Physician Payment Issues in the Wake of the Change Healthcare Hacking

By Elizabeth Woodcock, MBA, FACMPE, CPC

The results of an American Medical Association survey in the aftermath of the February 21 Change Healthcare cybersecurity attack demonstrate the continuation of challenges, despite parent company United Healthcare's declaration that the situation has been resolved. The April 29, 2024 AMA survey reveals:

- 60% of medical practices continue to face challenges in verifying patient eligibility.
- 75% still face barriers with claim submission.
- 79% still cannot receive electronic remittance advice.
- 85% continue to experience disruptions in claim payments.

More distressing, these challenges are resulting in cash flow issues that are forcing physicians to seek loans or go without personal compensation to avoid disrupting patient care. While there are no easy solutions, medical practices can take steps to navigate these uncharted waters.

Recognize key government interventions. The US Department of Health & Human Services has issued requirements for its Medicare contractors. For example, "the MACs [Medicare Administrative Contractors] must accept paper submissions if a provider needs to file claims in that method." The department, which includes the Centers for Medicare & Medicaid Services (CMS), has issued instructions to the states about Medicaid payments. Of particular importance is the resource guide the federal agency compiled and distributed to providers in March.

Identify payment relief opportunities - and the strings attached. Proactively seek financial resources available, including the Change/Optum program. Some accountable care organizations have stepped up to the plate to offer advance payments. Read the fine print before applying, however, as programs may have arduous application processes and challenging mechanisms for payback. Although far from ideal, some practices have found a business line of credit or loan from a bank the most effective option.

Track the progress. The February 21st cyberattack that hit Change Healthcare was initially thought to just affect claims distribution. However, the situation has affected many aspects of the health care data highway, including prescriptions and prior authorizations. Monitor the progress by function.

Measure the impact. While the media is full of anecdotes, let's identify the impact of the cyberattack on your practice. Tracking claims has always been important. Today, it's critical. Develop a report to pinpoint the claims that were not released and/or processed, documenting the date and associated charges. Maintain a record of your attempts to submit the claims, even if they do not get processed. That record will help you if you get denied for timely filing, an aftermath of the incident that practices around the nation are reporting. Appeal timely filing denials until you're successful in getting paid, reporting to your state insurance commissioner if you are not. Maintain meticulous records regarding the unprocessed claims, as well as those that have been denied. Consider reporting your efforts and (blinded) data to advocacy groups who are working with state and federal legislators to compensate providers for their financial losses.

The past decade has seen consolidation of the major insurance companies -- United Healthcare, which bought Change Healthcare in October 2022 - is a nearly $400-billion company. Not only does it control approximately 40% of health care claims processed each year in the United States, United Healthcare now employs 1 out of every 10 physicians. The cyberattack has put the company in the spotlight of federal lawmakers. Called to testify before Congress on May 1, CEO Andrew Witty's attestation underscores how much remains unknown about the attack itself - and the implications for the future. United Healthcare admitted that elementary safeguards were not present - hackers gained

entry via a portal that did not have basic multi-factor authentication in place. Despite the $22 million ransom payment by United Healthcare, the Russian hackers have begun posting sensitive medical records on the dark web, including charts from U.S. military personnel. United Healthcare's documented vulnerability - and their massive size -- may not bring comfort to physicians. The only promising news that may have come out of this nightmare is that United Healthcare is squarely on the radar screen of lawmakers. Whether physicians may benefit from this scrutiny will likely take years to understand.
