ELECTRONIC HEALTH RECORDS

Medical Protective
Clinical Risk Management Department

AUGUST 2013

For questions, products, or services, please contact 800–4MEDPRO or visit http://www.medpro.com/. This document should not be construed as medical or legal advice. Since the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney if you have any questions related to your legal obligations or rights, application of state or federal laws, contract interpretation, or other legal questions that may potentially impact the applicability of the information provided in this document.

© The Medical Protective Company. 2013. All rights reserved.
## CONTENTS

**Introduction** .......................................................... 4

**Objectives** ..................................................................... 4

**Identification of Basic Workflow Features** ........................................ 5

  - Certification and Compatibility ........................................... 5
  - Other Important Considerations ........................................... 5

**System Features: Communication, Interoperability, and Security** .......... 6

  - Care Chronology ................................................................. 6
  - Intra-Office Communication ................................................ 7
  - Decision Support and Alerts ................................................ 7
  - Interoperability .................................................................... 7
  - Security ................................................................................ 8

**System Implementation and Maintenance** ..................................... 8

  - Defining the Legal Health Record ........................................ 8
    - Version Management ......................................................... 9
    - Output Format ..................................................................... 9
    - Record Retention ................................................................ 10

**Policies and Procedures** ........................................................ 10

  - Scanned Documents ........................................................... 10
  - Data Fields .......................................................................... 11
  - Abbreviations ...................................................................... 11
  - Copy/Paste .......................................................................... 11
INTRODUCTION

This guideline provides information about the use of electronic health record (EHR) systems to improve the quality and safety of patient care, while decreasing potential liability risk.

EHRs are defined as technology systems that electronically record and transmit information about patients captured during the regular course of business — e.g., clinical encounters and telephone contacts — to compile the legal health record.

When successfully implemented, EHRs create efficiencies in time and productivity, allowing healthcare providers to spend more quality time with patients, to see more patients, and/or to have less hectic schedules.

However, maximizing efficiencies could inadvertently result in various shortcuts that begin to degrade the patient safety benefits that EHRs offer. So, EHRs could actually create new errors and propagate old ones. Furthermore, those same efficiencies could create a roadmap for a plaintiff’s attorney to attempt to justify a legal action.

This guideline will serve as a patient safety and risk management guide concerning the use of EHRs. It will caution against the use (including nonuse, modified use, or improper use) of EHRs that may actually increase liability risk.

The guideline is not all-inclusive; rather it focuses on areas most likely to involve liability or make litigation more difficult to defend. This document should not be regarded as a stand-alone document for implementation of an EHR system.

OBJECTIVES

The objectives of this guideline are to:

- List necessary workflow considerations prior to purchasing or replacing an EHR system;
- Describe important system features that should be included in an EHR system;
- Provide a structure for system implementation and maintenance;
- Guide the development of robust policies and procedures; and
- Review the importance of having a contingency plan for when the EHR is unavailable.
IDENTIFICATION OF BASIC WORKFLOW FEATURES

Certification and Compatibility

The first consideration in the choice of an EHR system is whether the system has been certified by a government-approved entity, whose goal is to ensure interoperability and functionality. To find out whether a system is certified, go to http://oncchpl.force.com/ehrcert.

The next consideration is whether the system is compatible with community networks or large providers that influence a practice (hospitals or major third-party payers, etc.).

It may be prudent to contact or visit other healthcare professionals located in the same service area to discuss products and vendors. Further, soliciting their feedback regarding the installation, implementation, and maintenance of a system can be invaluable in the planning stages. If local comparisons are not an option, ask prospective vendors to provide references.

Include your office staff in the research, planning, testing, and system purchase decisions, and evaluate whether the potential product is compatible with their daily workflow.

Other Important Considerations

- How easy is it to access and manipulate the electronic data to meet the needs of your practice? Access to patient information should not be complicated, and the format should be as easy to read as a paper patient record.
- How will the system interface with other internal and external systems? Internal systems might include scheduling and billing systems. External systems to consider include hospitals, diagnostic entities, laboratories, pharmacies, and third-party payers.
- Will required interfaces add considerable cost or administrative steps to the transition?
- Is the vendor responsive to requests and needs?
- Is template language adaptable to fit the needs of the practice?
- What additional data needs exist? For example:
  - Research activities.
  - Pay-for-performance initiatives.
  - Internal performance improvement/data monitoring.
  - Specialty service needs, including system responsiveness to terminology, flow sheets, screenshots, or data sets that might need to be integrated into the system to facilitate specific practice activities. How much will
modifications cost? Can office staff easily modify the fields? Can programming logic be retained for future modifications?

