JOURNAL OF CLINICAL RESEARCH BEST PRACTICES

Vol. 9, No. 10, October 2013 "Happy Trials to You"

Clinical Study Data, Electronic Medical Records, and Privacy

By Jeanne M. Mattern

The Affordable Care Act requires all U.S. healthcare providers to digitize all patient records by 2014 and place them in electronic medical records (EMRs).[1] This requirement is a boon to clinical research since it will, in theory, make all patient data (including certain clinical research data) accessible in a meaningful (structured and useable) form across the entire healthcare system. Clinical researchers can use this data to identify and screen potential research subjects, as well as to obtain health data during a study, e.g., about adverse events. This article will discuss privacy and other issues involved in making clinical research data accessible through EMRs.

An EMR can include data on all aspects of a patient's health history, including diagnoses (including STDs), disabilities, laboratory test results, prescriptions, treatments, progress notes, social/family history, sexual history, substance abuse and mental illness. Most patients thus prefer their EMR data to remain private. Since EMR records are often linked with a person's Social Security number, this data, in the wrong hands, could easily affect a person's health insurance availability and rates, credit, and educational and employment standing and opportunities. Further, medical records can include intimate details about a person's life and relationships that, if disclosed, could disrupt personal relationships or result in humiliation. As a result, healthcare organizations are required to protect the privacy of health information by multiple federal (and state) laws, including HIPAA, CFR 21 Part 11, ERISA, GCP, the Freedom of Information Act, the Gramm-Leach-Bliley Act, CLIA and others.[2-13]

Just as data from clinical care can be useful for clinical research, data from clinical research can be useful for clinical care, and subject to the same privacy concerns. For example, study data that should be included in the EMR includes the following:

- Information about the patient's clinical study participation
- Clinically significant data, e.g., diagnosis, treatment, laboratory and imaging results
- Clinical data initially recorded in the EMR (i.e., not specifically collected for research purposes)

Clinicians need access to their patients' clinical research data to provide appropriate treatment. They also need this information to determine whether a patient is a candidate for a clinical study. They need data from past clinical studies and information about current clinical studies. The obvious place to store this information is in the EMR, which is a repository of health-related information that provides tools for sharing clinically relevant data. Understanding how research data fits into the EMR helps clarify the role of research in the larger healthcare context.

Institutions should have clear policies and procedures on including study data in the EMR. The institutional review board (IRB) or privacy board should help create the policies and procedures, and review their application to specific instances. Prior to conducting a study, the study team should review the protocol for potential information of clinical significance and determine whether and how it will be recorded in the EMR.

Factors to Consider

Determining what study information should be recorded in a patient's EMR depends on multiple factors:

Studies and Patients Differ

At one extreme is the patient who participates in a very safe study that collects biospecimens to establish baseline data for a diagnostic device. At the other extreme is the advanced cancer patient who participates in a long series of clinical studies of various treatment combinations, with extensive adverse events. The privacy concerns of these patients also varies and in unpredictable ways. For example, the diagnostic device study might be for HIV/AIDS patients, some of whom care a great deal about privacy, while the advanced cancer patient might not care at all who knows about his condition. The data that can and should be recorded in the EMR for each patient thus also differs. However, if it is impractical to tailor the system for each patient, a general policy for the study is required.

EMR Systems Differ

The security and privacy of patient data within EMRs can vary.[11] An EMR system consists of the EMR software plus the policies and procedures for its use. For example, institutions can implement different rules for who can access which patient data under which circumstances. The rules can be enforced by the software or just policies and procedures, to varying degrees of reliability, depending on institutional culture and training programs.

One option is to create a secure section of the EMR for recording some or all clinical study information. This section might require special permission to access or just present a warning that it contains confidential or proprietary clinical study information. Data captured in accordance with what is required pursuant to the protocol should be noted in the EMR with a summary of results.

Data Differs

Not all clinical research data belongs in an EMR. For example, data from an experimental or unvalidated lab test could mislead clinicians. Non-standard or partial data can mislead. Genetic data, in particular, is often speculative and, thus, inappropriate for use by clinicians who are not expert in its interpretation.[10]

The "golden rule" for including data in an EMR is whether it will benefit the patient, especially his or her safety.[11] This rule can conflict with contractual obligations to a study sponsor. The sponsor might be concerned about potential liability if the use of study data contributes to an injury to the patient. Or, it might be developing a new lab test that requires nondisclosure to protect its intellectual property. Such concerns should be addressed with the study sponsor and might require special arrangements.

