HealthManagement.org
Promoting Management and Leadership

Increasing importance of EHR-related risk-mitigation strategies

A new report from The Doctors Company, a physician-owned malpractice insurer, shows a significant increase in malpractice claims for errors attributed to electronic health records. There were 161 claims for which EHRs were either the cause or (more likely) a contributing factor between 2011 and 2016, compared to just two claims during the period 2007-2010.

The alleged medical errors, according to the report, were caused by a variety of factors such as those related to technology and system design (e.g., drop-down menus, templates, alerts). Other factors had to do with human error, including lack of training and improper use of the "copy-and-paste" function.

The report found that system factors in the EHR itself – poor integration, suboptimal design and UX, failures of alerts and alarms – were up 8 percent since the last time The Doctors Company did a similar report in 2015. In contrast, factors that might be due to user error (data entry errors, alert fatigue and misuse of copy-and-paste) decreased 6 percent.

The study offers some useful tips to help providers avoid malpractice claims, reduce the chance of errors and improve patient safety.

- Be aware that physicians are the ones responsible for the data to which they have access. "Review all available data and information prior to treating a patient," says the report author David Troxel, MD, medical director at The Doctors Company. "The healthcare setting, accessibility of data, and acuity of the patient's situation and condition will dictate what will be considered reasonable by a court."

- Be careful with e-prescribing, which is useful but offers many opportunities for error. "Make sure you adhere to any alerts within the e-prescribing module of the EHR and document any actions taken," he notes.

- Alert fatigue is a problem, but physicians could be liable if they don't follow an alert that could have prevented an adverse event. "Do not disable or override any alerts in the EHR. Discuss alert fatigue issues with your organisation's IT department or your EHR vendor," according to the report.

- Be careful with copy-and-paste. "Avoid copying and pasting except when describing the patient's past medical history," says Troxel. "As with handwritten records, make sure your documentation is relevant, objective, and current."

- Stay aware of history & physical and procedure notes, which often autopopulate from older notes or

templates. "Contact your organisation's IT department or your vendor if you notice that the autopopulation feature causes erroneous data to be recorded," he explains. "If the autopopulated information is incorrect, note it in the record and document the correct information."

- Be careful with entry errors related to drop-down menus or other automatic features. "Erroneous information, once entered into the EHR, is easily perpetuated and disseminated. Review your entry after you make a choice from a drop-down menu," the report points out.

- Don't share passwords, and stay vigilant about cybersecurity. "Staff should not be allowed to use the physician's password to review, update, or sign off on lab and imaging results. Allowing this type of activity could result in a report being filed without the physician seeing it."

- Even if an error can be traced to bad EHR design, vendor contracts often have "hold harmless" clauses that try to put liability onto physicians. "Keep in mind that some insurance policies may exclude coverage for product liability and indemnification of third parties. In addition, vendors and users typically settle disputes out of court with 'nondisclosure' clauses that prevent open discussion of the patient safety issues involved," Troxel writes.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 24 Oct 2017