SEO DETAILS:

Page Title: Cybersecurity Issues After the Change Healthcare Data Breach | [INSERT RELATED SERVICE] | [INSERT FIRM NAME]

Meta Description: [NAME OF FIRM] discusses the aftermath of a major cyberattack on Change Healthcare and its profound implications for patient privacy and provider operations.

Headline: Cybersecurity Issues After the Change Healthcare Data Breach

BODY COPY:

Cybersecurity has long been an important concern in healthcare. Data breaches and other cyberattacks can threaten patient privacy and healthcare providers' bottom lines. A cyberattack in February 2024 targeted Change Healthcare, a service provider that processes payment claims and handles other critical matters for countless healthcare providers around the country. The attack disrupted billing and patient care across the country, affecting thousands of healthcare providers. This article will summarize the incident and its impact and provide tips for how providers can adapt their billing and claims processes.

What Was the Change Healthcare Data Breach?

On February 21, 2024, Change Healthcare experienced a ransomware attack. The company described it as a breach by a "suspected nation-state associated cybersecurity threat actor." It stated that it disconnected the affected systems "to prevent further impact."

A ransomware attack involves malware that disables a computer system. The attacker typically demands payment in exchange for an encryption key to release the system from the malware. Payment is fairly common, especially when an attack targets a system that cannot afford downtime. While neither Change Healthcare nor its parent company has commented on the matter, someone associated with the ransomware gang known as "Blackcat" reportedly claimed on March 4 to have received a cryptocurrency payment worth more than $22 million from the company.

What Was the Impact of the Change Healthcare Data Breach?

As a result of the ransomware attack, doctors, pharmacies and other healthcare providers were unable to submit insurance claims. Patients experienced delays in treatments and prescriptions unless they could pay out of pocket. Providers experienced delays in payments from insurance companies, Medicare and Medicaid. Many of the effects are still ongoing as of late March. No estimates of the total cost are available yet.

How Is the Government Responding to the Data Breach?

On February 26, the American Hospital Association (AHA) sent a letter to the U.S. Department of Health and Human Services (HHS) requesting the federal government's help. Requests included:

- Working "to facilitate communication and transparency from Change Healthcare to the provider community";
- Advising providers about requesting advanced and accelerated payments from Medicare;
- Extending "the timely filing requirements under federally regulated health plans"; and
- Informing the public that "good faith estimates…may temporarily be unavailable."

HHS issued a statement on March 5 announcing measures to improve flexibilities for hospitals affected by the ransomware attack:

- It directed Medicare Administrative Contractors (MACs) to expedite electronic data interchange (EDI) enrollment in new clearinghouses for affected providers.
- Affected hospitals can submit accelerated payment requests to their MACs, much like during the COVID-19 pandemic.
- It advised Medicare providers to contact their MACs about available waivers, extensions or exceptions.
- It instructed the Centers for Medicare and Medicaid Services (CMS) to issue relaxed prior authorization guidelines to Medicare Advantage and Part D sponsors.
- It urged state Medicaid and Children's Health Insurance Program (CHIP) managed care plans to relax their standards for prior authorization as well.

The AHA responded critically to HHS's announcement the same day. It described the measures as "not an adequate whole of government response." The White House convened a meeting with leaders of HHS and major health insurance companies the following week to discuss further ways to address the situation.

How Is Change Healthcare Responding to the Data Breach?

Optum, another subsidiary of Change Healthcare's parent company, announced on March 1 that it was launching a Temporary Funding Assistance Program (TFAP) to help providers experiencing short-term cash flow problems. TFAP advances funds to providers each week in amounts based on "the difference between their historical payment levels and the payment levels post attack." Recipients will not have to repay the advances "until claims flows have fully resumed." At that point, the company will send invoices, and repayment will be due within 30 days.

The company stated that "all major pharmacy claims and payment systems" were back to normal operations as of March 1. It announced several temporary measures to assist Medicare patients, which will remain in effect until March 31:

- Prior authorization is suspended for most outpatient services for Medicare Advantage plans.
- Drug formulary exception review processes are suspended for Part D benefits.

The AHA was also critical of these measures, saying they are "not even a band-aid" on the total damage caused by the attack.

What Can Healthcare Providers Learn from This Incident?

This incident underscores the importance of having plans in place for downtime that causes revenue interruptions. Possible steps include the following:

- Request information from one's MAC about Medicare accelerated payments and other ways to optimize claims and payments.
- Require physicians to complete their progress notes promptly.
- Review claim scrubbing procedures to ensure they accurately capture the rejection reason codes.
- Conduct internal audits and reviews of matters like unpaid claims, patient balances and collections.

- Use payer portals to simplify processes like claim submissions, appeals and corrections.
- Reduce the inventory of held claims by alternating between clearinghouses.
- Talk to payer provider representatives to address ongoing issues that delay the payment of claims.
- Ask payer providers about periodic interim payments.
- Look into ways to optimize billing workflows to minimize the number of claim touches, i.e., submitted claims that receive no immediate action.

CLOSE:

If you have any questions or would like additional information, please contact [NAME] in our [DEPARTMENT] at [NUMBER] or [EMAIL].

SUGGESTED IMAGERY:

https://stock.adobe.com/images/nurse-hands-or-tablet-for-medical-cybersecurity-lock-life-insurance-or-healthcare-data-safety-on-internet-zoom-doctor-or-futuristic-hologram-on-technology-for-night-support-or-woman-wellness-fund/565567523?prev_url=detail