AMA *Code of Medical Ethics*

3.3.3 Breach of Security in Electronic Medical Records

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:

(a) 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.

(b) Follow all applicable state and federal laws regarding disclosure.

Physicians have a responsibility to follow ethically appropriate procedures for disclosure, which should at minimum include:

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

(d) 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.

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

(f) Providing information to patients to enable them to mitigate potential adverse consequences of inappropriate disclosure of their personal health information to the extent possible.

AMA Principles of Medical Ethics: IV,VIII