Courtney Swink
CS462 Blog

Change Healthcare Data Breach: The Largest Breach of Health Care Data Ever Recorded

A common exploit, ransomware which is a type of malware, where attackers gain access to a company's network and plant malicious encryption software. They usually also take copies of the data to use the threat of leaking it. The malware is then activated, which usually locks devices and encrypt files, essentially locking them with a digital key that only the attackers have. A notification usually shows up on the screens of these devices, making the demand for ransom and how to make payment in exchange for the encryption key that will unlock and allow access to devices and data. The payment demand is usually to be made to an anonymous website and often in cryptocurrency.

Change Healthcare is a healthcare clearinghouse, which acts as a third party or middleman to healthcare providers and insurance companies, processing and transmitting patient medical claims, managing pre-authorizations, and verifying coverage for an estimated fifteen billion medical claims a year. This represents almost forty percent of all medical claims. In February 2024, Change Healthcare fell victim to a ransomware cyberattack, and as such, "has notified approximately one hundred million Americans"[1] that their personal information has been compromised. This is almost one-third of the United States population, making it the largest ever known breach of protected health information at a HIPAA-regulated entity. When Change Healthcare, a subsidiary of UnitedHealth, discovered someone had infiltrated their Citrix server, they disconnected their systems, taking it offline. This created a disastrous domino effect for financial operations because of unpaid claims in hospitals, pharmacies, and doctor's offices. Additionally, some insured patients were not able to fill prescriptions or had to pay for the prescriptions themselves out of pocket. The BlackCat/ALPHV ransomware gang claimed responsibility for the attack and depending on the source, is said to have stolen between 4 to 6 terabytes of information, including names, birthdates, addresses, patient Social Security numbers, medical records, diagnoses, imaging and care treatment plans, banking information and information on active military personnel. Although it has not been confirmed, somewhere around March 1, 2024, UnitedHealth is said to have paid BlackCat $22 million payment in bitcoin for the decryption key, and the prevention from the stolen data from being published online. Despite the unconfirmed payment made to BlackCat, which allegedly pulled an exit scam, which is when hackers close down and take the ransom money, leaving breached data in the hands of their affiliate partners, but not paying them any of the ransom money, proving that the old sentiment that there is no honor among thieves true. In a "ransomware-as-a-service (RaaS) such as this, 80% of the proceeds go the affiliate responsible for the intrusion and data theft, and 20% to the ransomware operators who provide the malicious code, infrastructure, and are responsible for negotiating with the victims."[2] A fake law enforcement notice appeared on the BlackCat/ALPHV site, attempting to make it look as though they had been shut down. A couple of days later, on March 3, 2024, a BlackCat/ALPHV affiliate posted to the Russian language ransomware forum, Ramp, that BlackCat/ALPHV never paid him his share of the ransom. This led to the BlackCat/ALPHV affiliate to presumably join a different, relatively new ransomware group, RansomHub, and demanding another ransom payment from Change

---

[1]Matt Kapko, "Change Healthcare's Drawn-out Recovery Catches Flak from Cyber Experts," Cybersecurity Dive, March 21, 2024, https://www.cybersecuritydive.com/news/change-healthcare-drawn-out-recovery/710995/.

[2] Ionut Arghire, "Second Ransomware Group Extorting Change Healthcare," SecurityWeek, April 9, 2024, https://www.securityweek.com/second-ransomware-group-extorting-change-healthcare/.

Healthcare. RansomHub showed up in February 2024 and has "made over a dozen victims."[3] Some speculate that the large payment made quickly by UnitedHealth, led the cyber attackers to believe that the company will pay again to keep the information from being leaked, however considering that the initial payment did not work, essentially leaving the affiliate with the stolen data, bitter as to not receiving any payment, it is assumed that paying the second ransom would also not do much good. The vulnerability exploited by the attackers was a result of compromised credentials and according to UnitedHealth CEO Andrew Witty, "UnitedHealth not using multifactor authentication (MFA)"[4], in one or more of their critical system servers. UnitedHealth had acquired Change Healthcare, an older company with older technologies, at the end of 2022, and apparently UnitedHealth had been working to upgrade the legacy systems.

The fallout from a breach like this, considering just how many healthcare providers large and small affected, on March 1, 2024, Optum provided a temporary assistance program in an attempt to help providers that are having cash flow issues as a result of the attack. However just three days later, the American Hospital Association (AHA) surmises that "Change Healthcare's temporary funding program deficient" and the "Senate asks that Change Healthcare speed up payments to hospitals, since large health systems can lose more than $100 million a day due to interruptions."[5] It was not until mid-March that Change Healthcare's system that processes electronic payments was back up and running, with UnitedHealth declaring that they have paid out $2 billion in advances to providers and will be introducing new software in order to speed up the claims process. Despite the efforts in advance payments, loans, and temporary funding assistance, according to a survey that was conducted by the American Medical Association (AMA), the financial impact of some physician practices declare just how dire the situation is, with some stating between $50,000-$100,000 in extra costs, some using personal funds to keep practice open, and others on the verge of bankruptcy.

