5. Quality, Safety, and the Electronic Medical Record

Carter Smith and Gretchen Purcell Jackson

Introduction

Electronic medical records (EMRs) are becoming increasingly prevalent across clinical settings, and as any other new technology, they have the potential both to enhance and to compromise the quality of medical care and patient safety. This chapter provides an introduction to the basic quality and safety issues pertinent to the adoption and use of EMRs by practicing surgeons.

Security and Privacy

EMRs provide a large amount of confidential information in a single, often easily searchable place. Concerns of healthcare providers, administrators, and patients regarding the use of EMRs commonly involve issues of privacy and security. This section describes the procedures and policies necessary for protecting electronically stored health information.

Authentication

Authentication is the process of verifying the identity of a person who accesses the medical record. Login procedures requiring individual usernames and passwords are the most common form of authentication. To provide robust security, the passwords must be increasingly complex to prevent unauthorized access. The best way to enhance the strength of a password is to increase the total number of possible character combinations, usually by requiring a greater number of characters and the use of upper

D.S. Tichansky, J. Morton, and D.B. Jones (eds.), *The SAGES Manual of Quality, Outcomes and Patient Safety*, DOI 10.1007/978-1-4419-7901-8_5,

case, lower case, numerical, and special characters. Remembering these long and complex passwords is difficult, but may be simplified by system integration so that one password is recognized across all systems. Ultimately passwords are a relatively vulnerable security measure. A computer program can systematically generate thousands or even millions of passwords per second until it guesses correctly or make more intelligent attempts using dictionary words or user information such as family names and birth dates. Malicious software can record username and password combinations as they are entered. System-level protections against such threats include login delays after the entry of incorrect passwords or lockouts after multiple failed attempts. Virus protection and regular system re-imaging, a process that reinstalls clean copies of software on shared workstations periodically, can reduce the risk of exposure to malicious software.

To enhance the security, many systems utilize some form of *multifactor authentication*, which necessitates more than one independent method to identify a user. Identify verification may occur through something a user knows, such as a password or personal identification number (PIN); something a user has, such as a digital token or smart card; or biometrics, such as fingerprints or retinal scans. These systems can be costly and are not without failures, but they are much more secure than password-only systems.

Authorization

Authorization is the permission for a user to access specific data or to perform certain actions (cm, such as writing orders). In an ideal world, only providers who need a patient's record should be able to access to it, but many EMRs provide broad authorization to all healthcare providers. Some systems allow individuals or groups of users to be assigned varied privileges so that they can only see or use the parts of the chart that are relevant to them. These safeguards can protect patients from malicious breaches in confidentiality and prevent a well-intended clinician from inadvertently reading the wrong chart or writing an order on an incorrect patient.

Encryption

The personal health information contained in an EMR is vulnerable to security breaches not only during active clinical use, but also during storage and transmission. Most EMRs employ some form of encryption.

Encryption is the process of transforming information to make it unreadable to anyone or anything without specific key or algorithm used to convert the data to a readable form.

Network-Level Security

Most EMRs reside on computer networks that not only interact within a healthcare system but also allow broad access to the Internet. Network-level security protects confidential health information from threats that can occur through such network connections. Firewalls are employed in many networks to monitor and restrict data communications. A *firewall* is a hardware and/or software barrier between networks that inspects the communications between them and stops unauthorized transmissions.

Clinicians often need access to EMRs from locations remote from their primary hospital or clinic, and they may need to use public networks that are far less secure than those provided by their institution. A *virtual private network* (VPN) allows users from outside of a firewall to share secure access to a network as if they were within it. There are various types and implementations of VPNs, but most use a combination of authentication and data encryption methods to protect the communications between the remote user and the network. These technologies offer safe access of patient information to healthcare providers while at home, traveling, or practicing at off-site locations.

User-Level Security

Clinicians who adopt EMRs are important components of security process, and they often must learn new behaviors to fulfill their responsibilities to protect confidential patient health information. Passwords should never be written down, shared with other users, or sent over email, text messages, or telephone. Healthcare providers should adopt strong security practices for password selection and maintenance. Using upper and lower case letters, as well as numbers, and creating longer passwords make the possible combinations larger and protect against brute force attacks. Changing passwords often prevents old password breaches from turning into new ones. It is extremely bad practice to use identical passwords for multiple accounts, and providers who use the same or similar passwords for accessing EMRs and personal electronic accounts (e.g., banks, email, or social networks) threaten their personal information in addition to that of their patients.

Secondary devices for authentication such as secure identification tokens or smart cards must be secured and reported if missing, just as one might report a lost license or credit card. Laptops and now even cellular telephones can be portals into the personal health information of patients. Users must remember to log out, and any device used to access the medical record should never be left unattended. Stolen or missing communication tools should also be reported promptly, especially if logins to secure systems are done automatically [1, 2].

