REPORT OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS*

CEJA Report 3-A-09

Subject: A Physician's Role Following a Breach of Electronic Health Information

Presented by: Regina M. Benjamin, MD, Chair

Referred to: Reference Committee on Amendments to Constitution and Bylaws (Daniel W. Van Heeckeren, MD, Chair)

---

Adopted Resolution 9 (A-08) asked our American Medical Association (AMA) to study the physician's role in informing a patient when the physician has reason to believe the individual's protected health information has been inappropriately disclosed. A physician's obligation to respect confidentiality and guard a patient's privacy is a well-established principle of professional ethics that dates back to the Hippocratic Oath.[1] The AMA's Code of Medical Ethics, in Opinion E-5.07, "Confidentiality: Computers," (AMA Policy Database) sets out precautionary steps to protect the confidentiality of electronically stored health information.[2] However, current policy does not address physicians' ethical responsibilities in the event the security of electronic records is breached and patient data are inappropriately accessed. This report examines physicians' professional ethical responsibility in this area.

## ELECTRONIC MEDICAL RECORDS (EMR)

Health information is "central to the practice of medicine and the quality of health care."[3] The capacity of electronic medical records (EMRs, also referred to as "electronic health records," EHRs) to store, access, and transmit detailed patient information accurately and rapidly among physicians and other health care professionals, health care administrators, and payers can greatly enhance patient care and the efficiency of the health care system overall. At the level of individual patient care, EMRs can support functions that are impossible or cumbersome to implement in paper record systems, including clinical reminders, drug interaction alerts, physician order entry systems, and decision support tools.[4, 5] At the level of the health care system, EMRs can facilitate administrative operations as well as enable access to population-level data for quality improvement, public health, and research purposes.[6, 7]

Physicians in the U.S. have been adopting EMRs in greater numbers in recent years. In a 2008 survey, 38.4% of physicians reported using fully or partially functional EMR systems, not including billing records, in their office-based practices.[8] These numbers represent a significant increase from 2001, when 18.2% of physicians reported using EMRs in their office-based practices.[9, 10] However, the collection, storage, and management of health information in the U.S. is carried out by numerous, diverse public and private institutions. The flow of medical information from patient to health care provider to health insurance industry and beyond is conducted with

* Reports of the Council on Ethical and Judicial Affairs are assigned to the reference committee on Amendments to Constitution and Bylaws. They may be adopted, not adopted, or referred. A report may not be amended, except to clarify the meaning of the report and only with the concurrence of the Council.

limited regulation and oversight. Existing data security laws and agencies have been characterized as a "confusing, sometimes conflicting, patchwork" of policies.[4] The combination of these factors may be contributing to breaches of EMRs. Physicians need guidance about their responsibilities when the confidentiality of patients' electronic personal health information has been compromised.[11]

## SECURITY BREACHES AND HARM TO PATIENTS

Recent developments have significantly increased the potential harms that can result when EMR systems are breached. For one, there has been a trend in recent years to gather and record more detailed information in medical records.[12] For another, the range of uses to which EMR systems are put have expanded. The aggregated nature of EMRs facilitates secondary use indirectly related to patient care, such as clinical research; quality measurement, reporting, and improvement; public health; marketing; and managed care decision-making.[7, 13]

The potential for harm from a security breach may depend on several factors, including the intent of the perpetrators of the breach, nature of the information that was breached, and to whom the information was disseminated. Still, the detailed and complex patterns of collecting and using patient information in today's health care environment mean that the risk of harm to patients from security breaches is higher than ever before. One profound harm may be medical identity theft, the fastest growing form of identity theft.[14, 15] Medical identity theft can result not only in inconvenience, discrimination, or negative effects on a victim's credit rating, but can pose harms specifically related to health care in the form of improper exhaustion of insurance benefits, wrongful billing for the costs of the thief's health care, and the burden of proving that the victim isn't responsible for such charges and can adversely affect insurability. Of particular concern are the potential adverse effects of such theft on a victim's subsequent health care, notably inappropriate care based on erroneous entries in his or her record.[3, 15]

Beyond this sort of material harm that may follow from inappropriate disclosure of a patient's personal health information are the dignitary harms that result. The commitment to benefit the patient is a basic tenet of a physician's professional ethic.[16-18] Effective healing cannot take place without a patient-physician relationship that rests on the physician's competence, skills, and good will.[19] The healing encounter is one in which the physician claims the necessary expertise and dedication to help and (implicitly) invites the vulnerable patient's trust.[20] The physician is accountable to his or her patients in this relationship of fidelity in trust.[21] Trust is fragile in today's health care system as patients increasingly question physicians' loyalty in the face of physicians' competing commitments to the interests of managed care plans, jobs, or incomes.[19]

The commitment to benefit patients also entails respecting a patient's freedom to act in accord with his or her values and sense of self.[1] Inappropriate disclosure of a patient's personal information violates his or her right to (informational) privacy, a fundamental expression of autonomy.

