HealthHacks: Addressing Increasing Cyberattack Incidences on American Healthcare

Nikki Jiang

10 Dec 2025

Defining the Problem

Increased reliance on technology and computer systems have transformed the healthcare industry through transitions to electronic medical records (EMRs), telehealth platforms, and artificial intelligence. While these digital solutions have streamlined administrative processes, increased convenience, and expanded the reach of healthcare delivery, they also introduce risk of vulnerability to malware and cyberattacks. Categorized as any “purposeful, malicious attempt to breach healthcare data, compromise patient confidentiality, or disrupt operational systems” (Neprash, 2025), cyberattacks pose an imminent threat to public health and national security that must be addressed through a multi-sectoral and government regulated approach.

The healthcare industry has been the number one target of cybercrime for years according to the American Hospital Association (AHA), due to its critical role in national infrastructure and direct access to sensitive data with personally identifiable information. Additionally, a majority (80%) of stolen health records were outside of hospital settings, with hackers mainly targeting third-party vendors such as health plans, software services, and business operations systems. Through a multi-targeted approach, cyberattacks on healthcare systems hold the potential to cause medical equipment malfunction, hinder lab testing, deliver false reports, and compromise patient confidentiality laws. Due to the complex interdependent network of EHR transport amongst third-party providers, health care organizations, service lines, etc, data breaches become difficult to monitor and control. The problem is further complicated by the influx of foreign hackers, making it difficult to track down origins of the breach and ensure adequate consequences are enforced.

Incidence rate of cyberattacks continue to increase annually, with the number of healthcare breaches (1 incidence defined as break of 500+ records) doubling from 2018 to 2020 (Li, 2025). In 2024 alone, 259 million Americans protected health information were hacked according to the AHA. The situation continues today with 364 hacking incidents reported to the US Department of Health and Human Services Office as of Oct. 3, 2025. While current data

breaches have been on smaller scales compared to the UnitedHealth Group/Change Health attack in 2024, the AHA warns that the current numbers are “still far too high and should not be tolerated as the norm”. Thus, it is crucial to address the threat cyberattacks pose on Americans through government and cybersecurity intervention.

Background & History

In February of 2024, United Healthcare’s subsidiary service, Change Healthcare, was the target of a large-scale cyberattack by the Russian group ALPHV BlackCat. This attack disrupted health care operations across the country, delaying authorization for medically critical care, causing significant financial losses, and threatening the stability of the provider network.

Change Healthcare is a revenue and payment processing system responsible for processing 1 in every 3 patient records (AHA). Its main functions include insurance eligibility verification, claims payments, and drug prescriptions, thus its disruption had a significant impact on the care delivery and financial processes for patients, providers, and communities. In a survey of 1,000 hospitals, 74% reported direct patient care impact and 94% reported financial impacts as a result of the cyberattack. Furthermore, 190 million individual patient data were exposed during this attack, violating the HIPPA rights of over ⅓ of the US population (Neprash, 2025). A January 2025 report from UnitedHealth Group announced a total loss of $3.09 billion in 2024 due to cyberattacks. A large portion of the loss is attributed to ransom payments. Therefore, it is also important to note that despite paying the ransom, there still remains significant risk of data continuing to circulate the dark web according to the CEO of UnitedHealthcare, Andrew Witty.

More recently in November 2025, the FBI and HHS, along with other governmental agencies, issued a joint advisory on another ransomware gang, Akira Ransomware, on its accelerated attacks on critical infrastructure including within the healthcare industry. They mainly operate through brute force double extortion on private networks without multi-factor authorization, stealing and encrypting data through remote access tools then demanding payment to prevent the publication of the stolen data on leaked sites (HIPPA Journal). Cybercrimes are highly financially motivated, with each patient record worth up to $50 on the black market and a full set of records worth up to $1000 (Wasserman, 2022). According to the FBI's cyber division, Akira has claimed $244 million in ransoms since late September 2025. Lastly, these cybercriminal groups often target major cloud computing grids, leading to the entire collapse of internet systems. In October, the FBI issued an emergency warning to hospitals, alerting a security vulnerability within Oracle’s E-Business Suite, an integrated management

application used by most major businesses across all industries totalling millions of users. Not only do cyberattacks significantly impact quality of care and lead to financial damages for healthcare providers, but they also indirectly impact the entire American population.

In order to mitigate the financial impacts, government organizations such as Centers for Medicare & Medicaid Services (CMS) provided relief funding, costing billions of taxpayer dollars, yet this band-aid solution only addresses the immediate crisis rather than underlying system vulnerabilities. Despite relief funding, many hospitals continued to experience delays in patient billing, workforce shortages, and revenue disruption, illustrating the deeply disabling impacts of cyberattacks even given the deployment of short-term relief programs.