- How will the system affect daily workflow processes? For example:
  - Chart retrieval and viewing: Are there standard system-wide views and customized views? The team should assess the readability and completeness of information.
  - Document and information capture:
    - How are scanned documents displayed?
    - Does the system electronically exchange information with other providers, health systems, pharmacies, third-party payers, etc.?
    - Does the system limit free text input (i.e., the ability to provide patient-specific notes and narrative)? Is text in narrative fields easily retrievable?
  - Chart completion: How does the system indicate that the chart is complete?
  - Release of information: Can you easily track released information?
  - Coding and abstracting: Will you need additional coding interfaces?
  - Transcription: Is the system capable of voice recognition?
  - Patient reminders and consultation letter templates: Are they easily formatted and automatically prompted?

**SYSTEM FEATURES: COMMUNICATION, INTEROPERABILITY, AND SECURITY**

The delivery of excellent care is dependent upon the accurate, understandable, complete, and timely communication of information. Evaluating the communication functions of an EHR system, in addition to evaluating the workflow processes as described above, is critical to the successful implementation of your system.

**Care Chronology**

For effective communication, certified EHR systems must reflect the continuous chronology of a patient’s care. This chronology of care includes a comprehensive problem list, a medication list consistent with medication reconciliation requirements, a complete patient history, and external clinical documents, such as lab and radiology reports (which are incorporated into the system via electronic interface or scanning technology). We will discuss how this clinical data should be arrayed and displayed in a subsequent section.
**Intra-Office Communication**

EHRs offer many features that assist in intra-office communication, including instant messages, task lists for completion of time-sensitive requirements, and quick access to medical records for reference in response to patient phone calls. All of these features can improve practice efficiencies, as long as they do not completely replace good interpersonal communication or become so overwhelming that the intended benefit is lost.

**Cautionary note:** Any information communicated through an electronic messaging feature — such as instant messages, patient portals, and emails — will be saved as metadata, even if the item is deleted. Metadata is “hidden data” that supports the entire EHR system. Examples of metadata include file properties and a tracked trail of changes to a document. These data could play an important role in a healthcare malpractice claim.

For additional information, consult the American Health Information Management Association’s (AHIMA’s) Practice Brief *Rules for Handling and Maintaining Metadata in the EHR* (link provided in the “Resources” section of this guideline).

**Decision Support and Alerts**

Another important communication feature of EHRs is their decision support capabilities, which include customizable care path templates and alert functions. These supports — which can be built in, subscription-based, or accessed via the web or a network — should be evidence-based and validated/accepted by professional organizations.

However, be mindful of “alert fatigue,” which can occur if providers are inundated with constant and/or unnecessary alerts. If frequent disregard of alerts occurs because of inappropriateness or insensitivity of the measure within the practice, consider reprogramming or changing alert functions to better fit the practice’s needs — but only if compatible with standards of care.

Frequent lack of compliance with alerts may reduce the effectiveness of the intended feature and lead to less-than-desirable patient outcomes. Your organizational policy should define the extent of exception documentation required.

**Interoperability**

Interoperability refers to the capacity of EHR systems to communicate with the electronic systems of other caregivers and provider facilities. Interoperability includes electronic transmission of prescriptions through a pharmacy interface and ordering diagnostic tests.
Note: No matter the interface capabilities, the system should support test tracking (such as the identification of outstanding test results) and flag potential medication interactions and patient allergies.

Security

Your practice should maintain a detailed plan for security of information, including electronic data. The plan should adhere to HIPAA guidelines, federal and state patient confidentiality tenets, and information technology standards.

It is also recommended that practices have backup recovery plans and detailed processes for documentation when the system is down and when it becomes available again. Work closely with your vendor to identify and fully understand all of the safety and privacy features of your EHR system.

