COOPERATIVE OF
AMERICAN PHYSICIANS

Ten Risks of Electronic Medical Records

DO YOU KNOW THEM?

Authored by:
Allan Ridings and Joseph Wager
Sr. Risk Management & Patient Safety Specialists

Introducing an electronic medical records system into the practice helps the physicians and staff provide more efficient health care by making medical records more accessible to all health care team members. It also brings some risks. In this two-part article, CAP Risk Management & Patient Safety identifies ten areas of risk exposure and provides some brief recommendations in each area.

EMR or EHR

Know your system. Electronic Medical Record is the term most often used for the electronic system now holding the medical records of the physician's patients. If patient's medical data is shared electronically with other facilities, locations, caregivers, and/or biller, the term Electronic Heath Records is more accurate. In articles and in practice, however, the terms are often used interchangeably.

Security Levels and Passwords

Confidentiality must be maintained in an electronic system just as with paper records. Administrators and/or the physician in charge should assign the levels of security clearance for the EMR for each staff member based on their individual job function. Prevent staff access to physician progress notes and prescription templates to avoid the creation or alteration of these areas for their own purposes. Each person should have their own password and the practice's policy should forbid sharing of those passwords. Immediately delete the password of any employee who leaves the practice.

Weights & Medications

Confusion in this area may adversely affect medication doses. The amount of medication will be dramatically different based on a patient's weight of 160 lbs. (pounds) versus 160 kgs. (kilograms). The physician should seek vendor assistance in choosing and securing either a metric or a United States format for weight measurements.

If choosing a United States format, employees must pay close attention to conversion calculations for medication dosages. Set an expectation that two employees check weight, conversion calculations, and dosage prior to administration to avoid mistakes. This can be especially critical in a pediatric practice.

Comments or questions related to this article may be sent to: consultant4EHR@CAPphysicians.com

HIPAA & PHI

Employers have responsibility, under Federal Law, to train employees in the protection of protected health information (PHI). Each physician's practice must have privacy and security policies that address patient privacy, preserving the security of data, and confidentiality of patient information. HIPAA violations may occur with EMRs when employees:

- Access, print, or download information that is not within the source of their job
- Disclose, or alter patient information without proper authorization
- Disclose to another person their sign-on codes or passwords, or use another person's, for accessing electronic records
- Attempt to access a secure part of the EHR without proper authorization

Prescriptions

Electronic-prescribing (e-Rx) is helpful if it saves the information to the patient's medical record. To be eligible for incentives, physicians should migrate to all-electronic prescription systems.

Know the source of the EMR's drug and clinical decision support information. Continual updates are important if needed to defend the adherence to a specialty's clinical standards of care or show knowledge of FDA updates and/or drug alerts for medications ordered.

All medication refill requests should be processed through the electronic system. Care must be taken when the dose of a medication is a "Change", a "Taper", or a "Sliding Scale". It is often necessary to enter these as separate orders. As a result, at eh patient's next visit, the EMR may only show the last dose, not the progressive order.

Diagnostic Testing

Tracking of laboratory and diagnostic orders and results is more efficient and timely when all orders are processed through the EMR with bi-directional interface. If possible, also set up to receive all results back through the system. If fax or paper reports are received, scan and index reports into the system the same day. The EHR system may also be used as a "tickler file" for verification of orders and paper reports.

Confidentiality of HIV/Drug History/Psychiatric Records

Some patient information is protected by law at a higher level. Your electronic record system should maintain this sensitive and legally protected patient data in an additional password-protected, secure area of the electronic records system. This will prevent the accidental copying of this information when a patient's record request is received. Again, the vendor can assist in this area. Designate specific staff members who may input and retrieve those reports or data.

Telephone Calls

Document all communications of physicians or staff with patients in the EHR system. Personal, non-patient, conversations between staff, however, should not be input into the patient medical record system as they could accidently be added into "open" records.

Devise a protocol to assure that after-hours phone calls (between patients, hospitals, and the licensed professionals) are entered into the system the following business day to ensure a complete medical record.

Comments or questions related to this article may be sent to: consultant4EHR@CAPphysicians.com

Data is NEVER Gone

Electronic medical records save all information into background files that cannot be deleted. This is to meet regulatory requirements and provide data security. Background files tell the story behind the story and may be helpful or hurtful to the physician. These files, also called "metadata" provide information about various aspects of the data – the who, what, when, and where. For Example:

- Did the physician view the alert giving a contraindication for a specific medication?
- How long did he view the alert before rejecting it and ordering the medication anyway?
- Was the physician's note really entered on the date stated – or added a week later?

Selecting the "Delete" or "Remove" key may make everything on the screen disappear. It DOES NOT remove it from the background data files. In other words, data is NEVER GONE. It may be subpoenaed in professional liability cases or in an allegation of a HIPAA violation.

Scanning

Optimally, patients' entire paper record is scanned and indexed for easy accessibility. While this is preferred, it is not always possible. The important thing is to develop a policy of how much of the medical record is captured and follow it consistently. Some physicians choose to scan the most recent 18 to 24 months into the active system while the older records are scanned into archive files. Each physician must determine the most pertinent data necessary in providing the best quality of care. Make sure not to overlook documentation of phone calls or medication refills.

During scanning, periodically test the print function to make sure it captures everything inputted.

Additionally, once scanned, ensure that the paper documents are properly stored, offered to patients, or destroyed.