Root Causes

Through examining the Change Healthcare incidence of 2024 and overall trends within the healthcare industry, increasing cyberattacks on the US healthcare system can be separated into 2 categories of root causes: 1) technological immaturity 2) gaps in government oversight.

In a report by *Kroll* on the State of Cyber Threats in Healthcare, only 3% of healthcare industries have mature, or complex, cybersecurity features beyond basic monitoring (2024). The attack on Change Healthcare is a clear example of technical cyber immaturity. Experts, along with the CEO of UnitedHealth named an absence of multi-factor authentication (MFA), to be the root cause. Despite being an industry standard this security measure was not implemented by United Healthcare, one of the largest EHR networks in the nation. This issue is widespread amongst the entire industry with over 26% of healthcare organizations having low security maturity, lacking all recommended threat detection capabilities.

This troubling reality raises a fundamental question: how has one of our most private and essential industries been allowed to remain so vulnerable? Firstly, Kroll's survey of over 1000 healthcare organizations found that healthcare is the most likely industry to self-report as having high security maturity level. Respondents within healthcare scored 16 points higher than the survey average in self perception of security. They were also found to be most likely to believe that "absolutely zero improvements are needed" to improve security. This self-diagnosis gap leads to inaccurate solution provisioning and risk assessments, both key steps in ensuring a cybersecure system. Lastly, survey respondents reported a low concern for ransomware, zero-day attacks, and supply chain compromises, opting to focus on credential access instead. While it should be ensured that patient credentials such as usernames and passwords are protected, there must be equal concern regarding larger scale attacks such as ransomware as they hold potential for far-reaching consequences, as seen in the Change Healthcare attack.

According to the U.S.Government Accountability office (GAO), HHS has experienced gaps in providing cybersecurity support. Despite launching several initiatives to mitigate ransomware attacks on public health and healthcare organizations, the department fails to adequately monitor implementation. Without accountability measures and awareness of regulation adoption levels, HHS risks not directing resources where necessary. Additionally, a lack of support for non-medical IT leaves the remainder of the healthcare system vulnerable. Operational technology devices and systems are neglected, resulting in a lack of knowledge regarding essential additional security measures (GAO). It is this same failure to correctly assess need that led financial assistance programs following the Change Healthcare breach to overfund certain hospitals while leaving others without sufficient support (Neprash, 2025).

With MFA being an established security measure for preventing unauthorized access and widely considered as industry standard, it is not explicitly mandated under the HIPPA security rule. Currently, HIPPA requires “reasonable and appropriate” authentication measures to safeguard protected health information (HIPPA Journal), leaving implementation methods up for individual interpretation.

Such oversight gaps create a fragmented security structure in which healthcare systems are left to interpret federal regulations on their own, without technical expertise or sufficient funds. As a result, cybersecurity practices dramatically vary within the industry. Under the absence of HHS monitoring, and therefore enforceable standards with consistent federal follow-through, healthcare organizations have little incentive to adopt robust preventative security measures. This then enables cybercriminals to exploit predictable weaknesses that are otherwise preventable, leading to nationwide risks on individual and organizational levels.

Proposed Solutions

In addressing cybersecurity threats on the American healthcare system, we must also emphasize a two-pronged approach through prevention and risk control. Additionally, there must be efforts for increased multi-sectoral and public private partnerships to provide both technical solutions and policy changes.

First, prevention programs implemented through public-private partnerships must be expanded across the country, equipping hospital systems with the expertise and tools to regularly maintain their networks. Following the 2024 ALPHV attack on Change Healthcare, the AHA cybersecurity and risk advisory team along with Microsoft developed joint solutions as part of a Rural Health Reliancy program. They offered free and discounted cybersafety measures for rural critical access and emergency hospitals to prevent future cyberattacks. This program

included services such as cybersecurity assessments, cloud capability evaluation, cyber and AI training, and certifications for rural hospital IT staff (AHA).

Building on this model, the Rural Health Reliancy program demonstrates how strategic public-private collaboration can strengthen security under even resource limited settings. To further reduce national vulnerability, this partnership model should be expanded into a federally supported cybersecurity safety-net for all American hospital systems. Through leveraging the technical expertise of industry actors such as Microsoft and the regulatory authority of government agencies, this expanded framework would result in consistent defensive capability across every hospital.

Next, policy reforms must strengthen risk management mechanisms through instating baseline federal regulations through HHS and HIPPA and establishing federal funding streams to relieve the financial burdens of cyberattacks. Such programs would close gaps in cybersecurity preparedness, holistically protecting the US healthcare system. Policy reforms must emphasize strengthening federal oversight through clearly defining and enforcing baseline security standards across the industry. One crucial step is to mandate MFA for e-health information systems through HIPPA requirements, leaving little room for interpretation on what measures qualify as “reasonable and appropriate”. By mandating MFA, federal organizations eliminate the current ambiguity that promotes technological immaturity.

