What Did We Learn From the Change Healthcare Outage?

Phyllis Dobberstein, CPC, CPMA, CPCO, CEMC, CCC

Nearly all of us in the healthcare ecosystem were impacted by the cyberattack on Change Healthcare in February that caused widespread network disruptions. Change Healthcare processes 15 billion healthcare transactions annually and is connected to one-third of patient medical records in the United States. More than 100 Change Healthcare applications across pharmacy, medical, dental, patient engagement, and payment services were affected by the disruptions. Months later, United Health Group (UHG), Change Healthcare's parent company, said it had restored 30% of its products, while another 57% had only partial service available, and some remained unavailable.

The group that claimed responsibility for the cyberattack was able to exfiltrate 6 terabytes of "highly selective data" by stealing a password and entering through a portal that didn't have secondary authentication enabled. It's a huge amount of data that was compromised.

Fewer But Larger Healthcare Companies

The breach highlighted a security vulnerability against a backdrop of large-scale mergers that keep consolidating healthcare into the hands of fewer corporations. For example, some major payers deal exclusively with certain clearinghouses to process their claims, so even some of the practices that did not contract with Change Healthcare still lost their ability to files claims with certain payers and receive reimbursement.

Meanwhile, the financial impact has been widespread. According to the American Medical Association's survey results in April, some of its members are still encountering issues with real-time eligibility (60%), claim submission (75%), receipt of electronic remittance advice (79%), and claim payments (85%). The cyberattack put a financial strain on practices, not just those that use Change Healthcare as their clearinghouse. An estimated 62% of practice owners also had to use personal funds to cover expenses just to keep the lights on.

"An estimated 62% of practice owners also had to use personal funds to cover expenses just to keep the lights on."

Reporting the Breach

The HIPAA Privacy rule defines covered entities as healthcare providers, health plans, and clearinghouses that electronically transmit health information. Covered entities have up to 60 calendar days from the date of discovery of a breach of unsecured protected health information (PHI) to file breach reports to Office for Civil Rights (OCR) when it affects 500 or more individuals. Covered entities and their business associates are also required to notify affected individuals, and sometimes the media, for a breach of this size.

Recently we learned more about the reporting obligations for individual practices under HIPAA and state breach notification laws as they relate to the Change Healthcare incident. When there is a breach of PHI, it is ultimately the responsibility of the covered entity to notify the affected individuals about the breach of their PHI, although the covered entity may delegate that responsibility to a business associate.

Provider groups asked the federal government to clarify whether or not UHG should handle the breach notifications stemming from this incident. UHG had previously stated that it would handle reporting for "customers." But this left several unanswered questions regarding which stake-

Phyllis Dobberstein, CPC, CPMA, CPCO, CEMC, CCC, is RCM Revenue Integrity Manager at Experity.

holder group was responsible for sending out the required HIPAA breach notifications.

In early June, OCR confirmed that breach notification may be performed by UHG and Change Healthcare. As a result, the notifications to patients whose PHI was compromised will come from UHG and Change Healthcare, thus sparing the covered entities from the administrative task and from appearing to have culpability for the breach.

Negative RCM Impact

The negative impact to revenue cycle management operations is extensive for some urgent care operators that are still recovering from the claims processing chaos that occurred during the public health emergency. Workarounds, such as resorting to paper claims, do not often provide proof of timely filing or guarantee of reimbursement. While some payers have waived certain requirements to speed up processes, others prefer to wait and see what happens.

Without electronic means to post funds, staff may be required to follow up on claims manually. This means unpaid claims may not be addressed in a timely manner. Patient satisfaction will also be impacted as patients may not receive a billing statement for many months or may be billed the wrong amount. All of these delays cause an increase in inbound phone calls and extra administrative work that chips away at margins.

"Ultimately, healthcare business owners are the losers in this situation, and it will impact them financially for likely the entire year with lost revenue and increased practice expense."

Ultimately, healthcare business owners are the losers in this situation, and it will impact them financially for likely the entire year with lost revenue and increased practice expense. Let's hope we can learn from this event and make the necessary changes in our industry to prevent another disruption of this size. ■