ION Solutions
AmerisourceBergen

Conducting a Security Risk Analysis

With reimbursement reporting under the Centers for Medicare & Medicaid Services (CMS), formerly under Meaningful Use (MU) and now under the Merit-based Incentive Payment System (MIPS), practices are required to report on their security risk analysis or protection of patient information. The government takes this protection very seriously. In 2016 alone, more than 329 breaches of more than 500 health records were reported, totaling more than 16 million patient records.[1] While cyberattacks and hacking accounted for some of the breaches, sometimes records are lost because of loss or improper disposal.

Many practices think that just installing a certified EHR or conducting a one-time training will cover everything for privacy and security. While EHR vendors can provide training on the privacy aspects of their products, it is up to the practice to ensure that they take steps to ensure privacy and document the process. CMS suggests that supporting documentation for attestation be retained for a minimum of six years.

Internal security risk audits must be completed by the end of the current reporting year, but it is not too early to start for the next year. Practices need to understand that it is not just putting a HIPPA policy in place – it is addressing questions that may come up about security.

Examples like:

- What if an administrator's laptop is stolen out of a car? Is the laptop password protected? Or is the data encrypted? How do you notify patients?
- If your server goes down, what do you have in place for backup? And is that backup protected?
- When your reception area is checking in patients, can the patient read the screen? With computers in the exam rooms, does your staff log off before leaving the room or is there an automatic logoff?

Security risk compliance and HIPPA enforcement are some of the most audited subjects conducted by CMS. After receiving an audit letter, practices have little time to respond (often just 10 days to send documentation) and if not answered completely and successfully, providers can lose thousands of dollars in previous reimbursements.

If your practice needs to ensure you are answering all the possible questions, and documenting the process, ION Solutions experts have a checklist and template available for accuracy and completeness as part of their standard consulting services. If you are interested in learning more about conducting a security risk analysis or more about MIPS, email us at sales@intrinsiq.com or call 877-570-8721 x2.

1. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/