Cyber Attacks and the Dark Web: Primer for Physicians

by James R. Rekowski, BS, Joseph T. Kannarkat, MD, Eric A. Packel, JD & Genevieve P. Kanter, PhD

The transition of medical record-keeping from paper charts to electronic health records (EHRs) has transformed clinical workflows, boosting physician productivity and enhancing patient care. However, dependence on EHRs and their integrated technologies—clinical reference guides, decision support, artificial intelligence (AI) prediction tools, and e-prescribing—have opened up new vulnerabilities. From covert theft of medical record data to paralyzing treatment and billing systems, cyberattacks can cripple health care institutions and threaten patient care.

James R. Rekowski, BS, (pictured), is a medical student at Ohio University, Heritage College of Osteopathic Medicine, Cleveland, Ohio, USA. Joseph T. Kannarkat, MD, MPP, is a resident in the Department of Medicine, Johns Hopkins University School of Medicine, Baltimore, Maryland, USA. Eric A. Packel, JD, is a partner with the Healthcare Privacy and Compliance Team, Digital Assets and Data Management Practice Group, Baker & Hostetler LLP, Philadelphia, Pennsylvania, USA. Genevieve P. Kanter, PhD, is an Associate Professor of Public Policy in the Department of Health Policy and Management, Sol Price School of Public Policy, and a Senior Scholar at the Leonard D Schaeffer Center for Health Policy and Economics, University of Southern California, Los Angeles, California, USA.

In this article, we offer a primer for physicians on cybersecurity, providing an overview of hacking and ransomware threats in health care, guidance for post-attack recovery, and practical advice for minimizing the risk of falling victim to cyberattacks.

Background

Ransomware Basics

Operating in an evolving technological landscape, hospitals, physician practices, and other health care delivery organizations (HDOs) face a growing threat of cyberattacks and other deliberate attempts to gain unauthorized access to computer systems and protected data. Ransomware is a particularly disruptive and costly type of cyberattack, in which attackers encrypt data, making the data inaccessible by the HDO without a special, digital key. Attackers will leave a "ransom note" with instructions on how to contact them and how to pay.

Encryption gives attackers leverage in demanding payment for decryption of the data. Many attacks involve a double form of extortion, in which a ransom payment, often in the form of cryptocurrency, is sought both to decrypt the data and to prevent protected health information (PHI) stolen during the attack from being publicly published by the threat actor. The payment through cryptocurrency is generally facilitated using a third-party intermediary and allows for the attacker to protect their own identity during the transfer of funds.[1]

Between 2010 and 2024, the annual number of patient records associated with large health care data breaches increased from six million to 170 million. In 2024, ransomware was shown to have been involved in incidents of 69% of affected patients.[2] Ransomware attacks have been posing serious cybersecurity threats to a range of industries—from energy and transportation to banking. However, the health care sector is unique in that health care data often includes sensitive health information as well personal financial information. Unlike credit cards or bank account information, personal health care information doesn't expire or change.

During a ransomware attack, with PHI encrypted by threat actors—and health information security teams forced to temporarily bring down systems to limit the spread of the ransomware—EHR systems, critical medication schedules, treatment status, or allergy information can become completely inaccessible, leading to life-or-death decisions. The urgent need to resolve these attacks places HDOs in a more vulnerable position than businesses in other sectors.

Threats to Health Care Organizations

As health care organizations face increasingly sophisticated threats, understanding the common cause of data breaches and ransomware incidents becomes crucial. In 2023, 80% of reported health care data breaches were from hacking or IT incidents.[3] These data breaches occurred at HDOs (hospitals, physicians), health plans (insurance companies, health maintenance organizations), business associates (companies that perform services for the organization including billing, cloud storage providers), and health care clearinghouses (organizations that process health information into standard formats).

Additionally, despite advances in security, phishing attacks remain prevalent and effective. Phishing attacks attempt to deceive employees into revealing sensitive information or downloading malicious software. Often, health care employees under typical work pressures are vulnerable to well-created deception sent by individuals who do not have authorized access.[4] A phishing email may appear to come from a hospital administrator requesting verification of login credentials. However, when that document or webpage is opened, ransomware is downloaded onto the device.

