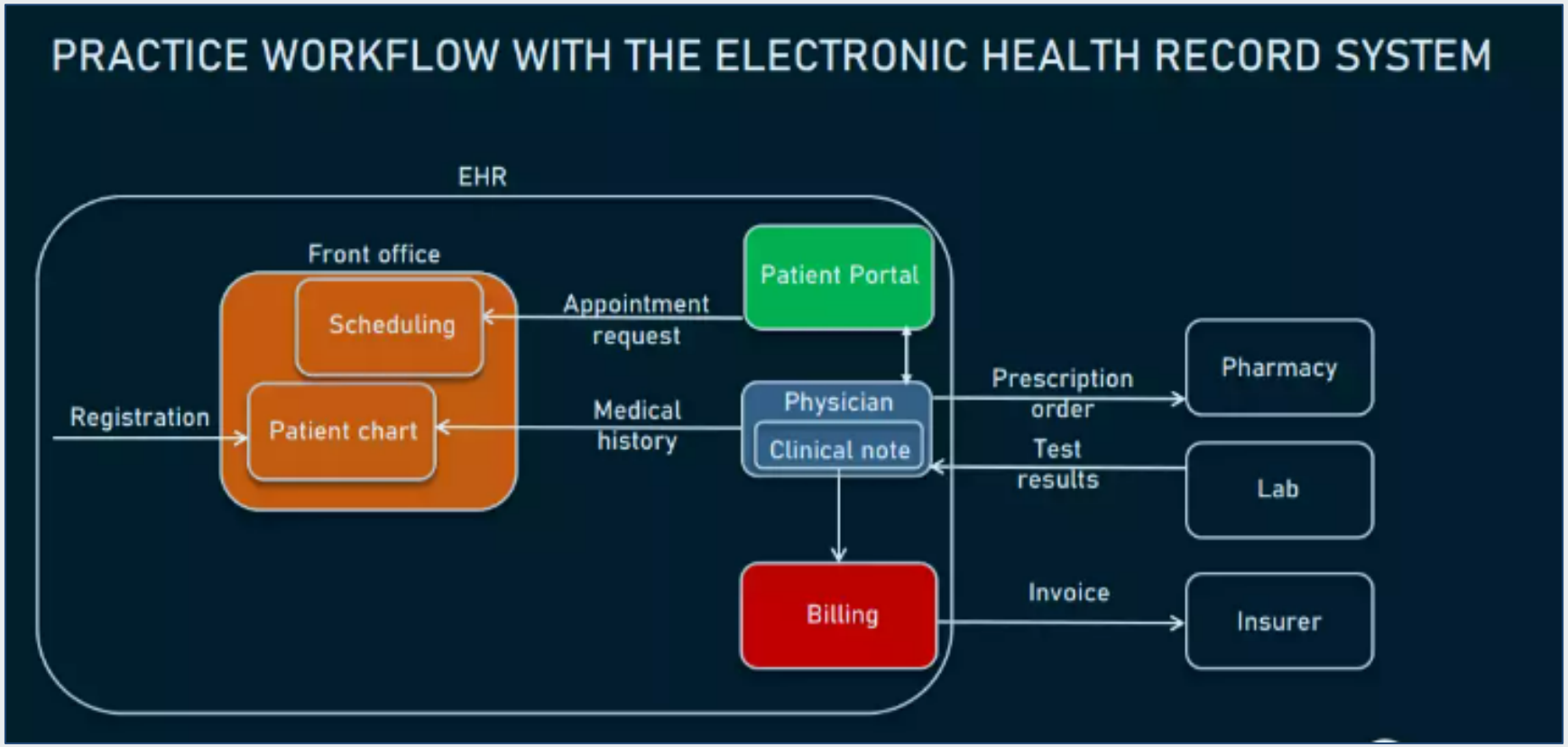
Benefits of Using EMR/EHR

Some of the most common benefits in regards to both EHR and EMR:

- Both EHR and EMR help reduce the number of medical errors and improve healthcare by keeping information accurate and up-to-date
- Comprehensive patient-history records
- Makes patient data shareable
- Improved quality of care
- Convenience and efficiency
- Patient charts and documents are much more clear as a result of reporting electronically
- Duplicate testing can be reduced to save both patients as well as providers time and money
- Both promote more patient participation, which in turn encourages healthier lifestyles and medical knowledge
- More complete and updated patient information can help lead to more accurate diagnoses and treatments

Source: appinventiv

Benefits of Using EMR/EHR, Part 2



Source: Altexsoft

Risks of Using EMR/EHR

The risks of using EHRs relate primarily to a range of factors that include user-related issues, financial issues and design flaws that create barriers to using them as an effective tool to deliver healthcare services. EMR is also a top target in healthcare breaches.

Additional risks are as follows:

- Security or privacy issues
- Can be vulnerable to hacking
- Data lost or destroyed
- Inaccurate paper to computer transmission
- Cause of treatment error

Source: appinventiv

Health Sector Under Siege

Notable Data Breaches and Cyber Incidents

Top Cyber Threats to Healthcare

It is imperative that organizations in the healthcare and public health sector gain an awareness of potential risks and implement the right threat intelligence tools to quickly identify, mitigate, and prevent cyber attacks.

According to Flashpoint, the following are the top threats to the healthcare and public health sector in 2022:

- Fraud
- Data breaches and vulnerabilities
- Third-party risk
- Ransomware
- Insider threats

Top Healthcare Data Breaches (2022)

Reports show that 90% of the 10 largest healthcare data breaches in 2022 were linked to third party-vendors:

- ***Health plans' printing and mailing vendor,*** Wisconsin, 4.11 million individuals
- ***EHR and practice management systems,*** North Carolina, 3.6 million individuals
- ***Healthcare system,*** Illinois, 3 million individuals
- ***EHR and practice management software provider,*** Pennsylvania, 2.2 million individuals
- ***Medical services provider,*** Massachusetts, 2 million individuals
- ***Hospital and medical facilities' debt collection firm,*** Colorado, 1.91 million individuals
- ***Hospital,*** Texas, 1.71 million individuals
- ***Healthcare provider,*** New York, 1.5 million individuals
- ***Healthcare provider,*** North Carolina, 1.36 million individuals
- ***Healthcare provider,*** Florida, 1.35 million individuals

January 2023 Healthcare Data Breaches

From third-party data breaches to pro-Russia hacktivist groups taking down health system websites, here is a list of health systems that have been affected by cybersecurity incidents in January 2023:

- A Maryland-based hospital reported a network outage on January 30 due to a ransomware attack. (Number of individuals impacted not released by organization.)
- A Memphis, Tennessee-based healthcare provider notified its patients that some of their confidential information may have been compromised in a data breach that affected its revenue cycle management vendor. (Number of individuals impacted not released by organization.)
- A Franklin, Tennessee-based healthcare provider notified patients that some of their confidential information was compromised when its cybersecurity firm experienced a data breach. (Number of individuals impacted not released by organization.)
- A Dover, New Hampshire-based healthcare provider notified its patients that some of their confidential information was exposed after an unauthorized party accessed its technology service provider. (Number of individuals impacted not released by organization.)
- A Springfield, Colorado-based healthcare provider notified patients that some of their protected health information may have been compromised after an unauthorized party accessed one of its employee email accounts. (1,435 individuals impacted.)

January 2023 Healthcare Data Breaches, Part 2

- A San Diego, California-based healthcare provider notified patients that an unauthorized party had stolen files from its system after it took over the health system's website server on January 12. (Number of individuals impacted not released by organization.)
- A Hayward, California-based hospital notified 501 patients and employees that some of their protected health information may have been stolen after an unauthorized user accessed its computer systems in November.
- An email phishing incident may have compromised the protected health information of about 300,000 members of a Pittsburgh, Pennsylvania-based healthcare organization.
- A Nashville, Arkansas-based hospital notified 53,668 patients that some of their protected health information may have been compromised in a December cybersecurity incident after an unauthorized party stole files from its network.
- Russian hacking group Killnet claimed responsibility for a cyberattack that disrupted 20 hospital and health system websites across the U.S.

