Virtual Mentor
American Medical Association Journal of Ethics
March 2011, Volume 13, Number 3: 161-162.

THE CODE SAYS

The AMA *Code of Medical Ethics'* Opinion on Computerized Medical Records

Opinion 5.07 - Confidentiality: Computers

The utmost effort and care must be taken to protect the confidentiality of all medical records, including computerized medical records.

The guidelines below are offered to assist physicians and computer service organizations in maintaining the confidentiality of information in medical records when that information is stored in computerized data bases.

(1) Confidential medical information should be entered into the computer-based patient record only by authorized personnel. Additions to the record should be time and date stamped, and the person making the additions should be identified in the record.

(2) The patient and physician should be advised about the existence of computerized data bases in which medical information concerning the patient is stored. Such information should be communicated to the physician and patient prior to the physician's release of the medical information to the entity or entities maintaining the computer data bases. All individuals and organizations with some form of access to the computerized data bases, and the level of access permitted, should be specifically identified in advance. Full disclosure of this information to the patient is necessary in obtaining informed consent to treatment. Patient data should be assigned a security level appropriate for the data's degree of sensitivity, which should be used to control who has access to the information.

(3) The physician and patient should be notified of the distribution of all reports reflecting identifiable patient data prior to distribution of the reports by the computer facility. There should be approval by the patient and notification of the physician prior to the release of patient-identifiable clinical and administrative data to individuals or organizations external to the medical care environment. Such information should not be released without the express permission of the patient.

(4) The dissemination of confidential medical data should be limited to only those individuals or agencies with a bona fide use for the data. Only the data necessary for the bona fide use should be released. Patient identifiers should be omitted when appropriate. Release of confidential medical information from the data base should be confined to the specific purpose for which the information is requested and limited to the specific time frame requested. All such organizations or individuals

should be advised that authorized release of data to them does not authorize their further release of the data to additional individuals or organizations, or subsequent use of the data for other purposes.

(5) Procedures for adding to or changing data on the computerized data base should indicate individuals authorized to make changes, time periods in which changes take place, and those individuals who will be informed about changes in the data from the medical records.

(6) Procedures for purging the computerized data base of archaic or inaccurate data should be established and the patient and physician should be notified before and after the data has been purged. There should be no mixing of a physician's computerized patient records with those of other computer service bureau clients. In addition, procedures should be developed to protect against inadvertent mixing of individual reports or segments thereof.

(7) The computerized medical data base should be online to the computer terminal only when authorized computer programs requiring the medical data are being used. Individuals and organizations external to the clinical facility should not be provided online access to a computerized data base containing identifiable data from medical records concerning patients. Access to the computerized data base should be controlled through security measures such as passwords, encryption (encoding) of information, and scannable badges or other user identification.

(8) Back-up systems and other mechanisms should be in place to prevent data loss and downtime as a result of hardware or software failure.

(9) Security

(a) Stringent security procedures should be in place to prevent unauthorized access to computer-based patient records. Personnel audit procedures should be developed to establish a record in the event of unauthorized disclosure of medical data. Terminated or former employees in the data processing environment should have no access to data from the medical records concerning patients.

(b) Upon termination of computer services for a physician, those computer files maintained for the physician should be physically turned over to the physician. They may be destroyed (erased) only if it is established that the physician has another copy (in some form). In the event of file erasure, the computer service bureau should verify in writing to the physician that the erasure has taken place.

Based on a report issued prior to April 1977; updated in June 1994 and June 1998.

Related in VM

Use of Electronic Patient Data in Research, March 2011

Reassessing "Minor" Breaches of Confidentiality, March 2011