System Implementation and Maintenance

Once an EHR product has been selected, the team should collectively plan transitional elements and an implementation timeline. An important component is education of current and future staff. Additionally, policy statements should be written for each phase of the plan.

The team should plan for periodic reviews and audits as members learn to work in the new environment so that the processes can be refined to enhance safety and performance.

Further, the vendor should be given a written set of expectations related to timelines, templates, policies, and procedures. The vendor’s commitment to supporting the practice during the implementation process should be required in writing.

Defining the Legal Health Record

The first step in implementing an EHR system is to write a policy statement defining the legal health record. In the policy, the organization should list and define the elements that will be standard in the patient record.

The policy should also describe how the record will appear in print format. This is important because it (a) determines the information that may or may not be disclosed upon request, (b) establishes consistency in the way that clinical information is arrayed and displayed for different data, and (c) lists documentation that should be retained and protected for required periods of time.

AHIMA’s practice brief Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes provides information on determining the health record content (link provided in the “Resources” section of this guideline). Other legal health record considerations include version management, output format, and record retention.
**Version Management**

Some considerations related to version management include the following:

- At what point is documentation considered complete? EHRs should be able to track corrections or changes once an entry has been made. Metadata will maintain a record of all changes made, including date, time, and author stamp.

- Will all versions be displayed or just the most recent version? Who is authorized to access the various versions? What visual clues are provided to alert the reader of the existence of other versions?

- Whose signatures are required to authenticate an entry? “Authentication” refers to a process that ensures and validates data accuracy and integrity by means of digital signatures or authentication codes. Authentication also signifies that the record has not been altered or improperly modified and is consistent with state and federal statutes.

- Whose signatures are required to validate changes? This ensures that no changes can be made without permission.

Policies related to version control should include audit mechanisms to validate completion of records (also important for billing purposes) or review modifications or corrections to the records, including who signed off on them. All final entries should be permanent and rules should be set forth to prevent alteration, tampering, or loss (covered in subsequent sections).

Policies also should define timeliness for each component of the EHR system, e.g., how long a record can remain incomplete.

**Output Format**

Some considerations related to output format include the following:

- The use of electronic and imaged health records is governed by state and federal law, including HIPAA and compliance standards. Ensure that your EHR policies and procedures comply with the appropriate state and federal laws, and consider consulting with an attorney during this process.

- EHR systems should produce output that chronicles patient encounters, and the record should reflect the chronology of the care given during these encounters. The timeline should be apparent in any given view.

- The record should be formatted to enhance readability and continuity of patient information. This ensures that the record, when printed for the patient or in response to other legitimate requests, will be logical and understandable. The vendor should assist with this process.
● Various disclosure requests — e.g., from legal entities, insurance companies, patients, etc. — will likely result in the need for different types of output formats/views. Privacy and security standards should be adhered to at all times.

● An organizational policy should determine (a) the rationale and authority for system access and data output, and (b) whether a record should be completed before output is generated.

● The organization’s statement that defines the legal health record should state whether certain privileged information will be excluded based on certain requests, such as mental health information or information obtained outside of the requested timespan.

● Strict control of printing policies should be in place. Printing should be tracked by an audit. When a central data repository is accessed by many users, the organization should define what information may be printed, when, and by whom. Printer output should be permanent; ink-jet printer ink is usually water-soluble, so laser printers are preferred.

Record Retention

Some considerations related to record retention include the following:

● Retention policies should be developed based on state and federal guidelines, special patient requirements, and research, legal, or compliance needs.

● Polices should address backup procedures to ensure retention and protection against data loss, including data from text, audio, video, and images.

● Policies should define purging data versus archiving, and how the EHR system supports both.

● If multiple systems are used, retention policies should be applied to each component but should also be adaptable to special needs.

Policies and Procedures

Policies and procedures for the EHR system should address several key items, including scanned documents, data fields, abbreviations, copy/paste, corrections/amendments, and patient communication.

Scanned Documents

All scanned documents should be legible, dated, and time-stamped. Some states mandate retention of original hardcopy documents along with electronic versions. In these cases, the documents should be cataloged and maintained in a secure environment. When appropriate, destruction of such records should abide by written protocols and state statutes for record destruction.
The team should develop a schedule for scanning current paper records and consider microfilming paper records that might have a long-term value. (For example, state laws often require longer retention periods for pediatric and occupational medicine records.)