A model of financial support can be seen in the CMS Change Healthcare/Optum Payment Disruption (CHOPD) program, established to alleviate provider financial strain. This program provided $3.3 billion from March to July 2024 with $2.55 billion to Medicare part A providers and $717.8 million to part B providers (Neprash, 2025). While this program was shut down in 2024, we should examine its strengths and weaknesses to develop a long-term sustainable cybersecurity fund to support healthcare organizations in establishing mature cybersecurity measures and reduce financial burdens of ransomware attacks. The program was successfully able to reduce financial damages for hospital systems across the country, particularly in rural communities. The scale and reach of CHOPD should be modeled in future cybersecurity financial assistance programs. However, any long term strategy must avoid its shortcomings, whose opt-in structure left many hospitals without urgently needed support. Establishing baseline funds accessible to all rather than through a voluntary enrollment process eliminates the potential to omit systems most in need.

Conclusion

The continued escalation of cyberattacks on American healthcare systems underscores an urgent national concern: our most essential and data-rich industry remains vulnerable to criminal and dark web access. As healthcare increasingly depends on interconnected digital platforms, possible points of attack expand, exposing payers, providers, and entire systems to threatening breaches. The consequences have already proven to be destructive, costing billions of dollars of damage for individual systems and American taxpayers. Change Healthcare's historic cyberattack highlighted the importance of cybersecurity in healthcare, ensuring financial stability, privacy of patients, and quality of care. Current vulnerabilities stem from systemic gaps in preventative measures and regulatory oversight. Moving forward, a cohesive national cybersecurity strategy must be established and grounded in clear regulations, consistent auditing, and financial support. Additionally, HIPPA must strengthen its protection of patient privacy to prevent cyberattacks. Through mandating MFA in e-health records, all healthcare organizations will have a clear baseline on how to protect data. Lastly, to provide direct technical support to healthcare systems, the U.S. must invest in public-private partnerships that expand successful initiatives such as the AHA-Microsoft Rural Health Reliancy program nationwide, offering hospitals ongoing support, monitoring and rapid incidence response.

Through combining security standards with technical capabilities, U.S. health systems can transition from crisis management and recovery to proactive resilience. It must be a public health and national security priority to protect our hospitals, data, and the health of Americans.

Works Cited

2025 cybersecurity year in Review, part One: Breaches and defensive measures: Aha News. American Hospital Association | AHA News. (2025, October). http://aha.org/news/aha-cyber-intel/2025-10-07-2025-cybersecurity-year-review-part-one-breaches-and-defensive-measures

Aguila, B. (2025, August 20). *Healthcare multi-factor authentication (MFA) & HIPAA: Protecting Patient Data*. Network Innovations. https://networkinnovations.us/strengthening-healthcare-cybersecurity/#:~:text=For%20healthcare%20organizations%2C%20MFA%20ensures,systems%20may%20require%20custom%20setup

Alder, S. (2025, November 14). *Warning issued about Akira ransomware as attacks on Critical Infrastructure Accelerate*. HIPPA Journal . https://www.hipaajournal.com/akira-ransomware-advisory-nov-2025/

Change healthcare cyberattack underscores urgent need to strengthen cyber preparedness for individual health care organizations and as a field: AHA. American Hospital Association. (2025, January). https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and

Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-attacks on Hospital Systems: A narrative review. *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*, *7*, 30–39. https://doi.org/10.1016/j.osep.2025.03.002

Neprash, H. T., Beebe, T. J., Yost, G., & Carroll, C. (2025). Lessons from CMS relief funding after Cyberattack on Change Healthcare. *Health Affairs*, *44*(12), 1466–1472. https://doi.org/10.1377/hlthaff.2025.00990

Office, U. S. G. A. (2024, November). *Healthcare Cybersecurity: HHS continues to have challenges as lead agency*. Healthcare Cybersecurity: HHS Continues to Have Challenges as Lead Agency | U.S. GAO. https://www.gao.gov/products/gao-25-107755#:~:text=HHS%20has%20several%20initiatives%20intended,not%20directing%20resources%20where%20needed.

The State of Cyber Defense: Diagnosing Cyber Threats in Healthcare. (2024, April 14). https://www.kroll.com/en/insights/publications/cyber/state-cyber-defense-healthcare

The State of Cyber Defense: Diagnosing Cyber Threats in Healthcare. Kroll. (2024, April). https://www.kroll.com/en/insights/publications/cyber/state-cyber-defense-healthcare

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*. https://doi.org/10.3389/fdgth.2022.862221

What we learned: Change healthcare cyber attack. House Committee on Energy and Commerce. (2024, May 3). https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack