REVENUE CYCLE SUCCESS

Are you leaving money on the table?

BY FIELDING EMMOTT

Efficiency and predictability should be the aim of the revenue cycle management (RCM) team at ophthalmic practices. Neglecting front-end RCM processes can cost a practice big money on the back end. Addressing inefficiencies in the RCM department is an obvious strategy, but maintaining a level of predictability requires a nuanced approach to revenue cycles.

Not only can efficient, predictable RCM improve the financial health of a practice, but it can also strengthen a practice's ability to provide excellent patient care by giving staff more time to focus on seeing and treating patients. As CMS and private insurers adjust their reimbursement rules and regulations, the staff is constantly challenged to keep up. From provider credentialing and patient scheduling to payments and accounts receivable, the staff is often under pressure to maintain efficient, optimized RCM processes.

To combat fraud and waste, federal agencies have introduced integrity initiatives, such as the Recovery Audit Program, that are designed to identify incorrect Medicare payments and collect overpayments. These initiatives bring further scrutiny to submitted claims, resulting in a 9% increase in Medicare Part B claim denials.[1]

The adaptability of a practice's RCM processes to this ever-changing landscape can directly affect how much time and revenue are wasted. Questions practice owners should ask themselves include:

- Which billing processes can be automated?
- Does the billing staff have enough time and resources to complete their tasks efficiently?
- Are the practice's systems protected from cyber attacks?

AUTOMATION AND EFFICIENCY

A growing need for optimal organizational workflow coupled with regulatory reforms and reclassifications is driving growth in the multibillion-dollar US RCM market—11% year-over-year in the next 5 to 7 years.[2] Instability created by the COVID-19 pandemic, including staffing shortages and claim fluctuations, has caused many practices to consider outsourcing their RCM.

Accelerating competition in this space is spurring the development of third-party RCM solutions aiming to capitalize on the growing market. The evolving intricacies of a practice necessitate a customized solution that will increase revenue, decrease the number of technical errors, and streamline engagement between staff and patients.

AT A GLANCE

- The adaptability of a practice's revenue cycle management processes to an ever-changing landscape can directly affect how much time and revenue are wasted.
- Transitioning from manual to electronic claims transactions can save a significant amount of time and money.
- To protect sensitive data, health care organizations increasingly rely on data loss prevention services.

Transitioning from manual to electronic claims transactions can save a significant amount of time and money. According to the Council for Affordable Quality Healthcare, electronic prior authorization offers providers the greatest time savings potential by reducing transaction time from 20 minutes to 6 minutes and cost from $7.50 to $1.89.[3]

CYBERSECURITY AND THE UNKNOWN

Suppose that RCM efficiency optimization begins to pay off but that, one morning, all of the practice's systems have been encrypted. What is the next step? How long of a shutdown is economically feasible? A practice's revenue is 100% dependent on its systems being fully operational.

Automating billing processes can save a practice time and money. Transitioning to electronic transactions, however, does not come without risk. The more a practice sends and stores patient data electronically, the more valuable its systems become to bad actors and malicious parties.

So, what is the risk? According to the Ponemon Institute, health care organizations had the highest costs associated with a data breach—$175 per compromised record—for the 10th year in a row.[4] This figure represents only the initial cost associated with stolen health records, not the additional time and resources spent investigating and resolving an issue that can be devastating to patient care and safety. The average time for an organization to move from a cyber attack to a completed forensic investigation is 49 days.[5] The $175 in damages likely represents just the tip of the iceberg for an affected practice. To secure and protect their sensitive data, health care organizations increasingly rely on the expertise of data loss prevention services.

The National Institute of Standards and Technology offers a cybersecurity framework that businesses and organizations of all sizes can implement to improve their cybersecurity posture. Relatively easy measures such as implementing two-factor authentication and training staff to detect suspicious emails are a start. The more proactive an organization is in protecting its networks and data, the more predictable its operational revenue will be. ■

1. What is healthcare revenue cycle management? Revcycle Intelligence. June 14, 2016. Accessed May 13, 2022. revcycleintelligence.com/features/what-is-healthcare-revenue-cycle-management
2. U.S. revenue cycle management market size, share & trends analysis report by end user, by product type, by component, by delivery mode, by physician specialty, by sourcing, by functions, and segment forecasts, 2021 – 2028. Grandview Research. March 2021. Accessed May 13, 2022. www.grandviewresearch.com/industry-analysis/us-revenue-cycle-management-rcm-market
3. 2016 CAQH index highlights adoption, costs and savings from electronic claims-related transactions. CAQH. January 2017. Accessed May 13, 2022. www.caqh.org/about/newsletter/2017/2016-caqh-index-highlights-adoption-costs-and-savings-electronic-claims
4. Brook C. What does a data breach cost in 2020? Digital Guardian. August 18, 2020. Accessed May 13, 2022. digitalguardian.com/blog/what-does-data-breach-cost-2020
5. Johnson J. Average cyber incident response timeline in the United States in 2019. Statista. January 25, 2021. Accessed May 13, 2022. www.statista.com/statistics/194119/average-time-span-until-a-cybercrime-incident-is-resolved

FIELDING EMMOTT
■ Copywriter, Medical Consulting Group
■ femmott@medcgroup.com
■ Financial disclosure: Employee (Medical Consulting Group)