Health Systems Affected (March 2023)

The cybersecurity threat landscape is ever changing. Here are some health system incidents of note from Becker's Hospital Review February 28 – March 20, 2023:

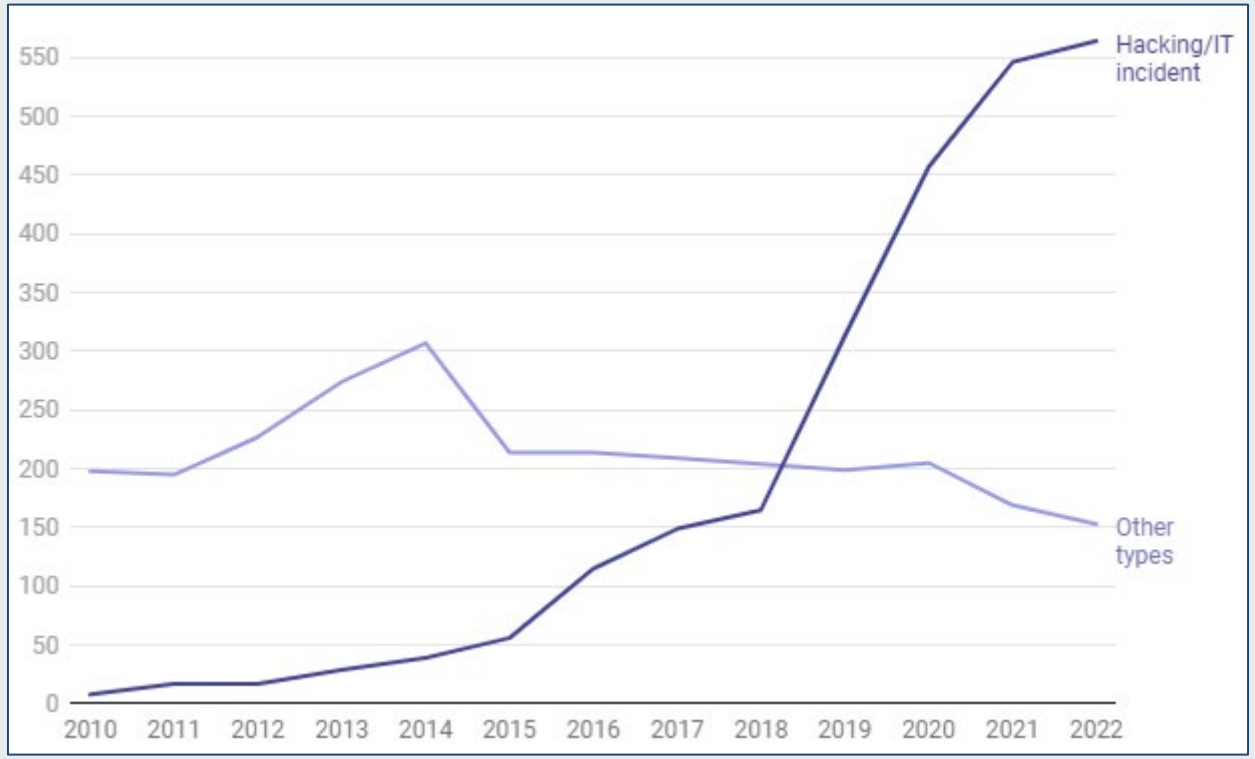
- A woman alleges that a contract employee from a Martinez, California-based healthcare facility gained access to her medical records and posted them to a Facebook account.
- A San Diego, California-based medical facility's technology vendor transmitted patients' confidential information to third-party service providers.
- A South Bend, Indiana-based healthcare provider notified 3,117 patients that some of their personal information may have been accessed by an unauthorized employee who viewed patient records outside the scope of their job duties.

Health Systems Affected (March 2023), Part 2

- A Livonia, Michigan-based healthcare provider filed a data breach notice with the Massachusetts attorney general on March 9 after it learned that some patient information was compromised as a result of unauthorized access.
- A Jamestown, New York-based healthcare provider notified patients that some of their protected health information was compromised when its medical records provider experienced an unauthorized disclosure.
- A Richmond, Virginia-based hospital notified 990 patients that some of their protected health information was compromised in a data breach.
- A cyberattack disrupted a Warner Robins, Georgia-based healthcare provider's operations; the health system was able to remain open and care for patients using its backup processes and downtime procedures.
- An anonymous individual called a Norfolk, Virginia-based healthcare provider to notify the hospital that a PDF copy of a Medicare remittance report for lab services was uploaded to an Adobe Acrobat website.

EMR/EHR Compromised: Healthcare Organizations Hacked

According to government documents (OCR Breach Portal), 385 million patient records may have been exposed in healthcare data breaches from 2010–2022.



Source: Healthcare Dive

Costs of A Data Breach

The healthcare industry's average cost of a data breach in 2022 has increased over the past year. According to IBM's Cost of a Data Breach Report 2022, the average total cost of a breach in healthcare increased from 9.23 million USD in 2021 to 10.10 million USD in 2022.

HIPAA stipulates four tiers of violations that reflect increasing levels of culpability, with minimum and maximum penalty amounts within each tier for each violation.

The most recent fines are as follows:

- Tier 1—***Lack of knowledge***: Penalty from $127 up to $63,973.
- Tier 2—***Reasonable cause and not willful neglect:*** Penalty from $1,280 to $63,973.
- Tier 3—***Willful neglect, corrected within 30 days:*** Penalty from $12,794 to $63,973.
- Tier 4—***Willful neglect, not corrected within 30 days:*** Penalty from $63,973 to $1,919,173.

Why Are EMR/EHRs Valuable?

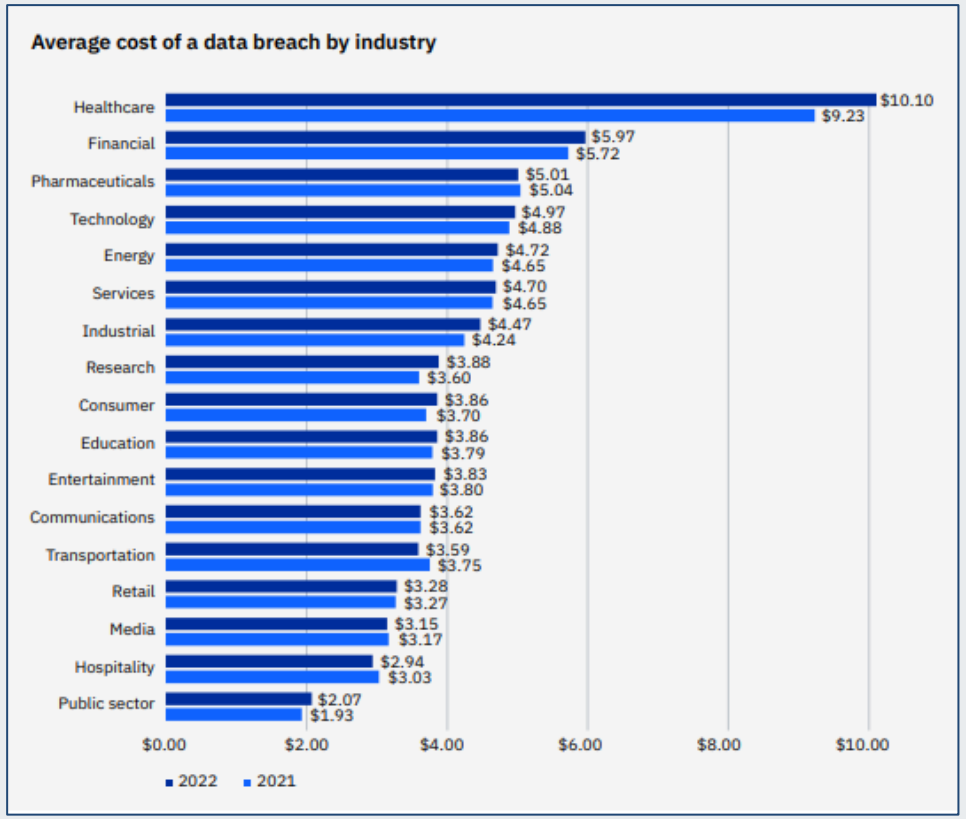
EMRs/EHRs are valuable to cyber attackers because of the PHI information they contain and the profit they can make on the dark web or black market. These 18 identifiers provide criminals with more information that any other breached record. Extortion, Fraud, Identity Theft, Data Laundering, Hacktivist/Promoting Political Agendas and Sabotage are some ways cyber attackers use this data for profit.