"Incidental findings" occur when data from a clinical study reveals an unrelated medical condition of importance to the patient. Clear evidence of a serious heart condition should be disclosed to the patient's physician. However, it may or may not be appropriate to disclose speculative evidence or data about an untreatable condition. An institution's policy on incidental findings should be consistent with its policy on including study data in the EMR.

Usefulness is Difficult to Predict

Information that appears inconsequential at present might prove later to be very important. For example, the half-life of a study drug in a patient's blood could be important if that drug interacts with another drug that the patient subsequently receives in combination. An EKG reading could provide useful baseline information years later for a cardiology patient. The

absence of an adverse reaction to an active control drug might later be useful to know when the patient's physician is deciding which drug to prescribe.

Genetic Data

Clinical studies can generate genetic data, e.g., the presence of a BRCA gene in a tumor, that have clear clinical significance and should be recorded in the patient's EMR, as well communicated directly to the patient's physician. However, other genetic data have uncertain or no clinical significance, and so should not be recorded in the EMR. Examples of such data include the following:

- Data generated solely as scientific information about genes or the genetic basis of a disease
- Data for which relevance to the disease and/or treatment is unknown or uncertain below a reasonable level
- Data obtained by genetic testing with inadequate sensitivity or specificity
- Data pertaining to an incurable and untreatable condition (that the patient does not want to know)

The privacy laws afford special protections to genetic data. Since recording any data in an EMR inherently makes it more vulnerable to disclosure or misuse, extra precautions should be taken for genetic data. For example, genetic data files could be encrypted, with a special procedure for gaining access.[10]

Information about the Study

In addition to study data about the patient, a clinician might want information about the study itself, e.g., drug mechanism of action, known interactions, potential adverse reactions, and contact information for the investigator.[1]

The EMR could thus include the protocol, consent form, and investigator's brochure. Such documents are usually the study sponsor's confidential information, so access to them should be limited to persons who need the information and have signed and understood the appropriate confidentiality agreements. Only one copy of the documents should be stored in the EMR, so it is necessary to reference them from patient records.

Voluminous Data

Study data — source documents, patient diaries, questionnaires, X-ray scans, device event logs, etc. — can be too voluminous or otherwise impractical to store in an EMR. However, the EMR can record their existence and document how to obtain access to them from the study archives. Such access might require partitioning the study records into those that have clinical significance and those that do not, or are confidential to the study sponsor. It might be necessary to store clinically significant records beyond the period required by the study sponsor.

CMS Medical Record Documentation Standards

The Affordable Care Act aims to improve healthcare and reduce the burden on covered entities and clinicians by requiring ICD-10 re-coding, standardization of quality measures, structured data for "meaningful use," and health information exchange (HIE) compatibility. New CMS medical record documentation standards are imminent and will affect the recording of study data in EMRs.[15,16]

Conclusion

EMRs are powerful tools for healthcare providers. However, like other powerful tools, they require proper training, maintenance and use. In particular, EMRs must balance the benefits of sharing information against the risks of disclosure or misuse of that information. Given the diversity of institutions, EMRs, studies and patients, the principles discussed above must be applied intelligently to specific circumstances to gain the healthcare benefits without sacrificing patient privacy or study sponsor confidentiality. The Affordable Care Act aims to create an EMR for every patient by 2014, so healthcare institutions that conduct clinical research should address these issues soon.

References

1. Dunlop, B.W. (2010). Should sensitive information from clinical trials be included in electronic medical records? *Journal of the American Medical Association (JAMA), 304*(6):665-666.
2. 21 CFR 50
3. 21 CFR 52
4. 21 CFR 56
5. 21 CFR 11
6. 21 CFR 213.62
7. 21 CFR 812.140
8. 45 CFR 2
9. 45 CFR 46
10. EPIC: Genetic Privacy. http://epic.org/privacy/genetic
11. EPIC: Medical Record Privacy. http://epic.org/privacy/medical
12. ICH GCP Guideline, Sect. 1.51
13. ICH Guideline, Sect. 1.52
14. CMS: Data and Data Systems. http://www.cms.gov/Research-Statistics-Data-and-Systems/Research-Statistics-Data-and-Systems.html
15. CMS: HIPAA Privacy and Security Standards. http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/PrivacyandSecurityStandards.html
16. Cleveland Clinic policies, standard operating procedures, and guidance documents.

Author

Jeanne M. Mattern, PHD, LSW, CCRP, is a Regulatory Compliance Officer in Quantitative Health Sciences at Cleveland Clinic. Contact her at 1.216.445.5775 or matterj@ccf.org.

