Breaches of Health Information: Are Electronic Records Different from Paper Records?

Robert M. Sade

Robert M. Sade, MD, is Professor of Surgery and Director of the Institute of Human Values in Health Care at the Medical University of South Carolina, sader@musc.edu; www.values.musc.edu. ©2010 by The Journal of Clinical Ethics. All rights reserved.

ABSTRACT

Breaches of electronic medical records constitute a type of healthcare error, but should be considered separately from other types of errors because the national focus on the security of electronic data justifies special treatment of medical information breaches. Guidelines for protecting electronic medical records should be applied equally to paper medical records.

The American Medical Association (AMA) Council on Ethical and Judicial Affairs (CEJA) provides guidelines for the first time on how physicians should respond to a breach in the security of an electronic medical record (EMR).1 In their report, “A Physician's Role Following a Breach of Electronic Health Information,” CEJA recommends that physicians do what they can to ensure that a breach of an EMR is reported to the patient promptly, along with a description of how the breach occurred, what information was disclosed, the potential consequences of the breach, any corrective actions that have been undertaken by responsible individuals or agencies, and how the patient might help to minimize adverse consequences. At all times, the report emphasizes, the physician should hold the patient's interests above those of the physician and any group or institution.

The recommendations that appear at the end of CEJA reports become an opinion in the Code of Medical Ethics (the Code), a body of ethical guidelines that is widely used by state medical licensing boards and by courts at various levels of jurisdiction in adjudicating allegations of physicians' ethical transgressions.2 Therefore, this report is important and is worthy of close scrutiny.

ARE ELECTRONIC MEDICAL RECORDS DIFFERENT FROM PAPER RECORDS?

Ethical obligations by physicians regarding medical records have been addressed in the Code for many decades. Currently, the Code contains 37 opinions that discuss or mention “confidentiality”3 and 19 opinions that discuss or mention “medical records.”4 Many of these opinions cite “breaches” of confidentiality or of medical records, yet none, until the current report, describes what a physician or institution should do when confidential information is released without authorization.5 This fact gives rise to several questions. If physicians’ responses to breaches of confidentiality did not require ethical guidance in the past, why are they required now? Is an EMR simply a digitized version of the familiar paper record or is an unauthorized release of EMR contents in some way more threatening than release of information in paper form? Paper records are not covered by the recommendations of this report, yet, if physicians are responsible for informing patients about breaches of confidential information in EMRs, do they not have the same responsibility with respect to paper medical records?
CEJA has provided persuasive answers to most of these questions. EMRs are not merely digitized versions of paper records. They contain large amounts of highly detailed clinical information about patients in an extremely compact form that can be easily stored and rapidly transmitted between healthcare professionals and institutions. This set of characteristics is the principle distinguishing feature of EMRs compared with paper records, for it makes unauthorized access to the entire content of EMRs relatively easy, especially in view of the absence of a consistently high level of electronic security in the healthcare system. CEJA’s report does not mention another growing potential threat to EMR security. Federal legislation, specifically, the USA Patriot Act of 2001 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has greatly expanded access — without the patient’s authorization — to protected health information by law enforcement agencies, exposing that information to the possibility of wide distribution with resultant potential for misuse. For these reasons, unauthorized access to medical records is more threatening — in terms of greater probability of occurrence and greater severity of consequences — in the era of EMR than it has been in the era of paper records, especially in view of the vigorous national push toward expanding the use of digital formats for medical records. For those intent on misappropriating medical information, the target promises to become much larger and more inviting than ever before.

A large proportion of medical records today is still stored and transmitted in paper form, and this situation is likely to continue well into the future. Although major breaches of confidentiality may be facilitated by an electronic format, such breaches may nevertheless occur with paper records. If paper-based records are stolen, the possibilities of misuse for medical identity theft and the many harms that can issue from such misuse are just as real, though perhaps not as likely, as theft of an EMR. The focus of CEJA’s report is on electronic records, but all of the recommendations apply equally to paper records. It seems likely that much of the stimulus for writing this report came from two recently enacted laws, the American Recovery and Reinvestment Act of 2009 and the Health Information Technology for Economic and Clinical Health Act of 2009, both of which are aimed at electronic personal health information. Therefore, it is understandable that CEJA’s report focuses on EMRs, but the council might wish to consider amending this new opinion in the future to include paper records as well as EMRs.