With the introduction of AI tools, sophisticated phishing campaigns are now targeting health care organizations. These modern AI systems can create personalized, convincing communications that may appear to come from someone within the organization. Traditional phishing attempts were easily exposed because of their frequent grammatical errors or stilted language. These new AI-crafted messages use appropriate language, organization-specific terminology, and can even mimic writing styles. This emerging technology allows attackers to create persuasive text, significantly increasing the likelihood that recipients will interact with the content. Also alarming is the development of "deep voice" technology, which can clone individuals' voices using small audio samples.[5] With this technology, attackers can use voice phishing, also known as vishing, to simulate calls from health care leadership, with the intent to deceive financial staff into transferring funds in response to urgent directives.

Threat Actors

Actors involved in these attacks fall into primarily state-sponsored groups, organized crime syndicates,

and, to a lesser extent, "lone wolf" hackers. State-sponsored actors are typically characterized by substantial resource backing and are driven by a variety of nation-state interests. Motives can include espionage and property theft, although financial gain is an important factor for countries known to be under international sanctions like Russia, China, North Korea, or Iran.[6] According to the 2025 Data Breach Investigations Report from Verizon, financial motivations were associated with 90% of all healthcare data breaches in 2024.[7]

In 2023, 80% of reported health care data breaches were from hacking or IT incidents.

Organized crime syndicates are another significant threat to the healthcare sector. These groups often benefit from either tacit approval of or lack of aggressive law enforcement against their activities in their country of origin. ALPHV/Blackcat, the group behind the massive cyberattack against Change Healthcare in 2024, is often characterized as an organized crime syndicate.

The traditional image of a "lone wolf" hacker, or an individual operating without affiliation to any group or country, is becoming less of a threat facing the healthcare sector. Though these actors undoubtedly still exist, most attackers are part of the larger organized groups described above. "Lone wolf" attackers may be motivated by notoriety, ideological reasons, or even simply the thrill of the intellectual challenge.

Fundamentals of the Dark Web

When health care data is stolen—through ransomware or other attack vectors—that data can often journey to hidden layers of the Internet that are invisible to the public. To fully appreciate this process, it is helpful to know the underlying structure of the Internet.

The Internet is divided into three distinct layers: the surface web, deep web, and dark web. Common daily Internet interactions such as shopping, reading news sites, posting on social media, and Google searches take place in the surface web, yet this represents only 4% of the entire Internet. The remaining 96% lies within the deep web and the dark web, layers that are not accessible through the standard search engines.[8] The deep web often requires passwords to access and is frequently used for secure commercial transactions. Some common websites are found within the deep web, including streaming services or banking sites.

The dark web describes a smaller, more notorious layer designed for anonymity, which hosts illicit marketplaces for stolen health care data, as well as terrorist activity and child pornography. The dark web is different from the surface web because it cannot be accessed by standard web browsers. The most common browser used to access the dark web is TOR (an acronym for "The Onion Router"). This system, formerly used by the United States Naval Research Laboratory for government communication, was made available to the public in 2002.[9] Data transmission on the dark web, through TOR, encapsulates data in multiple layers of encryption that creates a nearly untraceable communication system to protect user identity and location. Health care data stolen from ransomware attacks frequently appears for sale on dark web marketplaces precisely because these sites facilitate anonymous transactions.

Economics of Ransom Payments

When health care organizations fall victim to attacks, they face complex, difficult decisions that pose economic and ethical dilemmas. A central question facing these organizations is: pay the ransom or refuse?

To make this decision, organizations must first determine if the payment is even legally permissible. The Office of Foreign Assets Control (OFAC) prohibits transactions of any kind with entities on the Designated Nationals and Blocked Persons List (SDN LIST), or individuals that are covered by country or region embargoes. These organizations include terrorist organizations and their members, narcotics traffickers, and known arms dealers. Certain countries and regions identified to be involved in corruption are also included.[10] Organizations may face significant civil penalties from the US Treasury Department for making payments to these sanctioned actors, despite feeling under pressure to recover patient information.

