White Paper
Electronic Health Records

Summary
The health record is the legal business record for a healthcare organization. As such, it must be maintained in a manner that follows applicable regulations, accreditation standards, professional practice standards, and legal standards. The standards may vary based on practice setting, state statutes, and applicable case law. Many of the guidelines that originally applied to paper-based health records translate to documentation in electronic health records (EHRs).

Legal/Survey Considerations
Health records are business records that can be used as testimony in legal proceedings. A health record must meet certain standards in order to be admissible in court and not be considered hearsay. Rules of evidence for business records, include that they are documented and kept in the normal course of business, made at or near the time of the matter recorded by a person within the business with knowledge of the events, conditions, opinions, or diagnoses appearing in it. A carefully designed electronic health record that meets the requirements of a legal health record is an effective strategy to minimize a healthcare organization’s risk and liability. For these reasons it is recommended that an attorney should review policies related to legal documentation issues to ensure adherence to the most current standards and case law. Electronic health records systems must be set up to protect records from loss, destruction or unauthorized use. In addition they must be systemically organized, complete, accurately documented, readily accessible and maintained in accordance with acceptable standards of professional practice.

Regulatory Considerations
Nursing facilities are prohibited from violating the confidentiality of “personal and medical records, and the right to approve or refuse the release of these records to any individual outside the home, except in the case of transfer to another home, hospital, or health care system, as required by law or rule, or as required by a third-party payment contract.” Revised Code § 3721.13(A)(10). Pursuant to Ohio Administrative Code § 3701-17-19(C), the records that a nursing home is required to maintain may be maintained in electronic format. According to Revised Code § 3701.75(B) health care records may be authenticated by electronic signature if the following apply:
1. The entity adopts a policy that permits the use of electronic signatures on electronic records;
2. The electronic signature system utilizes either a two level access control mechanism that assigns a unique identifier to each user or a biometric access control device;
3. The entity takes steps to safeguard against unauthorized access to the system and forgery of electronic signatures;
4. The system includes a process to verify that the individual affixing the electronic signature has received the contents of the entry and determined that the entry contains what the individual intended; and
5. The policy must include: (a) a procedure by which each user of the system must certify in writing that the user will follow the confidentiality and security policies maintained by the entity for the system; (b) penalties for misusing the system; (c) training for all users of the system that includes an explanation of the appropriate use of the system and the consequences for not complying with the entity’s confidentiality and security policies. Revised Code § 3701.75.

An electronic signature for health records is defined as any of the following: “(a) a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual’s electronic signature; (b) a computer-generated signature code created for an individual; (c) an electronic image of an individual’s handwritten signature created by using a pen computer.” 3701.75(A)(2).

Policy/Procedure Considerations
Develop facility policies and procedures to include the following:
- Definition of Legal Record
  - What documents in EHR are part of legal medical record
  - Resident info versus administrative info
- Viewing
  - What can be viewed?
  - Procedures for resident viewing
- Printing
  - Who can print? When?
  - What is done when printed for reference only
- Procedures for viewing by physicians, surveyors, pharmacist, consultants, etc.
- Notice of electronic documentation
- Temporary logins
- Access only for those who would have access to paper record
- Continuity of care
- Response to subpoena or court order or oversight
- Valid release of information
  - Downtime and disaster recovery
    - Documentation process during downtime
    - Disaster planning
    - Recovery process
  - Storage and retention
    - Method
    - Retention requirements
    - Back up procedures
    - Access procedures for archived records, change in ownership
  - Purging and destruction
  - Training
    - All staff that access the medical record
    - Include everyone who needs to view as well as those who enter data
    - Review policies and procedures in addition to application use
    - Inservice staff regularly on policies and procedures, monitor compliance
  - Implementation

**Educational Considerations**
- Classes are most efficient, department meetings may be an alternative
- One-on-one training can focus at the provider's level of skill but is much more labor intensive.
- Training session are recommended to be brief (10 to 30 minutes) and focused on exactly what providers need to know to use the system and understand any work flow and policy changes.
- Trainers should have flexible schedules to allow informal support for a period following going live.
- Training super-users as trainers and to provide go-live support spreads training and support over a broader base and closer to end users. Checklists should be used to reduce the risk of inconsistency when multiple trainers are used.
- Use of video, CD-ROM, or Web-based training methods may be good training adjuncts
- Include screen shots in handouts or guides
- Providers should sign confidentiality agreements as part of the training process.
- If documents are to be signed in one system (e.g., an electronic signature module) and transferred to another system (e.g., the electronic health record), directions must be clear about where to sign documents electronically.
- If there are multiple electronic signature applications in the facility and the signing conventions differ, training must address the issue so distinctions in procedure can be pointed out to clinicians.
- Develop competency assessments to evaluate user knowledge and identify additional training needs.

**References/Resources**
- Health Policy Institute of Ohio, Assessing Health Information Technology in Ohio: [http://www.healthpolicyohio.org](http://www.healthpolicyohio.org)
- Ohio Department of Health, Ohio Administrative Code, Chapter 3701-17, Nursing Homes and Residential Care Facilities (Licensure Rules) [http://www.odh.state.oh.us/rules/final/chap17/fr17_1st.htm](http://www.odh.state.oh.us/rules/final/chap17/fr17_1st.htm)
- Ohio Revised Code (ORC) 3701.75, “Electronic Signatures”
- Ohio Administrative Code (OAC) 3701-17-13(B)(3) “Electronic signatures used to authenticate electronic records.”
- CMS Survey and Certification (S&C-05-14) Letter, “Electronic Signature Guidance Clarification”