## LEGAL ENVIRONMENT

Currently, 44 states require companies doing business in their state to advise residents when the residents' information may have been compromised.[15] These laws were intended to make victims of a data breach aware of the increased danger of identity theft so that they could take action to protect themselves. Many medical records, e.g., those that contain a patient's name and social

security number, could fall under such state statutes. California recently broadened its notification law to explicitly apply to medical or health insurance-related information.[22]

Until recently, federal law unfortunately provided little specific guidance for how privacy interests in identifiable health information are protected in the event of a breach. While the Health Insurance Portability and Accountability Act (HIPAA) established national standards for privacy and security designed to protect the confidentiality and integrity of electronic personal health information, it does not advise physicians or administrators how to respond in the event of an actual security breach.[23]

However, disclosure is now required by the newly enacted American Recovery and Reinvestment Act of 2009 (ARRA). The portion of the act devoted to health information technology, known as the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), strengthens existing federal privacy and security provisions and mandates that a health care provider notify data subjects when the provider knows or has reason to believe the individuals' information has been inappropriately disclosed.[24] The law provides detailed guidance on what is considered a "breach," outlines appropriate methods of notification, and specifies the content which must be included in the notice to the extent possible.[24] Wherever ARRA contains stricter health-related privacy and security measures than state law, this federal law takes precedence. ARRA also requires HHS to issue regulations on breach notification requirements by August 16, 2009.

## IMPLICATIONS FOR ETHICAL PRACTICE

Helping to restore a sense of control over health records to the patient is of great moral import. Indeed, studies consistently show that patients prefer to be informed of breaches of their health records or other medical errors.[25] Voluntarily disclosing to a patient that his or her information has (or may have) been inappropriately disclosed when the patient may otherwise be unaware of the breach respects the patient's dignity and supports his or her right to take appropriate steps to avert or minimize potential harms. Beyond fulfilling the physician's obligation to be candid with patients, disclosing the incident and taking time to discuss possible harms and potential means of averting them may enhance trust. Conversely, the lack of disclosure may erode trust, especially if it leads to harm.

The patient safety movement has made it clear how difficult it can be for health care professionals to take responsibility for an event that has created a significant risk of harm or has caused harm. Like being candid with a patient about a medical error, being candid with a patient when his or her information has been inappropriately disclosed may be difficult or uncomfortable. However, this does not change the fact that it is the ethically appropriate response.

The material cost of adequately responding to a breach of security can be significant in terms of actual costs associated with the loss of patients, recruitment of new patients, and damage to the reputation of the physician, practice or institution. However, evidence has shown that litigation rates and related costs decrease when errors are promptly disclosed to patients and families.[26-28] It is also important to keep in mind that security measures and breach notice requirements should be practical and affordable so as to not hinder the ability of physicians to operate their practices and care for their patients.

The emotional toll on physicians relaying bad news can be burdensome, particularly given the value the profession places on confidence, authority, and "perfection." Unfortunately, in some institutions a culture of silence impedes admitting error or implicating colleagues. Yet evidence suggests that disclosure may alleviate some of the burdens associated with knowing about a situation that might cause harm to patients.[29] Institutional efforts to support candor and transparency may not only help alleviate emotional discomfort, but also help prevent similar errors in the future by raising awareness and increasing caution. More importantly, the commitment to uphold trust in the patient-physician relationship, to prevent harms to patients, and to respect patient autonomy form a compelling basis for a physician's involvement in efforts to promptly disclose security breaches that pose a risk of harm. This commitment also supports an obligation to assist patients to minimize potential adverse consequences of disclosure of personal health information—for example, sharing information on steps individuals should take to protect themselves from potential harm resulting from the breach such as using credit monitoring services, an identity theft hotline or other services.