Once that legal bar has been cleared, the decision may come down to whether the organization needs the data that was encrypted (for example, the attackers may have accessed only an old legacy system), or if the encrypted data can be restored. If organizations have a backup system in place that allows for data to be successfully restored, then the incentive to pay diminishes significantly. However, many modern ransomware actors today use a double extortion tactic. This means they not only encrypt critical data, but also exfiltrate ("steal") sensitive data, and threaten to publicly release the data if their ransom demands are not met.

This situation presents a dilemma in which, even with perfect backups, organizations may consider paying the threat actor to prevent patient information from appearing on dark web marketplaces. Regardless, paying the ransom does not guarantee that the data will not be leaked or sold in time. After all, if these ransomware actors are engaging in criminal activity and unwilling to abide by laws, there is no particular reason to think they would abide by any other agreement.

Moreover, once PHI has been accessed or acquired by an unauthorized third-party, a breach has occurred, per Health Insurance Portability and Accountability Act (HIPAA) regulations and state laws. Thus, payments made to prevent publication of PHI do not resolve the legal/compliance issues related to the breach. Organizations may still have legal obligations to notify patients and can still be investigated and penalized by regulators for the incident even if all data is restored and even if the data is not published on the dark web. Accordingly, a decision on whether to pay the ransom is typically driven primarily by business needs, such as whether decrypting the data is necessary to remain fully operational or to have access to critical data.

But why pay a criminal anyway—can they be trusted? Surprisingly, contrary to what may be expected from a criminal enterprise, ransomware actors do generally fulfill promises when payment is made. Groups operate as a business, protecting their "reputation" in these criminal circles and to healthcare organizations. If organizations did not receive the decryption key or tool after payment, then the ransomware business model would collapse as word would spread amongst organizations that paying yields no benefit. Only on rare occasions do actors not fulfill their promise—often demanding additional funds for full access to compromised records.[11]

Beyond the direct cost of the ransom itself, healthcare organizations frequently face indirect expenses that are just as significant, even if some of the costs are covered by cyber insurance. These include:

- Legal expenses regulated to incident response, potential class-action lawsuits, and regulatory fines and penalties.
- Forensic investigation costs to contain the incident, determine the root cause and scope of the attack.
- Recovery costs related to restoring and/or replacing systems subject to the attack.
- Long-term reputational damage affecting patient trust which may reduce future revenue for the organization.

The financial impact associated with the attack extends beyond this immediate crisis. Healthcare organizations experience elevated direct and indirect expenses, underscoring the necessity for prevention and preparedness for these attacks.

Assessment

Case Studies of Notable Attacks

In February 2024, Change Healthcare, a data processing firm owned by UnitedHealth Group was the victim of an attack by the ransomware group ALPHV/Blackcat.[12] This resulted in encryption and theft of the PHI of approximately 190 million individuals, the largest health care data breach ever reported. This attack resulted in significant disruptions in the processing of claims across the country, impacting both patients

and physicians. Lawsuits have been filed against UnitedHealth by both individuals who had their data compromised in the attack as well as providers who were affected by disruption to their revenue cycles.[13]

Other regional attacks have demonstrated similar patterns of disruption to health care operations and compromising of patient information. In Missouri, two hospitals have experienced large security breaches in recent years. In December 2023, a hospital in Liberty detected a disruption due to a cybersecurity attack, prompting it to take its computer network entirely offline and necessitating the transfer of high-need patients to other hospitals.[14]

In Kansas City, a second hospital experienced a significant breach through a phishing campaign. Links in an email directed employees to a website where they disclosed their credentials. With these exposed credentials, attackers were able to download the mailbox of these compromised email accounts, resulting in the unauthorized access of the PHI of more than 63,000 patients.[15] These incidents underscore how organizations with strong security infrastructure can still be vulnerable to breaches of patient data and the need for continuing employee cybersecurity and technology training.