HIPAA Protected Health Identifiers (PHI)		
Names	Dates, except year	Telephone numbers
Geographic data	FAX numbers	Social Security numbers
Email addresses	Medical record numbers	Account numbers
Health plan beneficiary numbers	Certificate/license numbers	Vehicle identifiers and serial numbers including license plates
Web URLs	Device identifiers and serial numbers	Internet protocol (IP) addresses
Full face photos and comparable images	Biometric identifiers (i.e. retinal scan, fingerprints)	Any unique identifying number or code

Source: HIPAA Journal

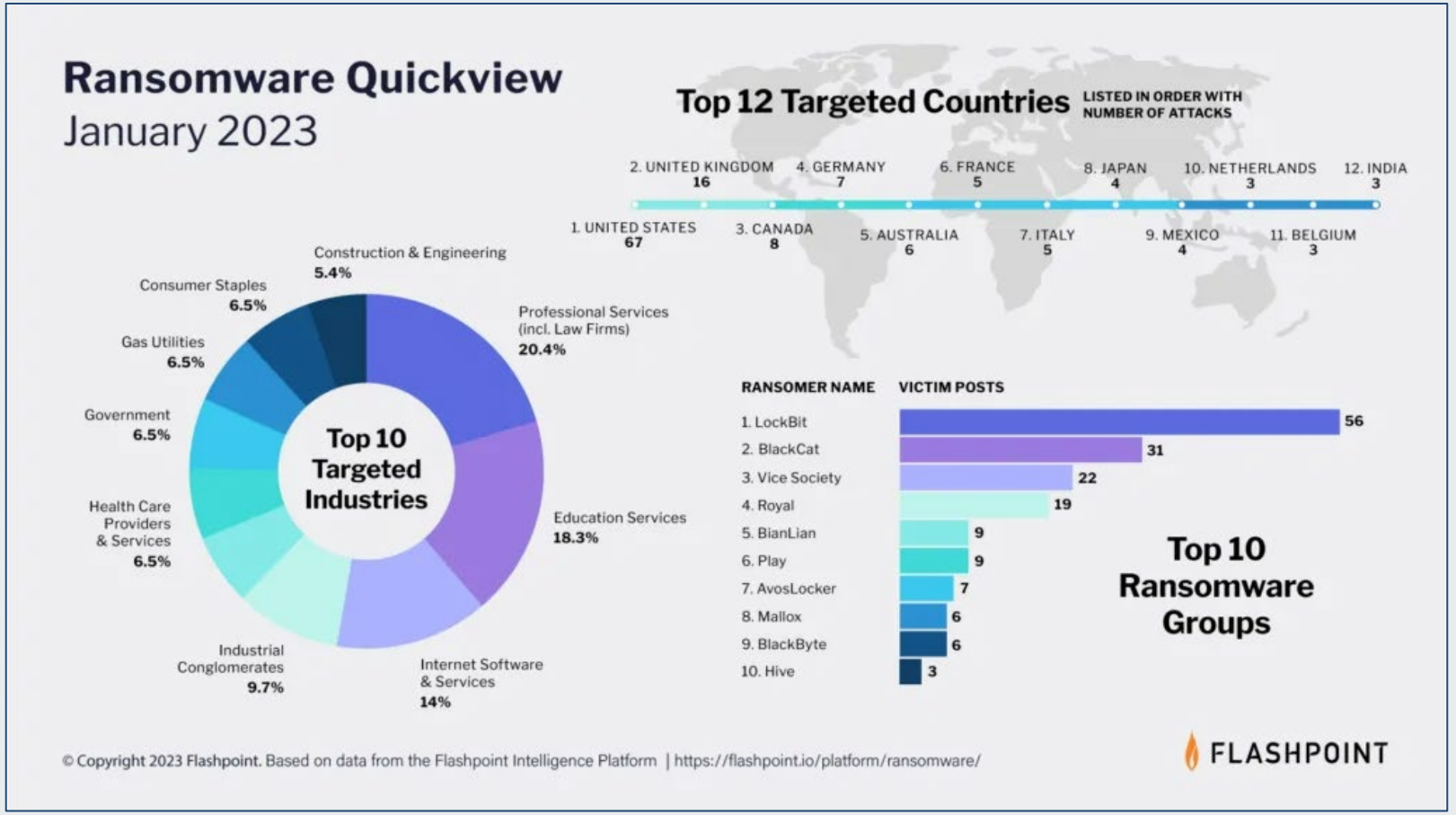
Why Are EMR/EHRs Valuable? Part 2

According to IBM Security, in 2022 Healthcare was the highest cost industry for the 12th year in a row. The average total cost of a breach in healthcare increased from USD 9.23 million in 2021 to USD 10.10 million in 2022.



Source: IBM Security

Ransomware At A Glance



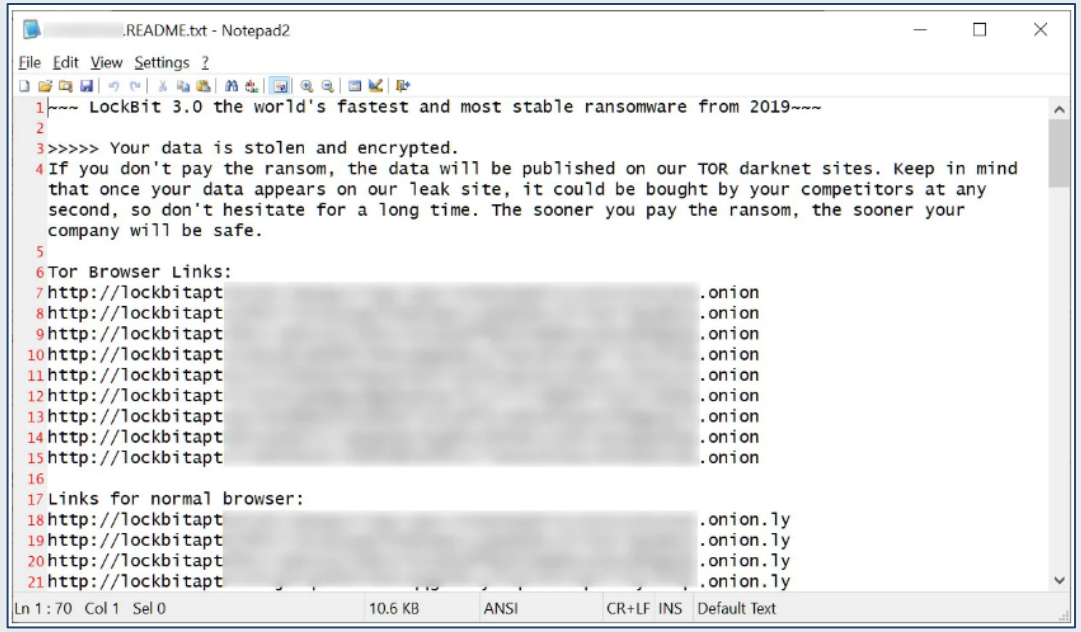
Source: Flashpoint

The Health Sector's Most Wanted

Threat Actor Profiles

LockBit 3.0

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit.



A LockBit ransom note.
Source: Bleeping Computer

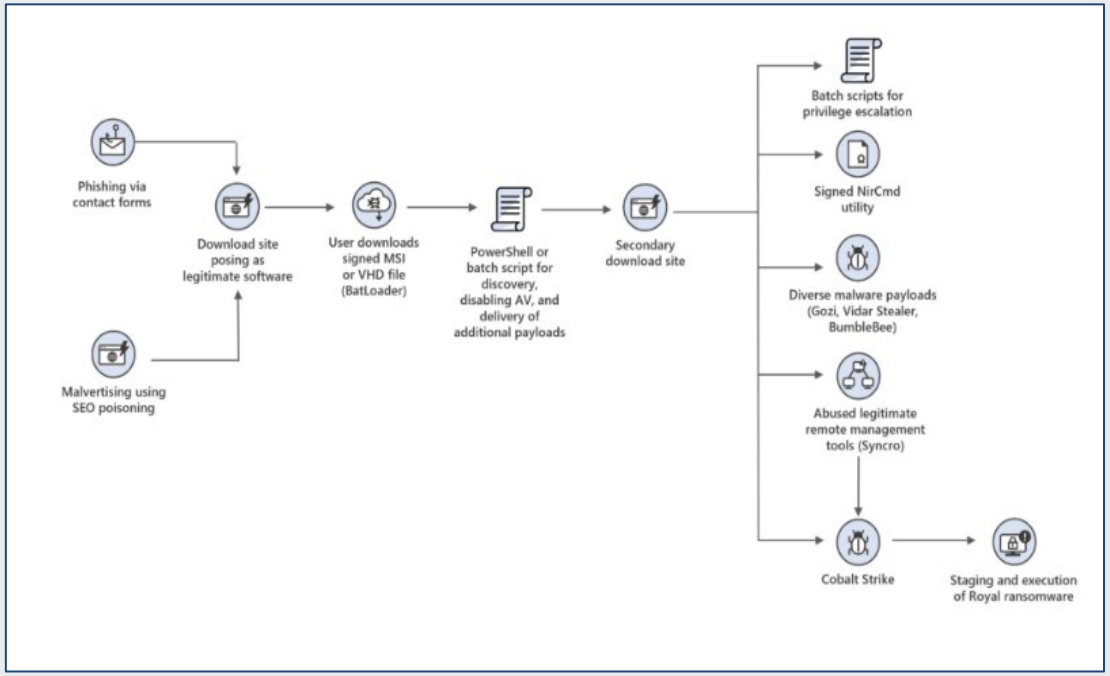
BlackCat, aka AlphV

- The BlackCat–also known as “AlphaV”–ransomware gains initial access to a targeted system using compromised user credentials, and uses them to gain access to a compromised user’s admin accounts in the Active Directory.
- This access enables the threat to configure malicious Group Policy Objects (GPOs) throughout the Windows Task Scheduler for the purpose of deploying its ransomware payload.
- During initial deployment, BlackCat disables security features in the victim's network, exfiltrating information prior to execution. It then uses numerous batch and PowerShell scripts to proceed with the infection. These include “est.bat,” which copies the ransomware to other locations, and “drag-and-drop-target.bat,” which launches the ransomware executable for the MySQL Server.