A physician's responsibility to notify patients of an inappropriate disclosure and to take steps to help mitigate potential adverse consequences is not without limit.[30] A physician's ability to act may be limited by several factors, including what relationship the physician has with the affected patient or what his or her administrative authority is. A physician who is not in a position to have personal knowledge that a breach has occurred or take effective action to prevent breaches—for example, who works in a large health care institution whose EMR system is managed by others—has relatively limited responsibilities. In such circumstances, physicians might join others in the institution to make sure that the institution takes appropriate action. Physicians in solo or small group practices or those who are institutionally responsible for ensuring the security and integrity of electronic health information have a more immediate responsibility, both to ensure the security of their EMRs and to notify patients when information has been inappropriately disclosed.

Whatever the nature of the physician's involvement, in dealing with inappropriate disclosure of patient information the physician should place the interests of affected patients above the interests of their practices or institutions. The commitment to affected patients should be tempered only by potential harms of equal magnitude to other patients. Such patient advocacy may take courage, but courage is implicit within a physicians' dedication to the well-being of their patients and their commitment to being trustworthy.[21]

Disclosure of a breach should occur as soon as practicable and in accordance with statutory timelines after the breach is known and should be carried out in a way that minimizes patients' distress and respectfully restores their control over their own privacy. Like relaying other "bad news," disclosing a breach in health records should generally occur in a setting conducive to discussion. A private place and adequate time may need to be set aside for this purpose.[29]

At minimum, the discussions should include a thorough explanation of what information was or might have been disclosed and how the breach happened, its potential negative consequences, the corrective actions that have been and will be taken by the institution or practice, and the steps that patients themselves could take to mitigate potential harm. The physician making the disclosure should communicate regret and avoid behaving defensively.

These suggestions are not intended to be comprehensive. They define a starting point from which to develop appropriate responses in light of the particular circumstances of a given breach and

medicine's fundamental ethical obligations to patients whose personal health information is inappropriately disclosed.

RECOMMENDATION

The Council on Ethical and Judicial Affairs recommends that the following be adopted and the remainder of the report be filed:

When used with appropriate attention to security, electronic medical records (EMRs) promise numerous benefits for quality clinical care and health-related research. However, when a security breach occurs, patients may face physical, emotional, and dignitary harms.

Dedication to upholding trust in the patient-physician relationship, to preventing harms to patients, and to respecting patients' privacy and autonomy create responsibilities for individual physicians, medical practices, and health care institutions when patient information is inappropriately disclosed. The degree to which an individual physician has an ethical responsibility to address inappropriate disclosure depends in part on his or her awareness of the breach, relationship to the patient(s) affected, administrative authority with respect to the records, and authority to act on behalf of the practice or institution.

When there is reason to believe that patients' confidentiality has been compromised by a breach of the electronic medical record, physicians should:

(1) Ensure that patients are promptly informed about the breach and potential for harm, either by disclosing directly (when the physician has administrative responsibility for the EMR), participating in efforts by the practice or health care institution to disclose, or ensuring that the practice or institution takes appropriate action to disclose.

(2) Follow ethically appropriate procedures for disclosure, which should at minimum include:

(a) carrying out the disclosure confidentially and within a time frame that provides patients ample opportunity to take steps to minimize potential adverse consequences; and

(b) describing what information was breached; how the breach happened; what the consequences may be; what corrective actions have been taken by the physician, practice, or institution; and what steps patients themselves might take to minimize adverse consequences.

(3) Support responses to security breaches that place the interests of patients above those of the physician, medical practice, or institution.

(4) To the extent possible, provide information to patients to enable them to mitigate potential adverse consequences of inappropriate disclosure of their personal health information, such as credit monitoring services or identity theft hotline.

(New HOD/CEJA Policy)

Fiscal Note: Staff cost estimated at less than $500 to implement.