Enforcement and Litigation

The US is actively pursuing perpetrators of health care cyberattacks. These international actors can be difficult to track down, but there have been some reported arrests and criminal charges. For example, in October 2024, two Sudanese nationals were indicted in a federal grand jury for a variety of cyberattacks against the US including against a hospital.[16]

On the other side, claims by patients in the wake of a breach of PHI are filed as class action lawsuits. These matters usually settle prior to formal adjudication. Settlements are frequently made to avoid the costs of litigation and discovery and are not necessarily indicative of valid claims. Plaintiffs face significant hurdles in data breach claims, including certification of the class and proof of actual damages or losses sustained as a result of the breach. In Federal court, Plaintiffs must have "standing" to proceed with a claim, demonstrating that the alleged facts show concrete harm, and not simply that their data has been accessed by an unauthorized party.

Guidance for Recovery Processes

Recovering from a ransomware attack or data leak requires a multifaceted approach that can extend over a long period of time. The initial response should focus on containment of the incident with temporary manual stop-gap measures (physically shutting down systems, disabling an account, or switching to paper records) to prevent further spread of attack in the system. Cyber insurance providers should be alerted, and legal and technical assistance should be engaged. The response typically involves isolation of affected systems, deployment of endpoint detection and response (EDR) tools, restoration of critical systems using secure backups, forensic investigation to determine details on the scope of the attack and file systems affected, and gradual reintegration of systems following security validation using EDR.

Clinicians and non-clinical staff should be made aware that system capabilities will likely not all be restored at once. The recovery process could take weeks or months, not days. As electronic capabilities return, there will be additional resource demands, as charts need to be reconciled, transferring information manually collected during the downtime to electronic format. Organizations must consider this extra burden on employees who also still need to perform their daily duties. Other available staff may need to assist with the high volume of data entry or determine that some manually recorded data will not being reconciled with the EHR for the time being.[17]

Upcoming Regulatory Change

With the technological landscape constantly evolving, the health care cybersecurity regulatory landscape is also constantly adapting. In early 2025, the Department of Health and Human Services (HHS) proposed updates to the HIPAA Security Rule to address the modern cybersecurity challenges faced by healthcare organizations. The Security Rule was first published in 2003, but had its last major modifications in 2013 as part of the "Omnibus HIPAA Final Rule."[18] The latest proposed modifications provide more clarity about many of the security requirements. For example, covered entities (i.e., HDOs, health plans) are required to encrypt ePHI, with limited exceptions, whereas previously, entities were able to assess whether the encryption was reasonable in their environment. This proposal would eliminate the need for entities to perform any analysis on whether encryption is reasonable and appropriate.

This proposed change to the Security Rule would provide 180 days for compliance after the effective date of the rule. HHS notes that many of

these processes should already be in effect given the current cybersecurity landscape, but security practices and procedures may need to be made more explicit internally.

There may, however, be different priorities or modifications to the originally proposed updates with the new administration and new leadership at HHS. See for example the recently announced Request for Information (RFI) from HHS, where "[HHS] is planning the largest deregulatory effort in the history of the Department."[19]

Recommendations for Providers

These recommendations apply to, not only clinicians, but also health administrators and other support staff working in HDOs and other health care organizations.

User education remains an extremely effective preventive measure. Regular training on identifying and reporting phishing emails should be provided to all staff members who work with PHI. The phishing scheme affecting a hospital in Kansas City, discussed in the Case Studies, is a good example of the importance of this type of education. One errant click on a link can compromise entire networks and affect thousands or millions of patients. Phishing simulation software tools are now available and should be used to train and test employees' response to phishing emails.