Quality and Safety Issues

The implementation and adoption of an EMR is a complex social, organizational, and technological process that often requires not only a substantial investment in hardware, software, and technical support, but also significant workflow redesign, employee education, and ongoing process evaluation. The EMR can potentially impact every aspect of quality and safety in hospital and ambulatory care, and the informatics literature provides evidence for both considerable benefits and alarming adverse events resulting from the introduction of EMRs. This section focuses on strategies for maximizing benefits and minimizing harm to improve quality of care and patient safety through use of EMRs, based on the recommendations of several leading experts [3, 4].

Questions to Address When Selecting and Implementing an EMR

The goals of minimizing harm and maximizing benefit are accomplished by both the selection of EMR software, its implementation, and monitoring of the system. The answers to the questions below can guide the EMR committee through this process.

1. *Are we selecting appropriate software and hardware?* The EMR software must be able to accomplish the required clinical activities and not disrupt clinician workflow. Emergency departments and operating rooms function very differently than inpatient or outpatient environments. The proposed software must also seamlessly interface with or replace existing hospital infrastructure such as the laboratory and radiology systems.

In addition, the software must be supported by proper hardware. Potential hardware additions and upgrades should be included in the selection process and budget. For example, additional computer workstations may be needed to facilitate clinician access.

2. *Is the system content up to date?* With the EMR, there is great potential for benefit through use of clinical decision support. The content used to drive such features must be evidence based, up to date, and error free. Logic controlling medication allergies and interactions, clinical alerting and reminders, order-entry safety checks, and specialty-specific features (e.g., postoperative order sets) must be properly implemented and maintained. It is important to identify how errors will be corrected and how new information will be incorporated in a timely manner. Additionally, adherence to communication and vocabulary standards like the Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT) and Health Level Seven electronic interchange standard encourage the application of advanced clinical decision support and information exchange through uniform and defined languages.
3. *How does the user interface affect groups of users?* It is important to consider how the system delivers information to each group of users. The specific needs of the surgeon are discussed in the next section. Pertinent information may vary across provider types, clinical environments, and specialty groups, and each may have separate needs for data entry and display. A system should be flexible enough to address diverse needs without creating confusion and communication breakdown with excessive customization. The modern clinician may want to use advanced technologies such as voice recognition and mobile devices to enter and access clinical data, and careful consideration must be given to the associated advantages and costs (e.g., interface adaptation and user training).
4. *What support personnel will we have?* It is crucial that ample support personnel be identified whether from within the institution or through outside agreements. Training staff is vital to implementation as well as integration of new users. Software engineers and other technical staff are needed to provide continued software updates and address issues as they arise, especially after hours. Inpatient facilities and other practices that care for patients overnight may need a special system to

solve problems that arise outside of typical business hours. Personnel needs in all of these areas may be significantly higher during the initial implementation of a new system.

5. *How will workflow be affected by this new system?* The implementation of an EMR usually requires changes to existing workflows. A thorough review of existing and proposed communication processes and information exchanges can potentially improve safety and optimize workflow; a failure to understand such changes can introduce errors and frustrate users. This process may require a multidisciplinary team of software designers, developers, trainers, policy makers, clinicians, and maintenance staff. Analysis of clinical workflows should be initiated early and continue through implementation to address risks that are foreseen as well as those that arise during use.
6. *What methods for testing the system are in place both before and after implementation?* System testing may be able to identify problems and workflow issues so that they can be addressed before there is potential for patient harm. Testing may be undertaken by the software manufacturer, by the local institution, or both. It is important to develop a plan for robust usability and performance testing both before implementation and during ongoing use. Testing may require time commitment of clinical staff as well as support personnel, and the associated costs must be anticipated.
7. *How will we report and study bugs, safety flaws, and incidents?* To address user concerns and to enhance EMR safety, it is important to have well-established internal and external processes for reporting and addressing flaws and incidents as they are identified. Each institution and its supporting vendors must specify a system for reporting of events and developing solutions to them. It is critical to recognize the limitations of local and institutional support personnel and to know when problems or errors require higher level intervention. Several authors have proposed federal oversight of this process as well as federal reporting to produce aggregate data [3, 4]. Partnering with other groups with common patients, software systems, or infrastructure may allow for creation of a knowledge base of risks, adverse events, and solutions. Collaborative groups can be invaluable in identifying common patterns of errors and deficiencies.

8. *What are the most recent state and federal regulations for EHRs and does our system address them?* Both the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the American Recovery and Reinvestment Act (ARRA) of 2009 have placed specific requirements on EMRs, and many details of the latter regulations are still in evolution [5, 6]. Both federal and state legislation have the potential to change and vary as more institutions implement electronic systems and federal oversight increases. Individuals and institutions with systems that meet the most current requirements may be eligible for financial incentives, and those that do not may be subject to a variety of penalties or punishments.

EMR Functions for the Surgeon

Surgeons as a group have unique needs from the EMR, and each surgical specialty may require particular functions or customizations for their practices. Surgeons are encouraged to participate in EMR advisory committees and test groups to insure their requirements are being met. This section discusses essential and desirable EMR features for surgeons.

Some general requirements for EMRs are shared across specialties. The surgeon practices from many locations including the emergency room, outpatient clinics, the operating room, and the intensive care unit, or even from home or while traveling. The EMR must be *accessible* from a variety of locations and ideally *portable* with access through the Internet and smart phones. *Installation services* and *training* are essential pieces of the overall package from the EMR vendor, and as are superior *service* and *support*. Ongoing support both during the installation period and after are important considerations. These services can be undertaken by the vendor or by the institution, but adequate support is absolutely essential. The *customizability* of the system for the needs of individual specialties or practice groups is a desirable feature. System-wide or specialty-wide customization is more practical than tailoring at the user level due to the difficulty of providing support when each user setup is unique. Because the implementation of a complete system or specialty-specific features may be prohibitive due to cost, training, or workflow limitations, a system's *modularity* and *extensibility* can allow for integration of additional components or customization as resources become available. In addition, *interoperability* between the new system and existing information systems is vital. It may be necessary to consider upgrades or replacements to existing laboratory, radiology, billing, dictation, and pathology systems to support compatibility. Finally, there must be plan for maintaining or integrating old records, either paper or electronic formats.

Surgery is an anatomically oriented specialty, and thus, it is particularly important that EMRs be able to incorporate *clinical and radiographic images*. Images may be acquired using the Diagnostic Image Communication Of Medicine (DICOM) transmission standard, or in non-DICOM formats (e.g., wound photographs and intraoperative photos), so inclusion of both DICOM and non-DICOM images is desirable, as is the ability to include and display and annotate a variety of multimedia from anatomic drawings to operative videos. If the institution uses an external picture archiving and communication system (PACS), it is useful for this system to be integrated with the EMR.

Many EMR vendors now support *electronic informed consent*, which can be particularly useful for procedurally oriented specialties. Such modules may also incorporate *educational materials, preoperative and postoperative instructions*, and relevant anatomic drawings, which can expedite clinical workflow and reduce liability risks. Surgeons should ask about the availability of such information in various *languages* and for *multiple reading levels* [7, 8].

User-Level Quality and Safety Guidelines

Provider behaviors can contribute significantly to both the benefits and harms that result from use of EMRs. EMR systems vary substantially, but most require new approaches to clinical documentation. This section provides some practical guidelines for safe EMR use to provide high quality care.

Each document in the EMR should serve as a succinct, effective communication tool to facilitate care of the patient. As with paper records, providers should take the time to carefully and thoroughly record an assessment and plan. This synthesis of applicable data is arguably the most important part of a provider's documentation and what marks a good clinician. Depending on individual skills and system support, this process may take longer than jotting a note in a paper chart, but users should not cut corners on any critical documentation (e.g., consent and procedure notes).

Similarly, important recommendations should not be buried in pages of erroneous data simply because it is easy to incorporate information from previous documents. EMR users should avoid excessive “reuse” or “copy and paste” functions because these tools inevitably introduce errors without careful editing. Although the duplication of information is often motivated by documentation requirements for maximal reimbursement, payers may deny compensation if the information is clearly copied, especially when incorrect data are introduced (e.g., a postoperative day or incorrect preoperative diagnosis is not updated). The same principles apply to using templates that automatically fill documents with data from other sources or standard text. These tools should be used with caution, and all text should be reviewed carefully for accuracy before saving.

Clinical decision support in the form of warnings and recommendations provide great potential for improvement of patient care and prevention of medical mistakes as well as common sources of EMR user frustration. It is important not to blindly click through such notifications. Likewise, it is critical that clinicians insist that the rules that drive the clinical alerts are driven by solid evidence and practice guidelines. Warnings must be clinically important and consistently relevant to the situation to be heeded and to avoid establishing a reflex reaction to ignore such alerts. It is essential that practicing clinicians participate actively in creating useful and pertinent decision support modules, and their contributions to quality and safety be evaluated in an ongoing manner [4].

Regulatory Issues

The Legal Electronic Medical Record

The EMR must meet regulatory requirements for a legal medical record. While the complete specifications for a legal medical record are beyond the scope of this chapter, this section highlights some of the most important considerations.

A unique record must exist and be maintained for each patient, and some key components of documentation must be included. The author, time, and date must be recorded accurately for each element added to the record. It is important to determine how successive versions of documentation are treated both before and after a signature is applied. The signature procedure must meet qualifications both legally and professionally. All corrections, amendments, or clarifications must be clearly noted.

The safe guards that are in place to prevent access without authorization must also prevent unauthorized alterations in both the individual record and system databases. Access audits and document version histories should be available to reproduce event timelines if needed. Additionally, policies and procedures should be defined for alterations and amendments to system components including templates and clinical decision support as well as for record retention, archiving, data reporting, and other forms of data abstraction [9].

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 specified two rules – the privacy and security rules – as they apply to patient identifiable information and those who transmit and receive this information. The privacy rule established a standard for the protection of personal health information. The security rule defined a national set of security standards for protecting certain health information that is held or transferred in electronic form. It specified how this information may be disclosed and what protections must be in place to prevent unauthorized access or disclosure. It also required that covered entities must create privacy policies and train workforce members as well as safeguard their data and mitigate harmful effects caused by disclosure of this type of information. Most clinicians are familiar with the concept that protected health information may only be transmitted and disclosed under certain guidelines according to this legislation. For the implementation of an EMR system, four types of security are needed: (1) physical security – the data storage must be in a location that prevents theft of data; (2) user security – efforts to prevent unauthorized access need to be in place; (3) system security – procedures and policies must protect the information from damage or destruction, and backup files in remote locations may be needed to safeguarded from fire, flood, or system crashes; and (4) network security – protection of the data while in transit and storage, and prevention of access to data from outside of the system [6].

The American Recovery and Reinvestment Act

The American Recovery and Reinvestment Act of 2009 (ARRA) is an economic stimulus package that was signed into law in February of 2009 and includes the Health Information Technology for Economic and

Clinical Health (HITECH) Act, which allocated $19.2 billion in funding to increase the use of EMRs. In the HITECH Act, Congress provides Medicare and Medicaid payment incentives to individual providers and hospitals that adopt certified EMR technologies and achieve "meaningful use." Short-term incentives that begin in 2011 are replaced by penalties in 2015 for failure to accomplish meaningful use of a certified EMR.

One of the most controversial aspects of this legislation is the definition of "meaningful use." Stage I criteria for meaningful use were issued in July of 2010 with planned biennial updates to these criteria to achieve "health care that is patient-centered, evidence-based, prevention-oriented, efficient, and equitable." To qualify for incentive payments, individual providers must complete 15 core and 5 additional of 25 meaningful use objectives; hospitals must achieve 14 core and 5 additional of 24 meaningful use objectives. Core objectives include the use of computerized order entry, maintenance of up-to-date problem, medication, and allergy lists, implementation of clinical decision support rules, and providing patients with electronic copies of health information and discharge summaries. Optional objectives include recording advanced directives for patients 65 years old or older and sending reminders for preventative care to patients according to their preferences. In addition to meeting these objectives, individuals must report 6 and hospitals must report 15 clinical quality measures to achieve meaningful use criteria. Examples of clinical quality measures are blood pressure measurements and tobacco use assessments for individual providers and measures of emergency department throughput for hospitals.

Realistically, the financial incentives are small compared to the costs of adopting and maintaining high quality EMRs, and thus, they are not the best reason to strive for meaningful use of EMR technologies. The proper application of healthcare information technology can lead to improvements in the quality and safety of care provided, and this legislation represents an emerging trend toward government requirements and oversight for EMR use [5, 10].

Selected Readings

1. Shortliffe EH, Cimino JJ. Biomedical informatics: computer applications in health care and biomedicine. New York: Springer; 2006.
2. Security aspects in electronic personal health record: data access and preservation. http://www.digitalpreservationeurope.eu/publications/briefs/security_aspects.pdf.

3. Sittig DF, Classen DC. Safe electronic health record use requires a comprehensive monitoring and evaluation framework. JAMA. 2010;303:450–1.
4. Walker JM, Carayon P, Leveson N, Paulus RA, Tooker J, Chin H, et al. Stewart WF: *EHR safety: the way forward to safe and effective systems*. J Am Med Inform Assoc. 2008;15:272–7.
5. 42 CFR Parts 412, 413, 422 et al. Medicare and Medicaid Programs.
6. Electronic Health Record Incentive Program. Final Rule. *Federal Register.* 2010;75:44314–588.
7. Health Information Privacy [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html].
8. Mukherjee K, Jackson GP. Optimal EMR system criteria offered. Surgery News. 2009;5:3–4.
9. Schwaitzberg SD. Successful implementation of EMR in your practice: I work in a large hospital. If they ask me what I need, what should I tell them? Presentation at the American College of Surgeons 94th Annual Clinical Congress, San Francisco, CA.
10. The legal electronic medical record [http://www.himss.org/content/files/LegalEMR_Flyer3.pdf].
11. Baron RJ. Meaningful use of health information technology is managing information. JAMA. 2010;304:89–90.