**IS BREACH OF CONFIDENTIAL MEDICAL INFORMATION MERELY A SUBSET OF HEALTHCARE ERRORS?**

The recommendations in this report bear striking resemblance to the recommendations in an earlier CEJA report, “Ethical Responsibility to Study and Prevent Error and Harm in the Provision of Health Care,” and the resulting Opinion 8.121. CEJA did not notice, or at least did not mention, this connection in the current report. Both sets of recommendations address physicians’ primary obligation to patients’ welfare, the obligation of physicians and institutions to respond actively to events that could harm patients, the need to investigate events that lead to such harms, honest disclosure to the patient of the causes of mistakes, an obligation to explain what is being done to prevent similar events in the future, and the importance of sustaining the patient’s trust in both the physician and the healthcare system.

Opinion 8.121 defines error in this way: “In the context of health care, an error is . . . a flawed system or plan that harms or has the potential to harm a patient.” Unauthorized release of medical information satisfies this definition; it is an error arising from a systemic flaw in electronic security and it has the potential to harm a patient. Rather than writing a separate report and a new set of guidelines, why did CEJA not simply amend Opinion 8.121 and include unauthorized access to an EMR as a subset of the general category of healthcare errors?

The similarities between these two reports are unmistakable, but there is at least one noteworthy difference between an error made during the care of a patient and a breach of confidential information: the differing responsibilities of the physician to communicate to the patient the nature and consequences of the adverse event. In the case of clinical errors, the physician is fully responsible for communicating with the patient, while in cases of informational breaches, the degree of responsibility varies with the physician’s level of involvement with the security and integrity of the electronic health information system, which in turn may vary with many factors,
including characteristics of the clinical setting in which care was provided. But this difference is minor, and by itself would not justify writing an entirely new report on informational breaches.

There is good reason, however, to consider unauthorized access to an EMR separately from healthcare errors. The challenges of secure data storage and transmission are playing an ever greater role in the national discourse on information technology, which has become a critical element of the national economy and is growing in importance to the healthcare industry. The national interest in and focus on data security fully justifies special treatment of medical information breaches as more than a subset of healthcare errors and warrants this well-conceived report from CEJA.

NOTES

3. Council on Ethical and Judicial Affairs, in Code of Medical Ethics, Opinions 2.015, 2.04, 2.05, 2.07, 2.079, 2.131, 2.136, 2.137, 2.23, 2.24, 2.25, 3.09, 5.026, 5.027, 5.045, 5.046, 5.05, 5.051, 5.055, 5.059, 5.0591, 5.06, 5.07, 5.075, 5.08, 5.09, 8.041, 8.047, 8.095, 8.21, 9.045, 9.055, 9.07, 9.11, 9.115, 10.01, 10.018, 10.03, see note 2 above.
4. Council on Ethical and Judicial Affairs, in Code of Medical Ethics of the American Medical Association, Opinions 2.068, 2.135, 2.136, 2.201, 2.22, 2.225, 2.40, 5.046, 5.051, 5.07, 7.02, 7.025, 7.03, 7.04, 7.05, 8.06, 8.181, 10.01, see note 2 above.
5. Two minor exceptions to this are found in the Council on Ethical and Judicial Affairs, in Code of Medical Ethics, Opinion 5.05, “Confidentiality”: “When the disclosure of confidential information is required by law or court order, physicians generally should notify the patient,” and Opinion 5.055: “Confidential Care for Minors”: “When the physician does breach confidentiality to the parents, he or she must discuss the reasons for the breach with the minor prior to the disclosure,” see note 2 above.