Several excellent off-the-shelf online training resources exist for organizations to support employee training. HHS is currently producing a series of "Knowledge on Demand" cybersecurity training videos that align with the top five cybersecurity threats mentioned in previous its Health Industry Cybersecurity Practice materials.[20] Certification courses such as those created by Coursera allow students to flexibly learn leadership and management strategies in cyberattacks and the importance of a positive cybersecurity culture.[21]

Health care providers should implement Multi-Factor Authentication (MFA) for access to systems and use an authorized organization-supported Virtual Private Network (VPN). MFA requires users to go through a second verification process beyond a password to access systems. This additional authentication uses a cellphone or other secondary device. With the increased use of remote work, VPNs are now regularly deployed to create secure connections to the organization's network from an outside location. The security ensured by VPNs can reduce unauthorized access.

Widespread utilization of AI tools for transcription and clinical support means organizations need to pay special attention to these systems and their processes for storing information. AI vendors, like other healthcare business associates, should be vetted for HIPAA compliance. Clear business associate agreements should define the proper use of patient information. These agreements, established between a covered entity (such as a provider, health plan, or clearinghouse) and a business associate (any person that performs functions with PHI) must legally bind the business associate on how they can use PHI, prohibit disclosures of data, and require data breach notifications. The health care organization needs to understand data retention defaults and evaluation or audit capabilities before using any AI tools that use patient data.

Healthcare organizations should implement advanced security software such as Endpoint Detection and Response, or EDR, tools. EDR systems monitor all network devices and can often detect suspicious behavior before the breach takes place in the first place. These tools can be a significant investment but provide necessary protection against cyber threats that are targeting health care data in increasingly sophisticated ways. EDR collects data from "endpoints" or system data, which is then analyzed in real time using advanced analytics and machine learning to identify potential threats. EDR is then capable of isolating the "endpoints" that may be infected by ransomware, preventing the spread to additional data.[22]

Every healthcare organization should have policies and procedures in place to comply with the HIPAA privacy and security rules. These include having an appropriate incident response plan. This plan should define roles, communication protocols, and standard operating procedures for recovery processes. Having a template ready for patient notifications and regulatory system reporting can save time if an actual breach were to occur. Providers should familiarize themselves with their designated roles, follow communication protocols, and understand recovery processes. They should be prepared to document accordingly and coordinate with IT security teams. Regular training sessions with incident response experts may help prepare providers to respond effectively when an actual breach occurs.

Health care professional associations and societies often offer resources around security practices that can be helpful for guiding clinicians in specific specialties. The American Medical Association published updated physician cybersecurity information in November 2024

which included information on recent cybersecurity incidents as well as guides for both large health systems and office practices for strong cybersecurity hygiene.[23] Other societies such as the American Academy of Family Physicians (AAFP) have proposed innovative ways of boosting cybersecurity efforts. In a 2023 report to Congress, the AAFP included several novel recommendations such as student loan forgiveness opportunities for cybersecurity professionals willing to work for healthcare organizations in under-resourced areas, whether rural or urban.[24]

Conclusion

The health care sector faces a critical moment in cybersecurity, with increasing sophistication of cyberattacks that threaten patient care and public organizational trust. Addressing these vulnerabilities requires technical safeguards as well as education and awareness to minimize the human role in data breaches. Potential upcoming changes to the HIPAA Security Rule reflect responsiveness to this growing risk and a recognition of cybersecurity as central to patient privacy protection. By implementing the recommendations outlined above, HDOs and other health care organizations can both prevent incidents from occurring in the first place and also be prepared and rise to these challenges if they do occur.