Due to the enormity of this ransomware breach, the Office for Civil Rights (OCR) at the Department of Health and Human Services, the U.S. department that administers and enforces the Health Insurance Portability and Accountability Act (HIPAA), initiated an investigation as to HIPAA compliance in mid-March. HIPAA establishes the minimum privacy and security requirements for all protected health information. Well before the attack, Change Healthcare earned HITRUST certification for its enterprise infrastructure. This certification solidifies compliance in key regulations and industry requirements. HITRUST is a cybersecurity institution that focuses on privacy, security, and risk management by implementing its Common Security Framework (CSF) as a certifiable standard in the healthcare industry and the means to achieve HIPAA compliance. Organizations are usually quick to embrace the HITRUST framework given that "only 0.64% of environments certified by HITRUST reported experiencing a data breach."[6]

---

[3] (Ionut Arghire, "Second Ransomware Group Extorting Change Healthcare," SecurityWeek, April 9, 2024, https://www.securityweek.com/second-ransomware-group-extorting-change-healthcare/.

[4] Cathy M. Rodgers, "What We Learned: Change Healthcare Cyber Attack," House Committee on Energy and Commerce, May 3, 2024, https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

[5] Hyperproof Team, "Understanding the Change Healthcare Breach and Its Impact on Security Compliance," Hyperproof, April 25, 2024, https://hyperproof.io/resource/understanding-the-change-healthcare-breach/.

[6] HITRUST, "HITRUST's Inaugural Trust Report Sets New Industry Standard for Cybersecurity Assurances and Information Risk Reduction," Hitrustalliance.net (HITRUST, April 15, 2024), https://hitrustalliance.net/press-releases/hitrusts-inaugural-trust-report-sets-new-industry-standard.

It is irrational to think that any cybersecurity approach is flawless, considering that new threats emerge and evolve. Despite HITRUST's framework gold standard status, it begs the question on how elite it really is given the magnitude of this security failure, paired with the obvious lack of cybersecurity disaster recovery plan, considering it is a critical part of HIPAA compliance. When most people think of cybersecurity, the first thought is usually prevention and detection, however with the evolution of actors and threats, backup, response, and recovery should make its way up the list. Four weeks after the discovery of the ransomware attack, most of Change Healthcare's critical infrastructure remained down, with only "twenty services resuming operations, and more than one hundred and ten remaining offline."[7] According to The HIPAA Journal's latest update, released November 19, 2024, Change Healthcare announced "that all services have been fully restored following its ransomware attack 9 months ago."[8]

The latest reports have raised the estimated total cost of the Change Healthcare data breach to "nearly $2.9 billion for the fiscal year, with the actual cost thus far is $2.5 billion, which is what the company predicted in July to be the total cost for the year."[9] This does not include the possibility of fines, as Change Healthcare has not been publicly fined however the maximum penalty could be roughly $2.1 million for noncompliance of HIPAA regulations.

The significant impacts on society as a result of the Change Healthcare data breach have already caused major disruptions to patients and providers. It could potentially result in widespread identity theft, financial fraud, and interruption to access healthcare, not to mention the deterioration of trust in healthcare data security.

---

[7] Matt Kapko, "Change Healthcare's Drawn-out Recovery Catches Flak from Cyber Experts," Cybersecurity Dive, March 21, 2024, https://www.cybersecuritydive.com/news/change-healthcare-drawn-out-recovery/710995/.

[8] Steve Alder, "UHG: Substantial Proportion of US Population May Be Affected by Change Healthcare Cyberattack," HIPAA Journal, November 19, 2024, https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

[9] Marianne K. McGee, "Change Healthcare Attack Cost Estimate Reaches Nearly $2.9B," Bankinfosecurity.com, 2024, https://www.bankinfosecurity.com/change-healthcare-attack-cost-estimate-reaches-nearly-29b-a-26541.

Bibliography

"Change Healthcare Breach Hits 100M Americans – Krebs on Security." 2024. Krebsonsecurity.com. October 30, 2024. https://krebsonsecurity.com/2024/10/change-healthcare-breach-hits-100m-americans/.

Ionut Arghire. 2024. "Second Ransomware Group Extorting Change Healthcare." SecurityWeek. April 9, 2024. https://www.securityweek.com/second-ransomware-group-extorting-change-healthcare/.

Rodgers, Cathy M. 2024. "What We Learned: Change Healthcare Cyber Attack." House Committee on Energy and Commerce. May 3, 2024. https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

Team, Hyperproof. 2024. "Understanding the Change Healthcare Breach and Its Impact on Security Compliance." Hyperproof. April 25, 2024. https://hyperproof.io/resource/understanding-the-change-healthcare-breach/.

HITRUST. 2024. "HITRUST's Inaugural Trust Report Sets New Industry Standard for Cybersecurity Assurances and Information Risk Reduction." Hitrustalliance.net. HITRUST. April 15, 2024. https://hitrustalliance.net/press-releases/hitrusts-inaugural-trust-report-sets-new-industry-standard.

Kapko, Matt. 2024. "Change Healthcare's Drawn-out Recovery Catches Flak from Cyber Experts." Cybersecurity Dive. March 21, 2024. https://www.cybersecuritydive.com/news/change-healthcare-drawn-out-recovery/710995/.

Alder, Steve. 2024. "UHG: Substantial Proportion of US Population May Be Affected by Change Healthcare Cyberattack." HIPAA Journal. November 19, 2024. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

McGee, Marianne K. 2024. "Change Healthcare Attack Cost Estimate Reaches Nearly $2.9B." Bankinfosecurity.com. 2024. https://www.bankinfosecurity.com/change-healthcare-attack-cost-estimate-reaches-nearly-29b-a-26541.