Zyron Sumulong

Professor Nasreen Arif

CS 462 Cybersecurity Fundamentals

30 November 2025

The 2024 Change Healthcare Cyberattack

Introduction

In recent years, healthcare has become one of the most targeted sectors for ransomware. In 2024, there were 181 confirmed ransomware attacks, affecting healthcare companies, like Change Healthcare (Alder). On February 21, 2024, the United States experienced one of the most significant cybersecurity incidents when Change Healthcare, a major healthcare technology provider and subsidiary of United Health group, was targeted in a ransomware attack. Change Healthcare plays a critical role in processing healthcare transactions, insurance claims, pharmacy prescriptions, and medical billing for millions of Americans. “Change Healthcare processes about half of all medical claims in the United States for approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories” (Robb). When the attack happened, it shut down vital systems nationwide and exposed sensitive data of nearly 190 million Americans. This breach quickly became one of the largest healthcare data compromises in American history. This incident highlights not only the dangers of poor cybersecurity practices but also the vulnerabilities created when an entire company relies heavily on centralized systems and networks.

Change Healthcare became a vulnerable target because of its influential joint infrastructure. The attack "disrupted health care operations on an unprecedented national scale, endangering patients' access to care, disrupting critical clinical and eligibility operations, and threatening the solvency of the nation's provider network" (American Hospital Association). Hospitals, clinics, and pharmacies rely on its systems to conduct services such as insurance verification, claims processing, and payment distribution. Rather than maintaining their own software systems, many healthcare facilities utilize Change Healthcare's centralized structure. This setup includes remote management tools, file transfer protocols, access portals, cloud infrastructure, and databases containing protected health information. While such centralized structures can increase efficiency, they also magnify the consequences if an attacker gains access to the network. The 2024 breach demonstrated how a compromise in one organization can rapidly affect thousands.

Attack Vector and How the Breach Occurred

The attack began when the Russian ransomware group BlackCat gained access to a remote-access system utilizing stolen credentials, resulting in being "the most significant and consequential cyberattack against the U.S. healthcare system in history" (Robb). A major contributing factor was the lack of multi-factor authentication, a basic cybersecurity control that could have prevented unauthorized entry even if credentials were compromised. Once the attackers accessed the system, they remained in the network for "nine days moving laterally through the network, exfiltrating data, and preparing for the ransomware deployment" (Robb). This group used tools to increase privileges, extract credentials, and explore network pathways. The attackers then encrypted Change Healthcare's systems, and the company was forced to

disconnect most of their systems to prevent further impact, resulting in a pause on health care services. The weaknesses in Change Healthcare's monitoring systems meant the attackers' activity went undetected, allowing them to access sensitive databases, internal servers, and networks without interruption.

Impact of the Attack

Before installing ransomware, the attackers exfiltrated large volumes of patient data. This method is known as double extortion, which allows attackers to retain the stolen data and threaten the public if future demands are not met. The data stolen reportedly included names, Social Security numbers, diagnoses, treatment histories, insurance claims, and financial account information. Protected health information cannot be altered, and exposure of these records poses long-term risks to patients, including identity theft, fraudulent billing, and misuse of medical information. "This attack made it harder for hospitals to provide patient care, fill prescriptions, submit insurance claims, and receive payment for the essential health care services they provide" (American Hospital Association).

After Change Healthcare attempted to recover its systems, the attackers continued to claim that they still possessed 6TB worth of stolen data. When the ransomware was deployed, its impact was immediate and widespread. Pharmacies across the country were unable to process insurance claims, which forced many patients to pay out of pocket or delay essential medications. Hospitals struggled to verify insurance coverage, submit claims, and/or receive reimbursements, leading to severe financial stress. According to surveys conducted after the incident, almost 95 percent of hospitals experienced financial harm, and many smaller and rural hospitals faced the possibility of closure due to financial ruin. About 74 percent of patients were

affected most directly through “delays in authorizations for medically necessary care” and “94 percent reported the attack impacted them financially” (American Hospital Association). To lessen the likelihood of the sensitive data being leaked, CEO of United Health Group, Andrew Witty confirmed that the company paid the ransom of $22 million in bitcoin to the BlackCat group (Robb). It has been reported that 192.7 million individuals have been impacted by the breach and the cost of the attack has risen to $2.457 billion. The devastating disruptions presented immediate financial repercussions and revealed how vulnerable digital health systems can be. This incident demonstrated that even organizations with significant resources are susceptible to cyber attacks and that even one vulnerability can impact a large number of Americans. Understanding these impacts is essential for identifying systemic weaknesses and improving cybersecurity practices across the healthcare industry.