References

1. Ransomware Attack - What is it and How Does it Work? Check Point Software. Accessed June 10, 2025. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
2. Jiang JX, Ross JS, Bai G. Ransomware Attacks and Data Breaches in US Health Care Systems. JAMA Netw Open. 2025;8(5):e2510180-e2510180. doi:10.1001/jamanetworkopen.2025.10180
3. Most Common Types of Healthcare Data Breaches | Data Security. Definitive Healthcare. March 4, 2024. Accessed May 29, 2025. https://www.definitivehc.com/resources/healthcare-insights/most-common-healthcare-data-breaches
4.Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: threats, mitigation and approaches. BMJ Health Care Inform. 2019;26(1):e100031. doi:10.1136/bmjhci-2019-100031
5. Dangers of Deepfake: What to Watch For. Stanford University IT. February 22, 2024. Accessed June 1, 2025. https://uit.stanford.edu/news/dangers-deepfake-what-watch
6. Nation-State Threats. Cybersecurity and Infrastructure Security Agency CISA. Accessed June 11, 2025. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
7. Alder S. Verizon DBIR: Surge in Vulnerability Exploitation and Healthcare Espionage Breaches. The HIPAA Journal. April 23, 2025. Accessed June 11, 2025. https://www.hipaajournal.com/verizon-dbir-2025/
8. Kaur S, Randhawa S. Dark Web: A Web of Crimes. Wirel Pers Commun. 2020;112(4):2131-2158. doi:10.1007/s11277-020-07143-2
9. Tor Project. Accessed June 1, 2025. https://torproject.org
10. OFAC Specially Designated Nationals List - Sanctions List Service. OFAC Sanctions List Service. May 29, 2025. Accessed June 1, 2025. https://sanctionslist.ofac.treas.gov/Home/SdnList
11. Kansas Hospital Hit by Ransomware, Extorted Twice. Trend Micro (US). TrendMicro. May 23, 2016. Accessed June 10, 2025. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kansas-hospital-hit-by-ransomware-extorted-twice
12. Kanter GP, Rekowski JR, Kannarkat JT. Lessons From the Change Healthcare Ransomware Attack. JAMA Health Forum. 2024;5(9):e242764-e242764. doi:10.1001/jamahealthforum.2024.2764
13. Alder S. UnitedHealth Adopts Aggressive Approach to Recover Ransomware Attack Loans. The HIPAA Journal. April 16, 2025. Accessed June 1, 2025. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
14. Lagasse J. Cybersecurity incident hits Missouri hospital. Healthcare Finance News. Healthcare Finance. January 3, 2024. Accessed June 1, 2025. https://www.healthcarefinancenews.com/news/cybersecurity-incident-hits-missouri-hospital
15. Alder S. Children's Mercy Hospital Sued for 63,000-Record Data Breach. The HIPAA Journal. July 13, 2018. Accessed June 1, 2025. https://www.hipaajournal.com/childrens-mercy-hospital-sued-for-63000-record-data-breach/
16. US Department of Justice Office of the US Attorney of the Central District of California. Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World. United States Department of Justice. October 16, 2024. Accessed June 10, 2025. https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals
17. Healthcare System Cybersecurity. Published online October 2022. Accessed June 1, 2025. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf
18. HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. Federal Register. January 6, 2025. Accessed June 1, 2025. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
19. Request for Information (RFI): Ensuring Lawful Regulation and Unleashing Innovation To Make American Healthy Again. Federal Register. May 14, 2025. Accessed June 1, 2025. https://www.federalregister.gov/documents/2025/05/14/2025-08384/request-for-information-rfi-ensuring-lawful-regulation-and-unleashing-innovation-to-make-american
20. Health Industry Cybersecurity Practices. HHS 405(d) Aligning Health Care Industry Security Approaches. Accessed June 1, 2025. https://405d.hhs.gov/cornerstone/hicp
21. Cybersecurity in Healthcare (Hospitals & Care Centres). Coursera. Accessed June 1, 2025. https://www.coursera.org/learn/cybersecurity-in-healthcare
22. Endpoint Detection and Response (EDR) in Healthcare. Cynet. January 17, 2025. Accessed June 1, 2025. https://www.cynet.com/endpoint-protection-and-edr/edr-in-healthcare/
23. Physician cybersecurity. American Medical Association. April 30, 2025. Accessed June 1, 2025. https://www.ama-assn.org/practice-management/sustainability/physician-cybersecurity
24. Congress Gets Detailed Cybersecurity Advice From AAFP. American Academy of Family Physicians. January 11, 2023. Accessed June 1, 2025. https://www.aafp.org/news/government-medicine/cybersecurity-safety-advocacy.html

Disclosure

No financial disclosures reported. Artificial intelligence, language models, machine learning, or similar technologies were not used in the conceptualization, study, research, preparation, or writing of this manuscript. **MM**