Source: AT & T Alien Labs Research

Royal

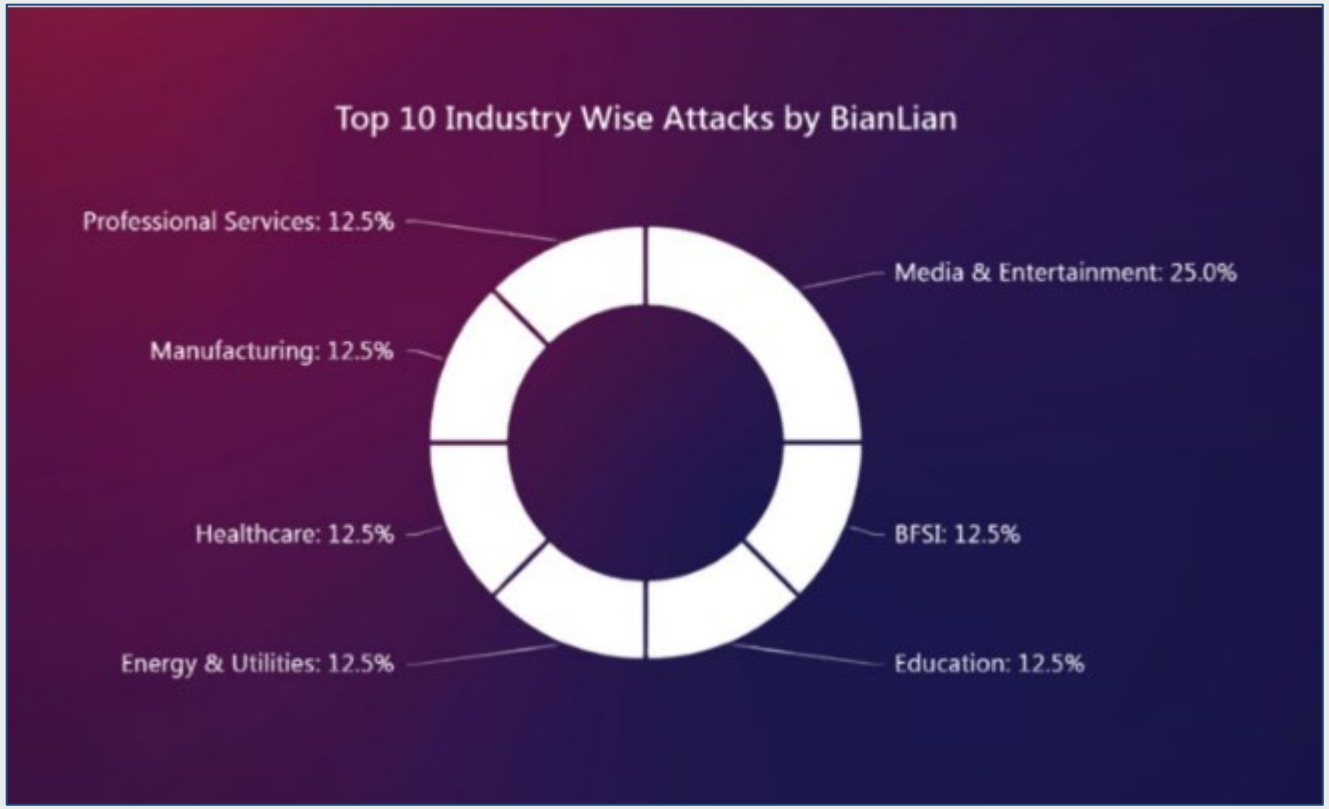
- Since September 2022, Royal has begun deploying its own ransomware.
- Royal appears to be a private group without any affiliates. Ransom demands range from $250,000 to over $2 million USD.
- The group will conduct methods seen from other operations, including deploying Cobalt Strike for persistence, harvesting credentials, and moving laterally through a system until files are encrypted.
- Royal Ransomware operations start in various ways, including phishing campaigns using common cyber crime threat loaders, such as BATLOADER and QBot.
- Following initial infection, Royal often leverages Cobalt Strike, QBot and BlackBasta for multi-stage attacks.



High-level view of observed DEV-0569 infection chains between August – October 2022.
Source: Microsoft

BianLian

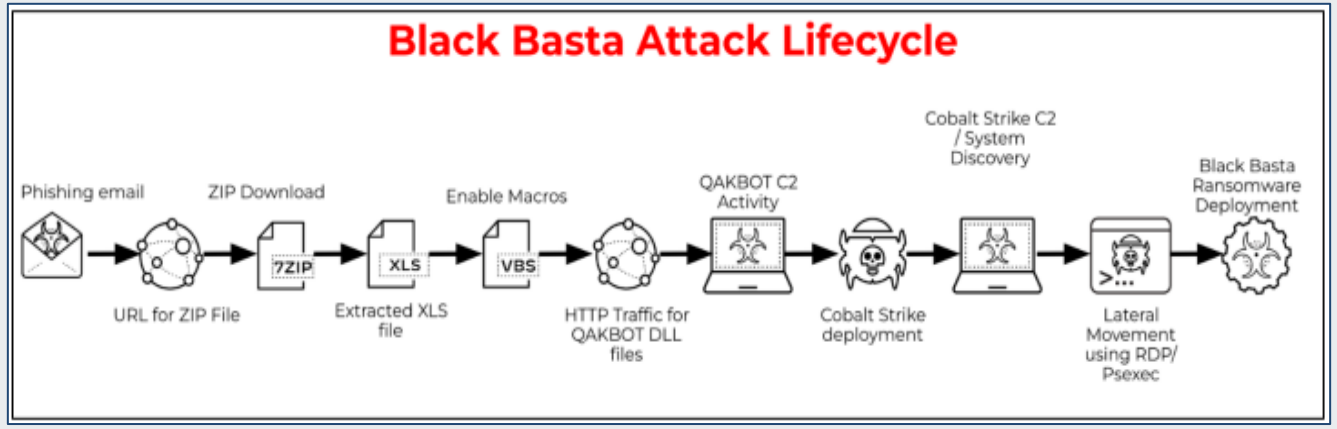
Healthcare is among top industries targeted by this threat actor group.



Industries Targeted by the BianLian Ransomware
Source: SecureBlink

Black Basta

- Black Basta is identified as a unique RaaS group and ransomware that is a credible threat to the health sector. Similar tactics, techniques, and procedures (TTPs) with other Russian-speaking threat actors suggest the idea among many that Black Basta is closely related to or has current and former operators from other groups, like Conti, FIN7, and/or BlackMatter.
- Black Basta operators often utilize unique TTPs to gain entry, spread laterally, exfiltrate data, and drop ransomware. The ransomware is a cross-platform ransomware that is only executed with administrator privileges on both Windows and Linux systems. The ransomware hinders machine processes and ultimately makes desktop files unusable before sending a ransom note to a victim.



Source: Unit 42

The Future of EMRs/EHRs

Key Takeaways

According to a report by Grand View Research, the global market for Electronic Health Records (EHRs) is projected to increase significantly.

- The global EMR/EHR market is expected to reach $38.5 billion by 2030.
- Documentation issues, such as risk-based management codes and use of modifiers, remain a concern for physician practices.
- The most significant improvements in EHR will be in patient engagement, integration, big data implementation and standardization.

