Security risks can be a MIPS score killer

By Art Gross

Prolonging the process of figuring out quality measures under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) and increasing scores for the Merit-Based Incentive Payment System (MIPS) could put medical practices at a competitive disadvantage.

Healthcare providers will earn a MIPS score each year, starting in 2019 (based on 2017 performance). According to Jim Tate, president of EMR Advocate Inc., Weaverville, N.C., and MIPS scoring consultant, the Centers for Medicare & Medicaid Services (CMS) will post their results on the Physician Compare website (medicare.gov/physiciancompare) for public viewing. Not only will Medicare Part B reimbursements have a swing of up to 4% by 2019 (escalating to plus or minus 9% in 2022), resulting in high gains or losses in revenues, but providers' scores will be public.

Because MIPS scores will be public, how well a particular physician or practice does could affect recruitment and marketing for practices. Under MACRA, a neurosurgery practice could hire a spine surgeon who brings a MIPS score of 93 (out of 100 possible points) to the practice, Tate says. The surgeon's reimbursements could contribute to the practice's bottom line. Likewise, a cardiology practice with a MIPS score of 93 could lure patients away from a competing practice with a much lower score. The value of the practice will soon be measured by its MIPS score, which will be recalculated every year.

Points lost for failure to perform a security risk assessment

There are four MIPS pillars that determine how providers will be scored. One of those pillars, advancing care information (ACI), requires a security risk assessment (SRA), among other criteria, to receive a base score. Practices must prove that their patients' electronic protected health information (ePHI) is being protected on their networks. Failure to perform an SRA will result in a base score of zero, an automatic loss of 25 points from their MIPS score, lower reimbursements and a lower ranking accessible to the public.

Moreover, under MACRA, MIPS participants are subject to a random audit for up to 10 years. In the event of an audit, participants may be asked to upload documentation to prove they performed an SRA. Even after going through the process of selecting and reporting on measures for each pillar, failure to perform an SRA puts the practice at risk for having its MIPS scores recalculated. Revised scores will be published by CMS, with subsequent recoupment of significant amounts of already received Medicare Part B payments.

»

Do the SRA footwork first

Although there are many areas of the practice that need to be examined for security and HIPAA compliance, here are five that the practice should address, at a minimum, to secure ePHI:

Inventory patient information: Locate where all patient information is stored. It could be in an EHR record, a Word document in the form of patient letters, spreadsheets as billing reports, or scanned images of an insurance carrier's explanation of benefits (EOB). This information resides on desktops, laptops and mobile devices, and should be encrypted.

Encrypt data: Encrypt patient data to prevent hackers from stealing proprietary information and to avoid costly penalties, as auditors will consider whether a firm took all reasonable steps to protect patient records.

Train employees: Make sure they know how to spot phishing scams and suspicious links in emails and recognize fraudulent "IT experts" who call in to upgrade an operating system. They should also know to avoid conducting business on public Wi-Fi and minimize sharing on social networks.

Prevent employee data theft: Employee theft of information is one of the leading causes of HIPAA breaches in small organizations. Consider this example: An employee steals patient information and opens a credit card account. The patient could then sue the practice for not protecting his or her ePHI. Employees should have minimal access to EHRs — only the information they need to perform their duties. Also data logs should be checked.

Create a breach response plan: Is there a response plan in place in case a breach does occur? The plan should include who will be on the response team, what actions the team will take to address the breach, and what steps they'll take to prevent another similar breach from occurring. Make sure the plan is documented and all employees are trained on what they need to do.

Invest the time and devote the resources to perform a comprehensive risk assessment yourself or employ a HIPAA security consultant to begin scoring MIPS points, maximizing your reimbursements and protecting your reputation. ■

Contact Art Gross at artg@hipaasecurenow.com.