Managing Vendor Risk: Lessons Learned After the Change Healthcare Breach

By Brian Johnson

The healthcare sector was dealt another blow on February 21, 2024, when Change Healthcare, a division of Optum and a subsidiary of UnitedHealth Group Incorporated, fell victim to a cyberattack. The company disclosed that the attack compromised customer data and disrupted operations, leading to a shutdown of customer-facing services. This interruption had a significant ripple effect, affecting an estimated one-third of all medical transactions in the U.S.[1], highlighting the critical role Change Healthcare plays in the nation's healthcare infrastructure.

Many medical practices were unable to process claims, verify insurance eligibility, access patient records, and conduct routine billing. As a result, the disruption caused lost income and forced some offices to temporarily close. This incident raises many questions regarding Change Healthcare's security practices and how an organization can protect itself from the same fate. This article highlights a crucial lesson about the risks of vendor dependency in the healthcare sector.

What Happened

Change Healthcare fell victim to a Russian-linked hacking group named BlackCat known for its expertise in ransomware attacks. The group exploited a vulnerability in a product called ConnectWise to infiltrate Change Healthcare's systems. Upon gaining access, they exfiltrated 6 terabytes of data containing protected health information (PHI) then launched a ransomware attack locking the company out of their systems[2].

Immediately following the detection of the incident, Change Healthcare initiated a shutdown of systems and services to contain the attack and prevent further spreading of the ransomware. The result of the massive shutdown left healthcare organizations helpless as they lost access to Change Healthcare services upon which they depended. Furthermore, these organizations were left in the dark for nearly a month before the first systems were restored.

Financial Impact on Health Organizations

The Change Healthcare incident significantly impacted a range of clearinghouse operations that included medical records, insurance, billing, and prescriptions. The resulting absence of these services placed financial strain on many health organizations. According to the American Hospital Association (AHA) 94% of hospitals reported a financial impact[3], and an American Medical Association (AMA) survey of medical practices reported that 77% of respondents experienced service disruptions, with 80% reporting lost revenue from unpaid claims, and 55% having to use personal funds to cover their practices' expenses[4].

In response, Optum has established a Temporary Funding Assistance Program to assist medical practices that are unable to meet their weekly shortfall[5]. Additionally, these events prompted the Centers for Medicare and Medicaid Services (CMS) to issue accelerated and advanced payments to affected providers[6]. These measures aim to provide financial relief to healthcare providers impacted by recent challenges.

Scrutiny of the Change Healthcare incident continues as this event has prompted numerous investigations, class action lawsuits, and calls to Congress. On March 13, the Department of Health and Human Services (DHHS) issued a letter stating that the Office for Civil Rights (OCR) would be opening an investigation focusing on whether a breach of protected health information occurred and compliance with the HIPAA Rules[7].

Making Vendor Management Part of Risk Management

Medical practices depend on third-party vendors for essential services critical to their daily operations, and they depend on these services being consistently available while protecting the confidential information entrusted to them. However, the Change Healthcare breach, along with its subsequent cascading effects, highlights the risks associated with reliance on vendors, particularly when a single vendor provides multiple services. Consequently, healthcare organizations must be prepared for potential disruptions and should incorporate specific strategies into their business continuity and disaster recovery plans to mitigate these risks.

Conduct a Risk Assessment

A risk assessment focusing on vendor management is an essential first step in preparing for future disruptions. Organizations should conduct a review of essential services provided by third-party vendors, identifying those that are critical for day-to-day operations. This process involves not only recognizing which services are vital but also understanding the potential consequences of their failure. By mapping out how each service contributes to the organization's overall functionality and identifying potential work arounds, practices

can ensure ongoing operations during unexpected vendor outages.

For each identified service, organizations should establish potential contingency solutions. These solutions could range from manual processing to alternative communication channels and the use of redundant vendors. For instance, if the current electronic process fails, is it feasible to revert to manual, paper-based operations? If so, organizations must ensure they have the paper documents and other resources necessary to carry out these tasks effectively.

During incidents like the Change Healthcare breach, where online electronic portals became inaccessible, organizations found themselves at a loss. To prepare for similar future scenarios, it's vital to consider how alternative processing might be executed. Options could include emailing or faxing documents directly to the vendors. Of course, the privacy and security of protected health information must be maintained when alternate processing methods are in use.

It's essential for organizations to identify and vet alternative vendors well in advance. This preparation involves understanding the specific requirements needed to establish service quickly and efficiently. Establishing these relationships and processes ahead of time ensures that, in the event of a disruption, organizations can migrate without significant delays. Service agreement terms with alternate vendors should be reviewed for understanding any contractual limitations or conditions for quickly bringing the secondary provider on-line. In addition, businesses should not wait until a crisis occurs to start identifying potential vendors. Proactive relationship management, with a clear plan for transitioning services during an incident, is crucial.

Plan for Revenue Disruptions

During the Change Healthcare outage, many medical practices continued services while revenue streams were disrupted. As part of the risk assessment, organizations need to identify potential impact on revenue and its impact on continued operations. Monthly expenses for payroll, utilities, rent, and other core functions should be determined, along with evaluating how long the organization can sustain these expenses without normal revenue inflow. This analysis will enable practices to identify the necessary buffer to support operations during extended periods of disruption.

Alternative solutions to consider include insurance, cash reserves, and lines of credit. Business Interruption Insurance is designed to compensate businesses for lost income due to external factors beyond their control, but like any other insurance, it is important to understand what is and what is not covered, as well as reporting obligations and policy limits. Cash reserves provide a financial cushion that can help a business stay afloat without the need for reliance on external funding during short-term disruptions. Similarly, lines of credit offer flexible, readily available funds that can be used to manage unexpected expenses or cash flow shortages. It's crucial that these measures are established well before any incident occurs.

Conclusion

The Change Healthcare breach serves as a stark reminder of operational risk imposed by third-party vendors, particularly the reliance of a single vendor for multiple core services. To combat such vulnerabilities, it is necessary for organizations to include vendor management in the broader risk management framework. This should include conducting thorough risk assessments focused on the operational dependencies on third-party services. Furthermore, the financial impact of the Change Healthcare breach underscores the necessity of planning for revenue disruptions. In conclusion, the lessons learned from the Change Healthcare incident are clear: healthcare organizations must not only prepare for the possibility of their own technological failures but also plan for disruptions caused by third-party vendors.

Resources are available to policyholders in SVMIC's cybersecurity center found HERE on the Vantage® site. SVMIC also recommends you talk with your professional business insurance broker to evaluate insurance coverage and determine a level of cyber coverage with which you feel comfortable in the event of a cyber incident.

If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email ContactSVMIC@svmic.com.

If you experience a cybersecurity or other HIPAA-related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

Supporting Hospitals and Patients After Cyberattack on Change Healthcare (AHA.org)

UnitedHealth Confirms Data Theft From Change Healthcare (crn.com)

Information on the Change Healthcare Cyber Response (UnitedHealthGroup.com)

AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances (AHA.org)

Temporary Funding Assistance Program for Providers (optum.com)

Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers (CMS.gov)

Cyber Attack on Change Healthcare (hhs.gov)