Importance Of EHR Trends

Electronic Medical/Health Records are here to stay for the foreseeable future, so organizations should work to protect Personal Identifiable Information (PII)/Protected Health Information (PHI) and should be aware of market trends.

Source: Grand View Research/ Select Hub

Future Trends

Electronic health records trends to keep an eye out for:

- Integration and Interoperability
- Cloud Computing
- Standardization
- Robotic Process Automation
- Telehealth
- IoT, AI, and Voice Recognition
- Error Reduction
- Blockchain and EHR
- 5G, 6G and Big Data
- Wearable Devices
- Real-time Data and Analytics

Robotic Process Automation (RPA)

According to Precedence Research, the global robotic process automation market was evaluated at $2.9 billion in 2022 and is expected to reach $6.2 billion by 2030.

IoT, Artificial Intelligence (AI) and Voice Recognition

The global internet of things (IoT) healthcare market is expected to grow at a compound annual growth rate (CAGR) of 21.41%, to reach $960.2 billion by 2030.

Blockchain and EHR

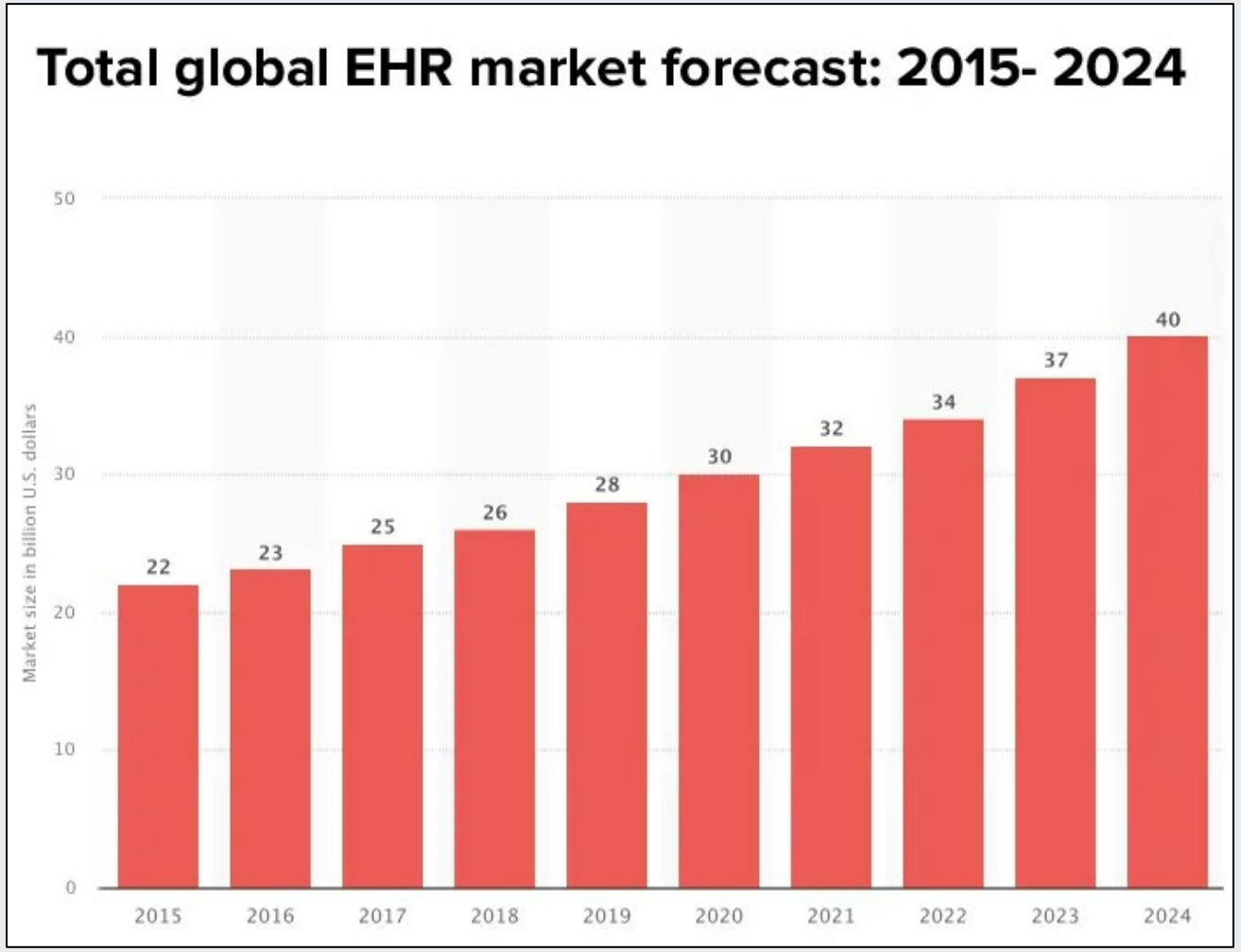
According to the Research and Markets August 2022 report, global blockchain technology in the healthcare market is expected to grow at a CAGR of 39.9%, reaching $5.8 billion by 2028.

Wearable Devices

According to Stratview Research, there will be a significant increase in the use of wearable devices. The wearable medical tech market is expected to grow at a CAGR of 23.7%, reaching $95.4 billion by 2028.

Global EMR/EHR Forecast

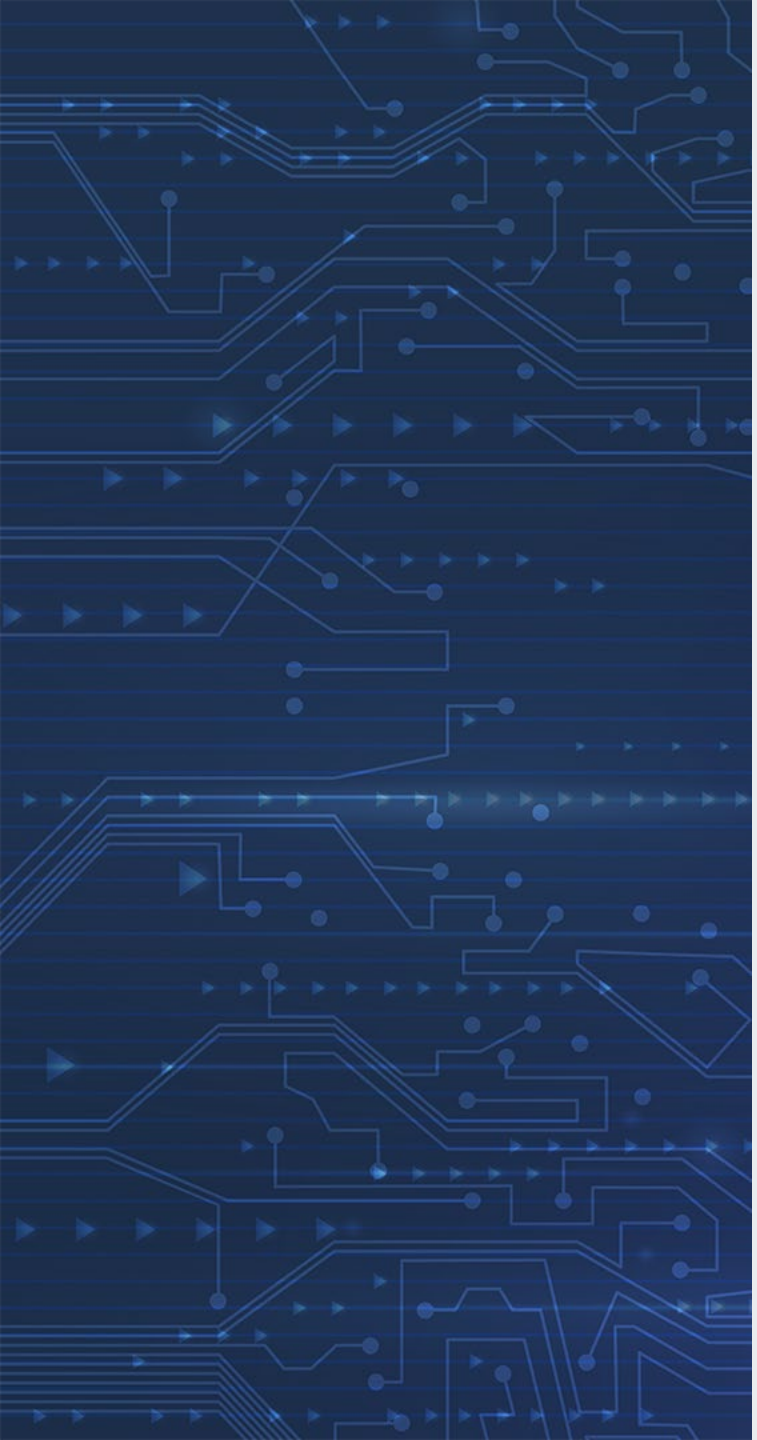
The global electronic health records market is projected to reach a valuation of $40 billion by 2024.