REFERENCES


1. Beauchamp T, Childress J. *Principles of Biomedical Ethics*. 6th ed. New York: Oxford University Press; 2009.
2. AMA. Opinion E-5.07, Confidentiality: Computers. *Code of Medical Ethics of the American Medical Association*. 2008-2009 ed. Chicago, IL: American Medical Association; 2008.
3. Blumenthal D, DesRoches C, Donelan K, et al. *Health Information Technology in the United States: Where We Stand*. Robert Wood Johnson Foundation;2008.
4. Anderson JG. Social, ethical and legal barriers to e-health. *International Journal of Medical Informatics.* 2007;76(5-6):480-483.
5. National Committee on Vital and Health Statistics. *Personal Health Records and Personal Health Systems*. Washington, DC: Department of Health and Human Services; 2006.
6. Committee on Data Standards for Patient Safety. *Key Capabilities of an Electronic Health Record System.* Washington, DC: Institute of Medicine; 2003.
7. National Center for Vital and Health Statistics. *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data*. Washington, DC: Department of Health and Human Services; 2007.
8. Hsiao CJ BC, Rechtsteiner E, Hing E, Woodwell D, Sisk JE. Preliminary estimates of electronic medical record use by office-based physicians. *National Center for Health Statistics, Health e-Stats*; 2008. http://www.cdc.gov/nchs/products/pubs/pubd/hestats/physicians08/physicians08.htm. Accessed April 13, 2009.
9. Burt CW, Hing E, Woodwell D. Electronic medical record use by office-based physicians: United States, 2005. *National Center for Health Statistics, Health e-Stats*; 2006. http://www.cdc.gov/nchs/products/pubs/pubd/hestats/electronic/electronic.htm.
10. Cherry DK, Burt CW, Woodwell DA. National Ambulatory Medical Care Survey; 2001 Summary. *Advance Data for Vital and Health Statistics*. 2003;337.
11. Myers J, Frieden TR, Bherwani KM, Henning KJ. Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age. *Am J Public Health.* 2008;98(5):793-801.
12. Etzioni A. Medical records: Enhancing privacy, preserving the common good. *Hastings Cent Rep.* 1999;29(2):14-23.
13. Chilton L, Berger JE, Melinkovich P, et al. Privacy protection and health information: Patient rights and pediatrician responsibilities. *Pediatrics.* 1999;104:973-977.
14. Dixon P. Medical identity theft: The information crime that can kill you. *World Privacy Forum*. 2006.
15. Hamilton BA. *Medical Identity Theft Environmental Scan.* Department of Health and Human Services; 2009.
16. ABIM Foundation Medical Professionalism Project. Medical professionalism in the new millennium: A physician charter. *Ann Intern Med.*2002;136(3):243-246.
17. AMA Council of Ethical and Judicial Affairs. *Code of Medical Ethics of the American Medical Association*. 2008-2009 ed. Chicago, IL: American Medical Association; 2008.
18. Campbell EG, Regan S, Gruen RL, et al. Professionalism in medicine: Results of a national survey of physicians. *Ann Intern Med.* 2007;147(11):795-802.
19. Goold S, Lipkin M, Jr. The doctor-patient relationship: Challenges, opportunities, and strategies. *J Gen Intern Med.* 1999;14(S1):S26-S33.
20. Pellegrino ED. The internal morality of clinical medicine: A paradigm for the ethics of the helping and healing professions. *J Med Philos.* 2001;26(6):559-579.

21. Pellegrino ED. Professionalism, profession and the virtues of the good physician. *Mt Sinai J Med.* 2002;69(6):378-384.
22. Information Practices Act of 1977, California Civil Code sections 1798 et seq.
23. The Office of Inspector General (OIG) to the Department of Health and Human Services (HHS) recently stated that, by relying on complaints to identify noncompliant covered entities, the Centers for Medicare and Medicaid Services (CMS) has no effective mechanism to ensure that covered entities are complying with HIPAA or that electronic personal health information is being adequately protected. OIG. Nationwide Review of the Centers for Medicare and Medicaid Services Health Insurance Portability and Accountability Act of 1996. A-04-07-05064 (October 2008). Similarly, the Red Flags Rule, which has been broadly interpreted to include health care entities, serves only to guide covered entities in implementing an identity theft prevention program. 82 Federal Register 63717-63775 (November 9, 2007).
24. American Recovery and Reinvestment Act of 2009.
25. Whetten-Goldstein K, Nguyen TQ, Sugarman J. So much for keeping secrets: The importance of considering patients' perspectives on maintaining confidentiality. *AIDS Care.* 2001;13(4):457-465.
26. Wood, D. *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*. Government Accountability Office; 2007.
27. Kraman SS, Hamm G. Risk management: Extreme honesty may be the best policy. *Ann Intern Med.* 1999;131(12):963-967.
28. *2006 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions.* Ponemon Institute; 2006.
29. National Center for Ethics in Health Care. *Disclosing Adverse Events to Patients*. Veterans Health Administration; 2003.
30. Fischer J. Recent work on moral responsibility. *Ethics*. 1999;110(1):93-139.