Analysis: Lessons for Modern Cybersecurity

Beyond operational disruptions, this breach revealed systemic weaknesses in the U.S. healthcare infrastructure. This attack showed how heavy reliance on a few technology vendors can create multiple vulnerabilities that threaten an entire nation. It also raised concerns about regulatory oversight and the need for organizations handling protected health information to comply with the Health Insurance Portability and Accountability Act. The scale of the breach drew significant federal attention, with many calling for stronger cybersecurity standards among healthcare vendors. The attack also highlighted how advanced ransomware groups increasingly use double extortion to increase their leverage against victims.

As society continues to rely on digital infrastructure for healthcare, the growing number of vulnerabilities in these technologies has significant implications for both the quality and

access to care for patients. Hospitals and clinics are severely impacted when centralized systems fail, leaving them unable to process insurance claims, verify patient eligibility, or provide timely treatment. As a result of failures in the central system, many patients experience disruptions in receiving necessary care, delayed care, and potential financial harm due to the compromise of both personal and medical information. Additionally, the continued failure of an organization's security systems to protect its data will continue to diminish public trust in healthcare organizations, leading individuals to be hesitant to engage fully with healthcare technology. Therefore, it is evident that cybersecurity is not simply a technical issue but rather a fundamental part of delivering healthcare services, where the failure of an organization's security system can have far-reaching impacts affecting millions of patients and thousands of healthcare providers throughout the country.

Mitigation Strategies and Cybersecurity Improvements

The Change Healthcare attack plays a significant role in cybersecurity practices today. It reinforces the importance of foundational security measures such as multi-factor authentication and network segmentation, where the initial compromise could have been prevented by implementing stronger authentication requirements. The attack highlighted the importance of continuous monitoring, behavior-based analytics, and rapid incident response, because when attackers can move freely within a system for days or weeks, the likelihood of data theft and operational disruption increases exponentially. Organizations that store large volumes of sensitive information should design their cybersecurity strategies with resilience in mind and prepare for the possibility that systems will be breached.

The Department of Health and Human Services has proposed the first major update to the HIPAA Security rule. The role of the HIPAA security rule is to ensure healthcare organizations implement policies and procedures to ensure that electronic health information is secured from unauthorized access. The updates include: the use of multifactor authentication, data encryption, network segmentation, vulnerability scanning twice a year, and penetration testing once a year (Alder). These updates will aid in addressing modern cybersecurity threats and strengthen the resilience of healthcare organizations. By complying with the newly updated HIPAA Security rule, healthcare organizations can better protect sensitive patient information and ensure the continuity of critical health services.

Conclusion

The 2024 Change Healthcare cyberattack remains one of the most damaging breaches in American healthcare network history. Through a single vulnerability, attackers infiltrated a system supporting millions of Americans and thousands of healthcare providers. This attack disrupted medical operations, caused financial hardships, and exposed sensitive data on a massive scale. As a cybersecurity student, this breach highlights the importance of proper protection, the risks of centralized systems, and the need for effective cybersecurity strategies. When healthcare infrastructure is compromised, the effects go beyond financial stress; they also impact patient care quality and the trust people have in these services.

Furthermore, this breach clearly shows the urgent need for healthcare organizations to prioritize cybersecurity in their operational planning. Implementing multi-factor authentication, network segmentation, encryption, and continuous monitoring will be essential to safeguard patient data, maintain care continuity, and comply with the HIPAA Security Rule. This incident should serve as a wake-up call for the healthcare industry to adopt a proactive, adaptable

cybersecurity approach within its digital health systems. By learning from this event and developing strong protective measures, healthcare organizations can better detect, respond to, and prevent future threats.

References

Alder, Steve. “2024 Was Another Bad Year for Healthcare Ransomware Attacks.” The HIPAA Journal, www.hipaajournal.com/2024-was-another-bad-year-for-healthcare-ransomware-attacks/. Accessed 30 Nov. 2025.

Alder, Steve. “HHS Proposes Strengthened HIPAA Security Rule.” The HIPAA Journal, www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/. Accessed 1 Dec. 2025.

“Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field.” American Hospital Association, Jan. 2025, www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and.

Robb, Brenda. “The Change Healthcare Ransomware Attack: A Landmark Cybersecurity Breach.” BlackFog, 25 July 2025, www.blackfog.com/change-healthcare-landmark-cybersecurity-breach/.