Source: appinventiv

Next Steps

Electronic medical/health records will continue to be a significant part of the healthcare industry, so utilizing all resources to protect PII/PHI is key. In the years to come, EMRs/EHRs will be enhanced with significant growth in IoT devices, big data technology and telehealth systems, and digitization will become a core offering in healthcare institutions.



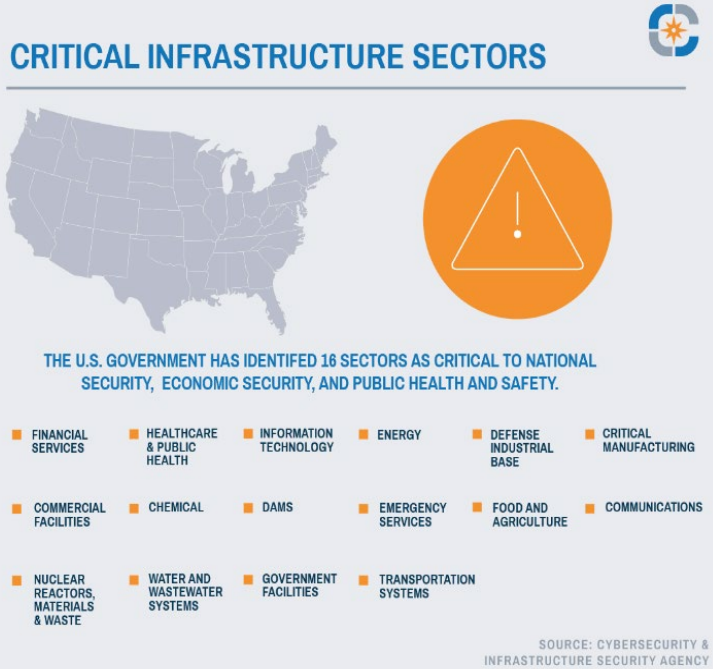
Law & Order

Data Breach Penalties

The Strengthening American Cybersecurity Act of 2022

Passed in March 2022, organizations within critical infrastructure sectors have 12-18 months to implement these and other policies and practices:

- Adopt Zero Trust, which is a shift away from the current practice of trusting all devices and traffic within a trusted network. Instead, zero trust applies security controls to ensure that employees have the appropriate access to the resources they need, and that access is continuously assessed.
- Apply the Principle of Least Privilege in managing access to data. With this approach to information security, end-users are given the minimum levels of access possible, and access to higher levels of access is reviewed regularly.
- Execute improved mobile security standards and enhanced mobile device management (MDM). Implementing MDM allows IT departments to monitor, manage, and secure employees' mobile devices that contain or access company assets.
- Identify and strengthen protections for systems likely to be targeted by ransomware. In addition, prepare for potential breaches by having an incident response plan and practice implementing it with tabletop exercises.



FD&C Act – “Ensuring Cybersecurity of Devices.”

In March 2023, the FD&C Act was amended to include section 524B, “Ensuring Cybersecurity of Devices.” According to this revision:

“A person who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as [FDA] may require to ensure that such cyber device meets the cybersecurity requirements under subsection (b).”

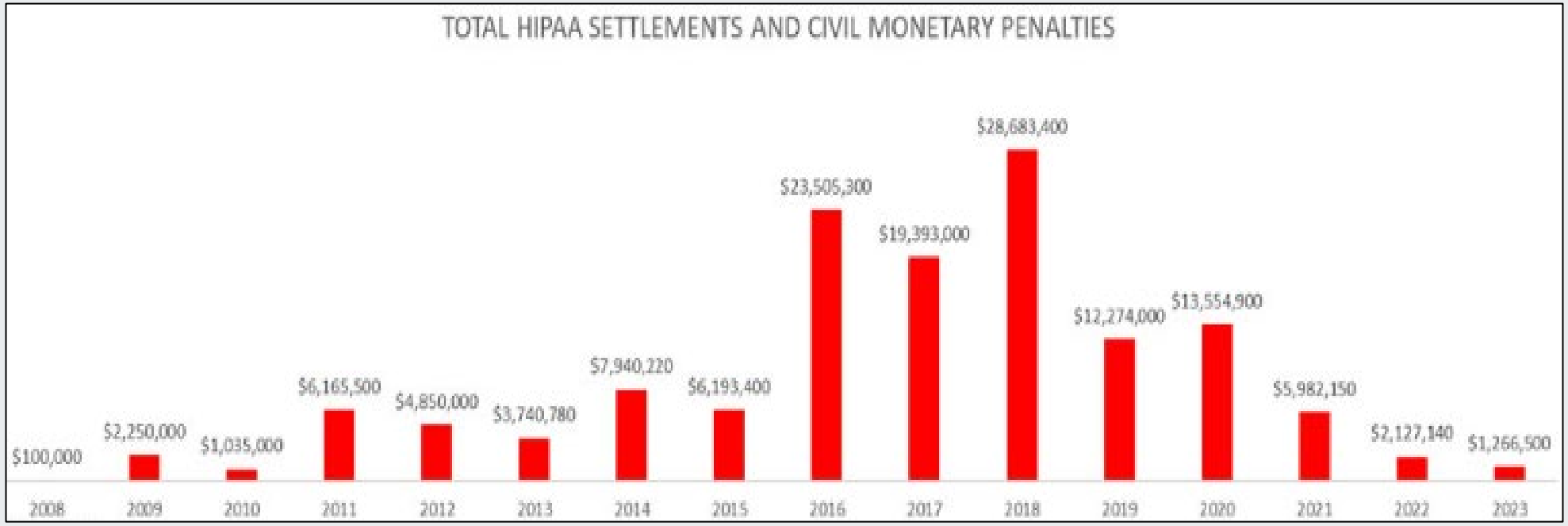
The entire document can be accessed here.

HIPAA Violation Fines and Penalties

Penalty Tier	Level of Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Limit
Tier 1	Reasonable Efforts	$127	$63,973	$1,919,173
Tier 2	Lack of Oversight	$1,280	$63,973	$1,919,173
Tier 3	Neglect – Rectified within 30 days	$12,794	$63,973	$1,919,173
Tier 4	Neglect – Not Rectified within 30 days	$63,973	$1,919,173	$1,919,173

Source: HIPAA Journal

HIPAA Violation Fines and Penalties, Part 2



Source: HIPAA Journal

Law Firm Fined for Failure to Protect Data

A New York law firm suffered a LockBit ransomware attack and agreed to pay a $200,000 financial penalty to the New York Attorney General, to resolve violations of the New York General Business Law and the Privacy and Security Rules of HIPAA. The law firm allegedly violated New York General Business Law and failed to issue timely notifications to 61,438 New York residents. Some of the 17 HIPAA violations are as follows:

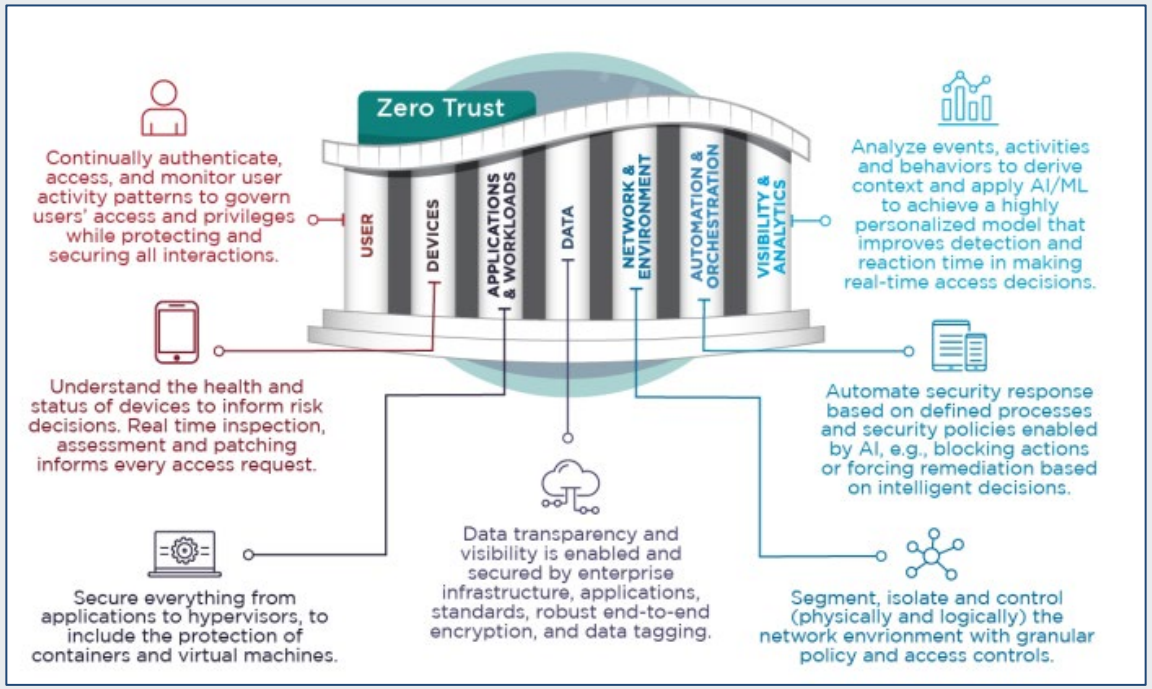
- The failure to safeguard electronic protected health information (ePHI).
- The failure to protect against reasonably anticipated threats to ePHI.
- The failure to review and modify data protection practices.
- The failure to conduct an accurate and thorough risk assessment.
- The failure to adhere to the minimum necessary standard.
- The failure to implement appropriate security measures to reduce risks to ePHI.
- The failure to implement reasonable and appropriate policies and procedures to comply with the standards of 45 C.F.R. Part 164, Subpart C.
- The failure to prevent unauthorized access to ePHI.

Protecting the Health Sector

Recommendations

Zero Trust Model

HC3 recommends organizations review and consider implementing the Zero Trust Security Model. The NSA's 2023 guidance can be accessed by clicking here.



Source: National Security Agency (NSA)

Core Tenets of Zero Trust

In their *Identity and Zero Trust* white paper, Health-ISAC shares NIST's guidance for "Zero Trust Architecture."

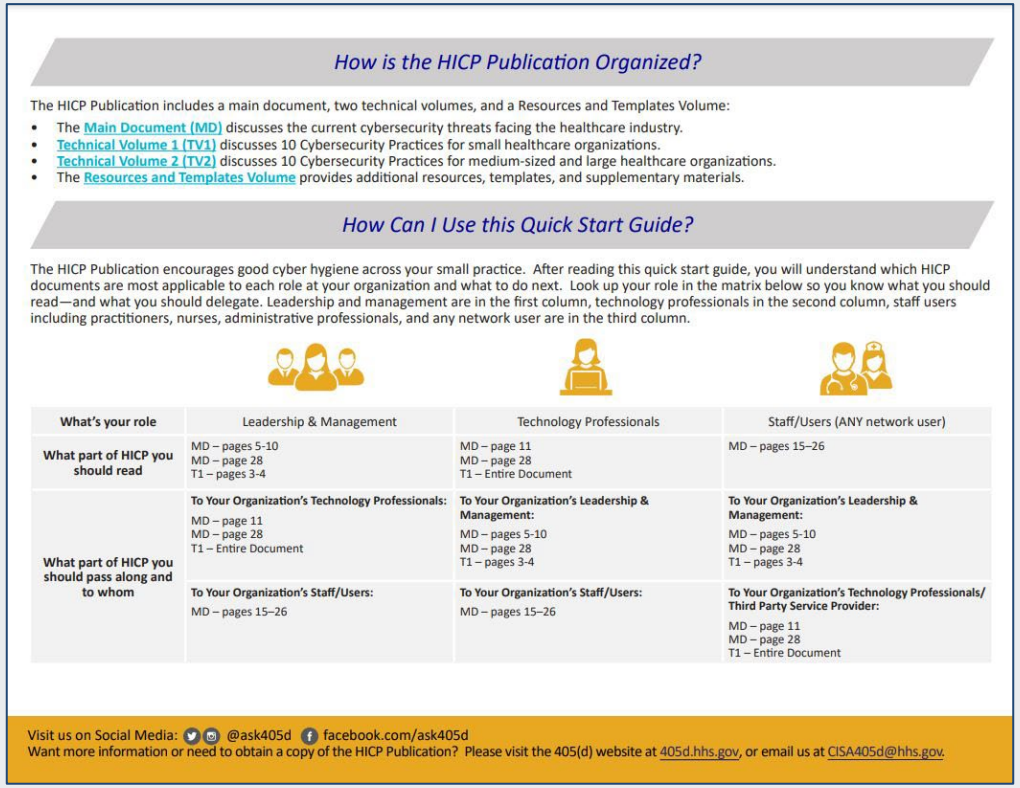
#	TENET	EXPLANATION	HEALTH CARE IMPLICATIONS
1	All data sources and computing services are considered resources.	Networks may be made up of multiple types of devices from cloud services, laptops, mobile devices, even personal devices that could be used to access resources.	Health care organizations have multiples types of devices – echocardiograms, infusion pumps, blood oxygen measurement, sending data to central monitoring stations.
2	All communication is secured regardless of network location.	Network communication is secured regardless of whether its inside or outside of the perimeter. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.	Communication with the network and all devices – including IoT devices – must be secure via encryption or other secure method.
3	Access to individual enterprise resources is granted on a per-session basis.	Trust is evaluated before access is granted with least privilege in mind.	For caregivers and individuals accessing multiple applications at different times their access rights need to be evaluated and sessions established appropriately.
4	Access to resources is determined by dynamic policy and may include other behavioral and environmental attributes.	An organization protects resources by defining its resources, its members, and the resources those members need to access. In addition to authentication and authorization at the time of request, zero trust may also look at behavioral attributes – i.e., device analytics and environmental factors, such as network location, reported activity.	Individuals accessing health care or billing records need to be validated beyond the typical username and password; multi-factor authentication is a must. This may include and may include specific certificates on devices or other behavioral attributes. This would prevent a heart rate monitor from accessing personal health information.
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Constant monitoring of all devices on a network to detect potential breaches or vulnerabilities.	In a health care setting the number of devices present on a network is more than what a typical enterprise may see and securing all of these different devices that use different standards could be challenging.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	All devices must have identities and roles within the enterprise to access only the necessary resources.	Individuals and devices must have restricted access based on least privilege.
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	Constant monitoring of all individuals, devices, and the network to spot anomalous or suspicious behaviors.	Monitoring all employees and devices on a network to prevent unauthorized behavior.

Source: Health-ISAC

Health Industry Cybersecurity Practices (HICP)

Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Small Healthcare Organization

Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Medium & Large Healthcare Organizations



How is the HICP Publication Organized?

The HICP Publication includes a main document, two technical volumes, and a Resources and Templates Volume:

- The Main Document (MD) discusses the current cybersecurity threats facing the healthcare industry.
- Technical Volume 1 (TV1) discusses 10 Cybersecurity Practices for small healthcare organizations.
- Technical Volume 2 (TV2) discusses 10 Cybersecurity Practices for medium-sized and large healthcare organizations.
- The Resources and Templates Volume provides additional resources, templates, and supplementary materials.

How Can I Use this Quick Start Guide?

The HICP Publication encourages good cyber hygiene across your small practice. After reading this quick start guide, you will understand which HICP documents are most applicable to each role at your organization and what to do next. Look up your role in the matrix below so you know what you should read—and what you should delegate. Leadership and management are in the first column, technology professionals in the second column, staff users including practitioners, nurses, administrative professionals, and any network user are in the third column.

What's your role	Leadership & Management	Technology Professionals	Staff/Users (ANY network user)
What part of HICP you should read	MD – pages 5-10 MD – page 28 T1 – pages 3-4	MD – page 11 MD – page 28 T1 – Entire Document	MD – pages 15–26
What part of HICP you should pass along and to whom	**To Your Organization's Technology Professionals:** MD – page 11 MD – page 28 T1 – Entire Document	**To Your Organization's Leadership & Management:** MD – pages 5-10 MD – page 28 T1 – pages 3-4	**To Your Organization's Leadership & Management:** MD – pages 5-10 MD – page 28 T1 – pages 3-4
	To Your Organization's Staff/Users: MD – pages 15–26	**To Your Organization's Staff/Users:** MD – pages 15–26	**To Your Organization's Technology Professionals/ Third Party Service Provider:** MD – page 11 MD – page 28 T1 – Entire Document

Visit us on Social Media: @ask405d facebook.com/ask405d
Want more information or need to obtain a copy of the HICP Publication? Please visit the 405(d) website at 405d.hhs.gov, or email us at CISA405d@hhs.gov.

Source: HHS

Office of **Information Security** Securing One HHS

Health Sector Cybersecurity Coordination Center

Cyber Threats and Best Practices

It is recommended that all organizations follow the best practices and implement the steps outlined in CISA Insights to protect against cyber threats.

Some recommended steps are:

- Reduce the likelihood of a damaging cyber intrusion.
- Take steps to quickly detect a potential intrusion.
- Ensure your organization is prepared to respond if an intrusion occurs.
- Maximize your organization's resilience to a destructive cyber incident.

Reduce the Likelihood of a Damaging Cyber Intrusion

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take Steps to Quickly Detect a Potential Intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by anti-virus/anti-malware software and that signatures in these tools are updated.
- If working with international organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Be Prepared To Respond

- Designate a crisis response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize Your Organization's Resilience

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

Strengthen Organizational Cyber Posture

In addition to being in compliance with the law, organizations within the health sector should strive to do their best to protect data and sensitive information from nefarious threat actors. Developing a strong cybersecurity posture is vital to any organization, particularly the HPH sector. The following are steps to strengthen your cyber posture:

- Conduct regular security posture assessments.
- Consistently monitor networks and software for vulnerabilities.
- Define which department owns what risks and assign managers to specific risks.
- Regularly analyze gaps in your security controls.
- Define a few key security metrics.
- Create an incident response plan and disaster recovery plan.

Reference Materials

References

- “Top 5 threats to the healthcare and public health sector in 2022,” Flashpoint. June 29, 2022. https://flashpoint.io/resources/e-book/top-5-cyber-threats-to-the-healthcare-and-public-health-sector/.
- “Cost of a Data Breach Report 2022,” IBM. July 27, 2022. https://www.ibm.com/downloads/cas/3R8N1DZJ .
- Zelinska, Solomija. “ Which Types of EMR/EHR Systems are the Best for Your Business,” Empeek. March 5, 2022. https://empeek.com/which-types-of-emr-ehr-systems-are-the-best-for-your-business/ .
- Jerich, Kat. “HHS cyber arm warns of EHR vulnerabilities,” Health IT News. February 22, 2022. https://www.healthcareitnews.com/news/hhs-cyber-arm-warns-ehr-vulnerabilities#:~:text=Top%20threats%20against%20EHRs%20include,of%20breaches%20involved%20compromised%20credentials.
- Liss, Samantha, Ye Han, Jasmine. “Hacking healthcare: With 385M patient records exposed, cybersecurity experts sound alarm on breach surge,” HealthCare Dive. March 9, 2023. https://www.healthcaredive.com/news/cybersecurity-hacking-healthcare-breaches/643821/ .
- McKeon, Jill. “Key Ways to Manage the Legal Risks of a Healthcare Data Breach,” Health IT Security. October 14, 2022. https://healthitsecurity.com/features/key-ways-to-manage-the-legal-risks-of-a-healthcare-data-breach#:~:text=October%2013%2C%202022%20%2D%20Healthcare%20data,most%20importantly%2C%20patient%20safety%20risks.

References

- Diaz, Naomi. “8 health systems affected by data breaches in the last 30 days,” Becker’s Health IT. March 20. 2023. https://www.beckershospitalreview.com/cybersecurity/health-systems-affected-by-a-data-breach-in-the-last-30-days.
- Dydra, Laura. “Russian hackers disrupt health system websites across US,” Becker’s Health IT. February 6,2023. https://www.beckershospitalreview.com/cybersecurity/russian-hackers-disrupt-health-system-websites-across-us.html.
- “Electronic Health Record Systems: Features, EHR Vendors, and Adoption Advice,” Altexsoft. May 19, 2020. https://www.altexsoft.com/blog/electronic-health-record-systems/.
- “Threat Actors Continue to Target Healthcare,” NJCCIC. November 10, 2022. https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/threat-actors-continue-to-target-healthcare.
- FBI, CISA, MS-ISAC. “Joint Cybersecurity Advisory #StopRansomware: LockBit 3.0,” March 16, 2023. https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf.
- Behling, Dana. “LockBit 3.0 Ransomware Unlocked,” VMWare Security Blog. October 15, 2022. https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html.

References

- Odogwu, Chris. “What Is BlackCat Ransomware and How Can You Prevent It?,” Make Use Of(MUO). December 14, 2022. https://www.makeuseof.com/what-is-blackcat-ransomware/.
- “DEV-0569 finds new ways to deliver Royal ransomware, various payloads,” Microsoft Threat Intelligence. November 17, 2022. https://www.secureblink.com/threat-research/bian-lian-a-new-golan-based-cross-functional-ransomware-in-action.
- “BianLian: A new golan based cross functional ransomware in action,” Secure Blink. September 16, 2022. https://www.secureblink.com/threat-research/bian-lian-a-new-golan-based-cross-functional-ransomware-in-action.
- “10 most common inpatient EHR systems by market share,” Definitive Healthcare. https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems.
- “HC3 Threat Profile: Black Basta,” Health Sector Cybersecurity Coordination Center (HC3). March 15, 2023. https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf.

References

- Arora, Kashish. “Future of EHR/EMR: Experts Predict Trends in 2023,” Select Hub. March 27, 2023. https://www.selecthub.com/medical-software/emr/electronic-medical-records-future-emr-trends/.
- Kaplan, Soren. “Six Trends Shaping the Future of Health Care,” Inc. March 1,2019. https://www.inc.com/soren-kaplan/six-trends-shaping-future-of-health-care.html.
- “ EHR vs EMR: The Difference Between Them,” Select Hub. https://www.selecthub.com/medical-software/the-difference-between-ehr-vs-emr/.
- Gupta, Dileep. “Ways Electronic Health Records Will Continue to Improve in 2023,” appinventiv. February 28, 2023. https://appinventiv.com/blog/impact-of-technology-on-ehr/.
- Hecht, Jeff. “The future of electronic health records,” Nature. September 25, 2019. https://www.nature.com/articles/d41586-019-02876-y.
- “S.3600 - Strengthening American Cybersecurity Act of 2022,”Congress.gov. March 1, 2022. https://www.congress.gov/bill/117th-congress/senate-bill/3600.
- FDA. “Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act - Guidance for Industry and Food and Drug Administration Staff,” U.S. Food & Drug Administration (FDA). March 29, 2023. https://www.fda.gov/media/166614.

References

- "HIPAA Violation Fines," The HIPAA Journal. January 1, 2023. https://www.hipaajournal.com/hipaa-violation-fines/.
- "What is Considered PHI Under HIPAA?," The HIPAA Journal. January 1, 2023. https://www.hipaajournal.com/considered-phi-hipaa/.
- "January 2023 Healthcare Data Breach Report," The HIPAA Journal. February 22, 2023. https://www.hipaajournal.com/january-2023-healthcare-data-breach-report/.
- "New York Law Firm Pays $200,000 to State AG to Resolve HIPAA Violations," The HIPAA Journal. March 28, 2023. https://www.hipaajournal.com/new-york-law-firm-200000-settlement-new-york-hipaa/.
- National Security Agency/Central Security Service. "Guidance on Advancing Zero Trust Maturity Throughout the User Pillar," NSA.gov. March 14, 2023. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/.
- Health-ISAC. "White Paper Identity And Zero Trust: A Health-ISAC Guide For CISOS," H-ISAC.org. August 25, 2022. https://h-isac.org/wp-content/uploads/2022/08/H-ISAC_White-Paper-ZeroTrust_FINAL_82522.pdf.
- "Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Small Healthcare Organization, "HHS. https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Small-Practices-Official-Document-R.pdf.

References

- “Health Industry Cybersecurity Practices (HICP) – Medium & Large Healthcare Organizations,” HHS. https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Medium-to-Large-Organizations-OfficialDocument-R.pdf.
- “Free Cybersecurity Services and Tools,” CISA. https://www.cisa.gov/free-cybersecurity-services-and-tools.
- “Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats,” CISA. January 18, 2022. https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf.
- “6 Steps to Strengthen Your Security Posture,” Hyperproof. April 28,2022. https://hyperproof.io/resource/strengthen-security-posture/.
- National Security Agency. “Advancing Zero Trust Maturity Throughout the User Pillar,” Media.Defense.gov. March 14, 2023. https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_ZERO%20TRUST%20USER%20PILLAR.PDF.
- Davis, Jessica. “Most of the 10 largest healthcare data breaches in 2022 are tied to vendors,” SC Media. December 12, 2022. https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors.

Questions

FAQ

Upcoming Briefing

- 5/11 – North Korea and China Cybercrime Threats to the U.S. HPH

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV