Virtual Mentor
American Medical Association Journal of Ethics
September 2012, Volume 14, Number 9: 712-719.

STATE OF THE ART AND SCIENCE

Electronic Health Records: Privacy, Confidentiality, and Security

Laurinda B. Harman, PhD, RHIA, Cathy A. Flite, MEd, RHIA, and Kesa Bond, MS, MA, RHIA, PMP

Health Information Systems: Past and Present

To understand the complexities of the emerging electronic health record system, it is helpful to know what the health information system has been, is now, and needs to become. The medical record, either paper-based or electronic, is a communication tool that supports clinical decision making, coordination of services, evaluation of the quality and efficacy of care, research, legal protection, education, and accreditation and regulatory processes. It is the business record of the health care system, documented in the normal course of its activities. The documentation must be authenticated and, if it is handwritten, the entries must be legible.

In the past, the medical record was a paper repository of information that was reviewed or used for clinical, research, administrative, and financial purposes. It was severely limited in terms of accessibility, available to only one user at a time. The paper-based record was updated manually, resulting in delays for record completion that lasted anywhere from 1 to 6 months or more. Most medical record departments were housed in institutions' basements because the weight of the paper precluded other locations. The physician was in control of the care and documentation processes and authorized the release of information. Patients rarely viewed their medical records.

A second limitation of the paper-based medical record was the lack of security. Access was controlled by doors, locks, identification cards, and tedious sign-out procedures for authorized users. Unauthorized access to patient information triggered no alerts, nor was it known what information had been viewed.

Today, the primary purpose of the documentation remains the same—support of patient care. Clinical documentation is often scanned into an electronic system immediately and is typically completed by the time the patient is discharged. Record completion times must meet accrediting and regulatory requirements. The electronic health record is interactive, and there are many stakeholders, reviewers, and users of the documentation. Because the government is increasingly involved with funding health care, agencies actively review documentation of care.

The electronic health record (EHR) can be viewed by many users simultaneously and utilizes a host of information technology tools. Patients routinely review their electronic medical records and are keeping personal health records (PHR), which

contain clinical documentation about their diagnoses (from the physician or health care websites).

The physician, practice, or organization is the owner of the physical medical record because it is its business record and property, and the patient owns the information in the record [1]. Although the record belongs to the facility or doctor, it is truly the patient's information; the Office of the National Coordinator for Health Information Technology refers to the health record as "not just a collection of data that you are guarding—it's a life" [2]. There are three major ethical priorities for electronic health records: privacy and confidentiality, security, and data integrity and availability.

Privacy and Confidentiality

Justices Warren and Brandeis define privacy as the right "to be let alone" [3]. According to Richard Rognehaugh, it is "the right of individuals to keep information about themselves from being disclosed to others; the claim of individuals to be let alone, from surveillance or interference from other individuals, organizations or the government" [4]. The information that is shared as a result of a clinical relationship is considered *confidential* and must be protected [5]. The information can take various forms (including identification data, diagnoses, treatment and progress notes, and laboratory results) and can be stored in multiple media (e.g., paper, video, electronic files). Information from which the identity of the patient cannot be ascertained—for example, the number of patients with prostate cancer in a given hospital—is not in this category [6].

Patient information should be released to others only with the patient's permission or as allowed by law. This is not, however, to say that physicians cannot gain access to patient information. Information can be released for treatment, payment, or administrative purposes without a patient's authorization. The patient, too, has federal, state, and legal rights to view, obtain a copy of, and amend information in his or her health record.

The key to preserving confidentiality is making sure that only authorized individuals have access to information. The process of controlling access—limiting who can see what—begins with authorizing users. In a physician practice, for example, the practice administrator identifies the users, determines what level of information is needed and assigns usernames and passwords. Basic standards for passwords include requiring that they be changed at set intervals, setting a minimum number of characters, and prohibiting the reuse of passwords. Many organizations and physician practices take a two-tier approach to authentication, adding a biometrics identifier scan, such as palm, finger, retina, or face recognition.

The user's access is based on preestablished role-based privileges. In a physician practice, the nurse and the receptionist, for example, have very different tasks and responsibilities; therefore, they do not have access to the same information. Hence, designating user privileges is a critical aspect of medical record security: all users have access to the information they need to fulfill their roles and responsibilities, and

they must know that they are accountable for use or misuse of the information they view and change [7].

Under the HIPAA Privacy and Security Rules, employers are held accountable for the actions of their employees. In 2011, employees of the UCLA health system were found to have had access to celebrities' records without proper authorization [8]. UCLA failed to "implement security measures sufficient to reduce the risks of impermissible access to electronic protected health information by unauthorized users to a reasonable and appropriate level" [9]. The health system agreed to settle privacy and security violations with the U.S. Department of Health and Human Services Office for Civil Rights (OCR) for $865,000 [10]. Controlling access to health information is essential but not sufficient for protecting confidentiality; additional security measures such as extensive training and strong privacy and security policies and procedures are essential to securing patient information.

Security

The National Institute of Standards and Technology (NIST), the federal agency responsible for developing information security guidelines, defines *information security* as the preservation of data confidentiality, integrity, availability (commonly referred to as the "CIA" triad) [11]. Not only does the NIST provide guidance on securing data, but federal legislations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act mandate doing so. Violating these regulations has serious consequences, including criminal and civil penalties for clinicians and organizations.

The increasing concern over the security of health information stems from the rise of EHRs, increased use of mobile devices such as the smartphone, medical identity theft, and the widely anticipated exchange of data between and among organizations, clinicians, federal agencies, and patients. If patients' trust is undermined, they may not be forthright with the physician. For the patient to trust the clinician, records in the office must be protected. Medical staff must be aware of the security measures needed to protect their patient data and the data within their practices.

A recent survey found that 73 percent of physicians text other physicians about work [12]. How to keep the information in these exchanges secure is a major concern. There is no way to control what information is being transmitted, the level of detail, whether communications are being intercepted by others, what images are being shared, or whether the mobile device is encrypted or secure. Mobile devices are largely designed for individual use and were not intended for centralized management by an information technology (IT) department [13]. Computer workstations are rarely lost, but mobile devices can easily be misplaced, damaged, or stolen. Encrypting mobile devices that are used to transmit confidential information is of the utmost importance.

Another potential threat is that data can be hacked, manipulated, or destroyed by internal or external users, so security measures and ongoing educational programs must include all users. Some security measures that protect data integrity include firewalls, antivirus software, and intrusion detection software. Regardless of the type of measure used, a full security program must be in place to maintain the integrity of the data, and a system of audit trails must be operational.

Providers and organizations must formally designate a security officer to work with a team of health information technology experts who can inventory the system's users, and technologies; identify the security weaknesses and threats; assign a risk or likelihood of security concerns in the organization; and address them. The responsibilities for privacy and security can be assigned to a member of the physician office staff or be outsourced.

Audit trails. With the advent of audit trail programs, organizations can precisely monitor who has had access to patient information.

Audit trails track all system activity, generating date and time stamps for entries; detailed listings of what was viewed, for how long, and by whom; and logs of all modifications to electronic health records [14]. Administrators can even detail what reports were printed, the number of screen shots taken, or the exact location and computer used to submit a request. Alerts are often set to flag suspicious or unusual activity, such as reviewing information on a patient one is not treating or attempting to access information one is not authorized to view, and administrators have the ability to pull reports on specific users or user groups to review and chronicle their activity. Software companies are developing programs that automate this process. End users should be mindful that, unlike paper record activity, all EHR activity can be traced based on the login credentials. Audit trails do not prevent unintentional access or disclosure of information but can be used as a deterrent to ward off would-be violators.

The HIPAA Security Rule requires organizations to conduct audit trails [12], requiring that they document information systems activity [15] and have the hardware, software, and procedures to record and examine activity in systems that contain protected health information [16]. In addition, the HITECH Act of 2009 requires health care organizations to watch for breaches of personal health information from both internal and external sources. As part of the meaningful use requirements for EHRs, an organization must be able to track record actions and generate an audit trail in order to qualify for incentive payments from Medicare and Medicaid. HIPAA requires that audit logs be maintained for a minimum of 6 years [13]. As with all regulations, organizations should refer to federal and state laws, which may supersede the 6-year minimum.

Integrity and Availability

In addition to the importance of privacy, confidentiality, and security, the EHR system must address the integrity and availability of information.

Integrity. Integrity assures that the data is accurate and has not been changed. This is a broad term for an important concept in the electronic environment because data exchange between systems is becoming common in the health care industry. Data may be collected and used in many systems throughout an organization and across the continuum of care in ambulatory practices, hospitals, rehabilitation centers, and so forth. This data can be manipulated intentionally or unintentionally as it moves between and among systems.

Poor data integrity can also result from documentation errors, or poor documentation integrity. A simple example of poor documentation integrity occurs when a pulse of 74 is unintentionally recorded as 47. Whereas there is virtually no way to identify this error in a manual system, the electronic health record has tools in place to alert the clinician that an abnormal result was entered.

Features of the electronic health record can allow data integrity to be compromised. Take, for example, the ability to copy and paste, or "clone," content easily from one progress note to another. This practice saves time but is unacceptable because it increases risk for patients and liability for clinicians and organizations [14, 17]. Another potentially problematic feature is the drop-down menu. Drop-down menus may limit choices (e.g., of diagnosis) so that the clinician cannot accurately record what has been identified, and the need to choose quickly may lead to errors. Clinicians and vendors have been working to resolve software problems such as screen design and drop-down menus to make EHRs both user-friendly and accurate [17].

Availability. If the system is hacked or becomes overloaded with requests, the information may become unusable. To ensure availability, electronic health record systems often have redundant components, known as fault-tolerance systems, so if one component fails or is experiencing problems the system will switch to a backup component.

The Future

Some who are reading this article will lead work on clinical teams that provide direct patient care. Some will earn board certification in clinical informatics. Others will be key leaders in building the health information exchanges across the country, working with governmental agencies, and creating the needed software. Regardless of one's role, everyone will need the assistance of the computer.

Medical practice is increasingly information-intensive. The combination of physicians' expertise, data, and decision support tools will improve the quality of care. Physicians will be evaluated on both clinical and technological competence. Information technology can support the physician decision-making process with clinical decision support tools that rely on internal and external data and information. It will be essential for physicians and the entire clinical team to be able to trust the data for patient care and decision making. Creating useful electronic health record systems will require the expertise of physicians and other clinicians, information

management and technology professionals, ethicists, administrative personnel, and patients.

References

1. Odom-Wesley B, Brown D, Meyers CL. *Documentation for Medical Records*. Chicago: American Health Information Management Association; 2009:21.
2. Office of the National Coordinator for Health Information Technology. *Guide to Privacy and Security of Health Information*; 2012:5. http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed August 10, 2012.
3. Warren SD, Brandeis LD. The right to privacy. *Harvard Law Rev*. 1890;4:193.
4. Rognehaugh R. *The Health Information Technology Dictionary*. Gaithersburg, MD: Aspen; 1999:125.
5. Rinehart-Thompson LA, Harman LB. Privacy and confidentiality. In: Harman LB, ed. *Ethical Challenges in the Management of Health Information*. 2nd ed. Sudbury, MA: Jones and Bartlett; 2006:53.
6. Rinehart-Thompson, Harman, 54.
7. American Health Information Management Association. The 10 security domains (updated). *J Am Health Inf Management Assoc*. 2012;83(5):50.
8. University of California settles HIPAA privacy and security case involving UCLA Health System facilities [news release]. Washington, DC: US Department of Health and Human Services; July 7, 2011. http://www.hhs.gov/news/press/2011pres/07/20110707a.html. Accessed August 10, 2012.
9. US Department of Health and Human Services Office for Civil Rights. UCLA Health System settles potential HIPAA privacy and security violations. http://www.hhs.gov/ocr/privacy/hipaa/news/uclahs.html. Accessed August 10, 2012.
10. US Department of Health and Human Services Office for Civil Rights. Resolution agreement [UCLA Health System]. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/UCLAHSracap.pdf. Accessed August 10, 2012.
11. National Institute of Standards and Technology Computer Security Division. *An Introduction to Computer Security: The NIST Handbook*. U.S. Department of Commerce. Gaithersburg, MD: NIST; 1995:5. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html. Accessed August 10, 2012.
12. Greene AH. HHS steps up HIPAA audits: now is the time to review security policies and procedures. *J Am Health Inf Management Assoc*. 2011;82(10):58-59. http://www.ahimajournal-digital.com/ahimajournal/201110?pg=61#pg61. Accessed August 10, 2012.
13. American Health Information Management Association. Mobile device security (updated). *J Am Health Inf Management Assoc*. 2012;83(4):50.

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463. Accessed August 10, 2012.
14. American Health Information Management Association. Copy functionality toolkit; 2008:4. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042564.pdf#xml=http://library.ahima.org/xpedio/idcplg?IdcService=GET_XML_HIGHLIGHT_INFO&QueryText=%28cut+copy+and+paste%29%3Cand%3E%28xPublishSite%3Csubstring%3E%60BoK%60%29&SortField=xPubDate&SortOrder=Desc&dDocName=bok1_042564&HighlightType=PdfHighlight. Accessed August 10, 2012.
15. US Department of Health and Human Services. Security standards: general rules, 46 CFR section 164.308(a)-(c).
16. US Department of Health and Human Services. Technical safeguards. 45 CFR section 164.312(1)(b).
17. American Health Information Management Association. Auditing copy and paste. *J Am Health Inf Management Assoc*. 2009;80(1):26-29. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042416.hcsp?dDocName=bok1_042416. Accessed August 10, 2012.

Further Reading

American Health Information Management Association web site. http://www.ahima.org. Accessed August 10, 2012.

American Health Lawyers Association. *Red Flag Compliance for Health Care Providers: Protecting Ourselves and our Patients from Identity Theft Member Briefing*. Chicago: American Health Information Management Association; 2010.

American Medical Informatics Association web site. http://www.amia.org. Accessed August 10, 2012.

Amatayakul MK. *Electronic Health Records: A Practical Guide for Professionals and Organizations*. 5th ed. Chicago: American Health Information Management Association; 2012.

Amatayakul MK, Lazarus S. *Electronic Health Records: Transforming Your Medical Practic*e. Englewood, CO: Medical Group Management Association; 2010.

Baldwin KA, Ball K, Dougherty M, Hedges RJ. *e-Discovery and Electronic Records*. Chicago: American Health Information Management Association; 2012.

Dennis JC. *Privacy: The Impact of ARRA, HITECH, and Other Policy Initiatives*. Chicago: American Health Information Management Association; 2011.

LaTour KM, Eichenwald Maki S, eds. *Health Information Management: Concepts, Principles, and Practice*. 3rd ed. Chicago: American Health Information Management Association; 2010.

MGMA-AHIMA Smart Pack. *Health Information Technology: Implementing an Electronic Health Record in Physician Practices.* Chicago: American Health Information Management Association; 2006.

Trites PA, Gelzer RD. *How to Evaluate Electronic Health Records*. Chicago: American Health Information Management Association; 2008.

Wolter J. *The Personal Health Record*. Chicago: American Health Information Management Association; 2009.

Laurinda B. Harman, PhD, RHIA, is emeritus faculty at Temple University in Philadelphia. She has a bachelor of science degree in biology and medical records from Daemen College, a master of education degree from Virginia Polytechnic Institute and State University, and a PhD in human and organizational systems from Fielding Graduate University. Ethics and health information management are her primary research interests.

Cathy A. Flite, MEd, RHIA, is a clinical assistant professor in the Health Information Management Department at Temple University in Philadelphia. She earned her BS in health information management at Temple University, a master of education degree from Widener University, and a master of arts in human development from Fielding Graduate University. Her research interests include professional ethics.

Kesa Bond, MS, MA, RHIA, PMP, earned her BS in health information management from Temple University, her MS in health administration from Saint Joseph's University, and her MA in human and organizational systems from Fielding Graduate University. She was the director of health information management for a long-term care facility, where she helped to implement an electronic health record. Her research interests include childhood obesity.

Related in VM

Copying and Pasting Patient Treatment Notes, March 2011

Reassessing "Minor" Breaches of Confidentiality, March 2011

THE HITECH ACT—An Overview, March 2011

Ethical Dimensions of Meaningful Use Requirements for Electronic Health Records, March 2011

The "Decrepit Concept" of Confidentiality, 30 Years Later, September 2012

Would Patient Ownership of Health Data Improve Confidentiality? September 2012