Electronic healthcare records (EHRs) provide access to information, resulting in more coordinated and efficient care for your patients. However, a data breach or human error may compromise EHR confidentiality and result in a failure to comply with HIPAA Privacy and Security Rules. The following recommendations can help your organization properly document and maintain EHRs.

**Develop documentation standards**

Documentation should be complete, accurate and timely and include pertinent assessment findings.

- Develop and train staff on documentation standards.
- Documentation should:
  - Include a response to prescribed treatment and medications.
  - Clearly describe clinical analysis and the plan of care.
  - Include care and treatment that meet professional standards of care.
  - Delineate patient education and post-treatment or discharge instructions.
  - Include evaluation of patient understanding.
  - Reflect pertinent interactions with the patient and family.
- Train your staff on established documentation criteria.
- Carefully consider the organization of the EHR, including where informed consent documentation will be located.
- Create a defined section for scanned documents and establish a schedule to integrate them into the EHR.
- Develop a tracking system for patient notification of diagnostic and other test results, normal and abnormal.
- Complete chart notes at the time of patient treatment or shortly thereafter.
- Establish a time limit for completing documentation.
- Periodically evaluate printed records from the perspective of an auditor or expert witness.
- Review printed records carefully to ensure that information located in other tabs or screens is included.
- Develop a system and policy to determine the use of alerts in the EHR.
- Be cautious about using generic templates and do not create templates that automatically re-populate patient information.
- Understand how the time-stamp feature works (at the time care was delivered or documentation was entered).
- Audit your EHR for quality, patient safety and completeness.
- Ensure that your EHR system either does not permit a cut-and-paste functionality or that it may be disabled. If copy-and-paste functionality is used, ensure that it is used on a limited basis and only in specified situations.
Comply with confidentiality rules

The HIPAA Security Rule requires that health care providers establish physical, administrative and technical safeguards to protect EHRs.

- Focus on how work stations are set up in examination and treatment rooms.
- Periodically review reports that list who has accessed patient records. Immediately address any unauthorized access to those records.
- Limit access to all patient records to only those employees and providers whose roles necessitate access for documentation and review purposes.
- Be aware of similar patient names/patient identifiers.
- Encrypt all electronic protected health information (EPIH) in storage on systems, networks, portable devices and electronic media.
- Encrypt all EPHI while in transit across public networks.

Prevent fraud and ensure patient safety

The Ponemon Institute estimates that data breaches cost the U.S. healthcare industry nearly $7 billion a year.*

- Verify that the record accurately documents the work or procedures completed by each provider who treated the patient.
- Avoid auto-authentication or signing multiple documents simultaneously in the absence of opening documents.
- Avoid copying and pasting in order to eliminate the ability to sign and acknowledge the record as accurate without actual record review.
- Avoid automated insertion of clinical data. Templates that enter positive/negative findings or data by default may lead to serious recordkeeping and clinical errors.
- Create policies and procedures to address addenda, amendments, corrections and late entries in the EHR.
- Establish clearly defined policies on when a record is considered complete and how it is to be closed. Changes that must be made after a record is locked should be managed on a case-by-case basis.
- Never add documentation on a previous encounter or event in the record once a liability claim has been filed.
- Implement an internal audit system to identify and track any issues.
- Ensure that your EHR system tracks every entry, including corrections. Tracking all entries is an important requirement for proper defense if the integrity of the record is questioned during the claim process or legal proceedings.
- Educate staff and providers on what metadata is and how it can be used in a lawsuit.

For more information about documenting and storing EHRs, please contact your CNA Risk Control consultant, call 888-600-4776 or visit www.cna.com/riskcontrol.