American Psychiatric Association Resource Document on Computerized Records: A Guide to Security

The use of computer record keeping by psychiatrists and health care systems is rapidly increasing. At present, many psychiatrists and patients have serious concerns about the privacy of computerized records. The APA resource document "Preserving Confidentiality in the Era of Information Technology" (published in this issue) indicates that given the potential damage of inappropriate disclosures from computer information systems, psychiatrists and patients may prefer not to have private information stored electronically. However, in some settings, this option may not yet exist. Moreover, computerized records have positive attributes and patients may benefit by their use: They offer the promise of ready access to integrated health care information that may facilitate treatment.

The need for effective security measures to protect patient records is apparent. If computerized health information systems can compile a track record of maintaining patient privacy, then patients will feel that they can entrust their medical data to electronic storage. In 1987, the APA "Guidelines on Confidentiality" recognized the need to develop and implement security measures for computer information networks. However, many psychiatrists are not familiar with computer security measures.

This document presents suggested measures for medical records maintained in computer system and personal computers. Information technologies and security techniques are rapidly evolving, and this guide is intended to offer psychiatrists an introduction to the topic and a list of resources.

Computer Systems

Computerized records should be protected by a security system. Security must protect against modification, destruction, loss or unauthorized disclosure of the records, in whole or in part, intentional or unintentional. A complete medical record security program includes policies, standards, training, technical and procedural

This resource document was prepared by the APA's Committee on Confidentiality and the Council on Psychiatry and Law and approved by the Board of Trustees in December 1996 as a resource to the APA's District Branches. This document does not represent official policy of the American Psychiatric Association.

controls, risk assessment, auditing and monitoring, sanctions for violations, and assigned responsibility for management of the program. In addition, information deemed sensitive by tradition or by agreement between physician and patient should be protected with extra levels of security. Some ways to accomplish this are the following.

1. Institution of a unique patient-identifier should be required. The identifier should not be the patient's social security number, nor should it be the same number across systems.
2. The use of a password should be required to log onto the system. The password may be short but hard to duplicate in a random manner, nonsensical (alphanumeric with no vowels), and received in a secure manner by the user. It needs to be regarded as the equivalent of a legal signature. Consequences of the misuse of a password must be known and carried out, and therefore monitoring procedures are essential.
3. Passwords need to be changed in a planned fashion at regular intervals and when needed in the event of a suspected or known breach of security.
4. In addition to use of a password, the terminals used for access may also be limiting. For instance, an admissions clerk may access the system, but the combination of his/her password and an admissions department terminal could access only admissions information.
5. Users of the system are automatically signed off after a time-out period of five minutes.
6. The computer system should maintain an audit trail of all accesses to the record. The patient may request a copy of the audit trail. The patient's psychiatrist may look at the audit trail at any time. Minimally, an audit trail would record:
   A. The unique identifier of the call;
   B. The telephone number from which the call is made;
   C. The computer address of the caller;
   D. The date and time of the initiation of the call;
   E. The date and time of the disconnect;
   F. A "flag" for an unsuccessful attempt to connect. [Audit trail is from Institute of Primary Care Infomatics.]
7. Terminals should be blocked if an illegal password is used, or an authorized password is used illegally, a small but random number of times.
8. Terminals may automatically display confidentiality warnings if a user looks at a record warranting special care. These records may be defined by the institutions using the computer system, but usually minimally include employees and their families. The confidentiality display also is shown randomly every few hundred times any patient record information is sought.
9. Certain information is deemed more sensitive than other. This should be determined by the psychiatrist and

the patient. It is possible to have extra levels of security to protect such information. One possibility is to have "monitored notes." This entails an audit trail which is always flagged to the attention of the psychiatrist who created the note, thereby ensuring that the access to this sensitive material will not be achieved without discovery. Another option is to have a warning displayed each time access to this record is sought, inquiring of the "need to know."

10. There may also be material in the record which the physician deems unsuitable for the patient to know. This may include clinical thinking or information provided by a third party. This also could receive a special flag so that it is not released without notification of the psychiatrist. It is important, however, to be aware that it is generally believed to be unacceptable practice to have a record of health care information concerning the patient of which the patient is unaware.
11. Access to the system from an outside telephone should require the use of a second password.
12. When deleting patient care information from the computer base, the psychiatrist should be notified, both before and after. The deletion should be followed by a writeover of the hard disk. This deletion should occur before discarding, selling, or otherwise losing control over the access to the computer.
13. Communication of health care data between one system and another increases the risk of breach of confidentiality. Dedicated phone lines, callback procedures, extra passwords, and encryption are the measures which are being used for secure transmissions.
14. Consider the use of a committee similar to an institutional review board, including laypersons, for the establishment of policies regarding the computerization of health care records.
15. Since no system is absolutely secure, do not enter anything which should not be seen. The APA "Guidelines on Confidentiality" state that "information in a medical record should be limited to that which is necessary to meet the requirements of law and to maintain a documented data base appropriate for continued treatment."

Suggestions for the PC or Laptop User

For the psychiatrist who has a computer used only in his/her own office, there should be a capacity to "lock" the system, just as cabinets holding hard copies can be locked. This may be done with the use of passwords.

For psychiatrists using laptops outside the office, on which patient information is entered, an extra level of security must be considered. Possibilities include the use of an additional password and/or encryption.

Backup for a laptop or a PC must be done routinely and often. It is helpful to the physician if backup retrieval can be done file-by-file, rather than *en bloc*.

- The legal requirements for emendation of records must be met.

If the PC or laptop is left connected to a modem, a dedicated phone line may be used to decrease the risk of breaches of confidentiality. So too, an automatic sign-off may be used after a brief time-out period. Purging of records should be followed by a writeover of the hard disc.

Resources

- Institute of Medicine: Health Data in the Information Age: Use, Disclosure and Privacy. Edited by Donaldson MS, Lohr KN. Washington, DC: National Academy Press, 1994
- Institute of Medicine: The Computer-Based Patient Record: An Essential Technology for Health Care. Edited by Dick RS, Steen EB. Washington, DC: National Academy Press, 1991
- Publications from Beth Israel Hospital in Boston: (Their CCC, Warner Slack, MD, is often a coauthor.) Of particular note is Safran C: Protection of confidentiality in the computer-based patient record. MD Computing 12: 187–92, 1995
- Publications from the University of Vermont, David Sobel, PhD
- Computer-Based Patient Record Institute, Security Guidelines published 1995. 919 N. Michigan Ave., Ste 1400, Chicago, IL 60611 (FAX 312-787-7244)
- Publications of The Institute for Primary Care Infomatics. A contact person is Ronald Smuckler, MD, Ontario, Canada (FAX 416-226-2676)
- American Society for Testing and Materials (ASTM), 1916 Race Street, Philadelphia, PA 19103-1187 (FAX 215-299-2630)
- Report of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Dept. of HAS, April 1998
- Workgroup for Electronic Data Interchange (WEDI). The AMA is active in this group.