**Data Fields**

All data fields should be linked to patient and record, and patient identification should appear on every page that is viewed, printed, or transmitted. Every entry should have a real-time date stamp and be associated with a signature when the entry is completed.

**Abbreviations**

Abbreviations should be avoided and eliminated from formatted templates or entry lists/choices as much as possible. When they are used, they should be standardized within the practice. Voice recognition or transcribed documents may be formatted or programmed to eliminate abbreviations.

**Copy/Paste**

This functionality can pose significant risk. Copied and pasted data may not reflect current information or may be placed in the wrong patient encounter or record. Also, the original author’s identity may be lost, thereby invalidating use without the author’s knowledge or permission.

Copying and pasting can be avoided by devising boilerplate text or libraries of common/routine information. However, providers should always review the information entered to ensure accuracy and relevance.

**Corrections/Errors/Amendments**

In some circumstances, corrections, additions, or clarifications to patient care documentation are necessary and legitimate. In these cases, the chart should clearly reflect the progression of the amending actions. The organization should have a policy — consistent with system programming — that limits the timespan a document may remain in draft status.

Other considerations include the following:

- The system should have the ability to track corrections, amendments, and incomplete status.
- The original entry should remain viewable as an alternate version, and the reason for the change should be stated. An alert should be displayed signaling existence of another version after changes are made.
- The preferred method for correction is a strikethrough with commentary. If a hard copy was made, it should be retrieved and amended as well.
The organizational policy should define retraction, reassignment, and resequencing as follows:

- **Retraction**: Removing a misfiled document from a patient record and placing it in another record in the system. The document (entry) is not considered a part of the original record and does not remain visible to anyone. However, an annotation in the record notes that the retracted document has been relocated. It is recommended that the organization designate someone to print retracted documents and retain them in a cataloged file (with appropriate documentation remarks to justify/identify the situation).

- **Reassignment**: Moving a document from one episode of care to another within the same patient record. This is handled in the same manner as a retraction.

- **Resequencing**: Moving a document from one place to another in a specific record within the same episode of care. No annotation is required.

**Patient Communication and Reminders**

Good documentation practices include recording all interactions with patients and their representatives. The organizational policy should reflect that patient reminders are part of the defined legal health record.

Some systems will create automatic phone or email reminders. Patients should be asked their preferred method of contact, keeping confidentiality constraints at the forefront. Tracking and following up on missed appointments, screenings, and diagnostic tests also is important. System reports should facilitate this process.

**Contingency Plan**

As part of the EHR implementation process, consideration should be given to the possibility that the EHR may be unavailable at times due to power outages, system crashes, connectivity to remote sites, property loss, or other causes. Thus, the organization should have a plan for ensuring continuity of patient care, including reversion to paper-based records that can be scanned into the EHR upon recovery.

Ensure that all staff is aware of the contingency plan to minimize disruption and prevent loss of patient information. Following restoration of the EHR, make sure that alerts that may have been triggered during the unavailable period are not lost. As with any technology, you should backup files offsite — or ensure that your vendor does so — on a frequent and regular basis to guard against permanent loss.
CONCLUSION

The EHR is not just a chart or record but a system for managing patient care. Tests and treatments can be managed from central locations electronically or at least without necessitating the patient’s presence at the provider site. Data are available for analysis that will justify ongoing evidenced-based changes to treatment modalities. Patients will have more access to their own information and will find it easier to participate in their care. And, reimbursement is changing to a system predicated on outcomes and compliance with evidence-based standards.

These changes have increased pressure on healthcare providers to implement modalities capable of supporting new infrastructures and networks. Yet, through it all, the basic need for maintenance of a patient health record will abide.

Good documentation will remain the best means of memorializing and communicating patient health status and plans of care. Patient records should be maintained in a manner that follows applicable regulations, accreditation standards, professional practice standards, and legal standards.

Medical Protective will support this process by helping healthcare professionals answer challenging questions and find solutions to newly identified practice needs.

RESOURCES


- The Office of the National Coordinator for Health Information Technology: Providers & Professionals — [http://www.healthit.gov/providers-professionals](http://www.healthit.gov/providers-professionals)