3.3.2 Confidentiality & Electronic Medical Records

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.

Physicians who collect or store patient information electronically, whether on stand-alone systems in their own practice or through contracts with service providers, must:

(a) Choose a system that conforms to acceptable industry practices and standards with respect to:

  (i) restriction of data entry and access to authorized personnel;

  (ii) capacity to routinely monitor/audit access to records;

  (iii) measures to ensure data security and integrity;

  (iv) policies and practices to address record retrieval, data sharing, third-party access and release of information, and disposition of records (when outdated or on termination of the service relationship) in keeping with ethics guidance.

(b) Describe how the confidentiality and integrity of information is protected if the patient requests.

(c) Release patient information only in keeping with ethics guidance for confidentiality.

AMA Principles of Medical Ethics: V

Background report(s):

CEJA 3-A-16 Modernized *Code of Medical Ethics*

CEJA-CSA Report 3-A-09 Confidentiality of computerized patient records

3.3.2 Confidentiality & Electronic Medical Records

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.

Physicians who collect or store patient information electronically, whether on stand-alone systems in their own practice or through contracts with service providers, must: [new content clarifies scope of guidance]

(a) Choose a system that conforms to acceptable industry practices and standards with respect to:

  (i) restriction of data entry and access to authorized personnel;

  (ii) capacity to routinely monitor/audit access to records;

  (iii) measures to ensure data security and integrity;

  (iv) policies and practices to address record retrieval, data sharing, third-party access and release of information, and disposition of records (when outdated or on termination of the service relationship) in keeping with ethics guidance.

(b) Describe how the confidentiality and integrity of information is protected if the patient requests.

(c) Release patient information only in keeping with ethics guidance for confidentiality.

AMA Principles of Medical Ethics: V

(Joint Report)

JOINT REPORT OF JUDICIAL COUNCIL AND COUNCIL ON MEDICAL SERVICE

The following report was presented by Burns A. Dobbins, Jr., M. D., Chairman of the Judicial Council, and Donald N. Sweeny, Jr., M. D., Chairman of the Council on Medical Service:

CONFIDENTIALITY OF COMPUTERIZED PATIENT INFORMATION (RESOLUTION 38, A-77)

(Reference Committee A, page 234)

HOUSE ACTION: ADOPTED

At the 1977 Annual Convention, the House of Delegates adopted Resolution 38 (A-77), as amended, asking that guidelines be established to (1) define procedures for the management of a computerized patient data base, (2) define procedures to control access to clinical data and limit access to the computerized data base, and (3) establish accrediting guidelines for computer service bureaus to reassure patients and physicians that their information will not be misused.

Background

The issues of access to confidential medical and other personal information and the use of such information once computer technology has permitted the accumulation, storage, and analysis of an unlimited quantity of it have been under discussion in both the public and private sectors for more than a decade. Legislation at both the state and federal levels has focused on policies governing the release of various kinds of information, with particular emphasis given to the patient's right to have access to confidential medical information, to have an opportunity to be informed of the use to be made of it, and to have access to it for making corrections. The House of Delegates has, on a number of past occasions, adopted reports dealing with issues related to confidentiality of medical information, including guidelines on PSRO data policy developed by the Council on Medical Service, and model state legislation on confidentiality of medical information developed by the Council on Legislation.

The federal Fair Credit Reporting Act, the National Health Planning and Resources Development Act, the Professional Standards Review Organization amendments to the Social Security Act, and the federal Privacy Act are examples of the Congressional interest in the right of individuals to have certain types of information protected and to be assured access to such information in the custody of specified agencies and entities. At the federal level, for instance, the Fair Credit Reporting Act sets requirements concerning the accumulation, verification, and release of medical record information obtained by a proper credit reporting agency. Information relating to medical practice and care also may be accumulated by the Bureau of Census, HEW, the Secretary of Commerce, Health Systems Agencies, and other governmental agencies.

Two major research studies undertaken for the federal government on these issues were completed in 1976 and 1977. The publications based on these studies are: "Computer, Health Records and Citizen Rights" by Alan F. Westin, Ph.D., principal investigator, and "Personal Privacy in an Information Society—The Report of the Privacy Protection Study Commission,"

Daniel F. Linowes, Chairman. The Report of the Privacy Protection Study Commission recommended, among other things, the creation of Medicare and Medicaid regulations and state legislation to assure patient access to medical records and related medical record information, to allow correction of medical records, and to assure both the protection of confidentiality of information and the disclosure of information pursuant to patient authorization.

At the state level, at least eleven legislatures have enacted statutes in the past four years to allow patients greater access to the information contained in medical records that concern patients' care or treatment. Other states have rules and regulations on this subject. Although the traditional professional and legal view has been that a physician is entitled to possession or ownership of the medical notes he makes in his private practice, a patient or his legal representative may also have certain legal rights to the information in such notes. The patient does have a right to information from the records, at least to the extent that the information is necessary to protect his health interests or legal rights. In those states that have specific statutory language or rules and regulations governing access to medical records, compliance with these requirements is mandated.

A physician also has a professional responsibility to keep information secret about a patient that is obtained in the course of the physician-patient relationship. Section 9 of the Principles of Medical Ethics states: "A physician may not reveal confidences entrusted to him in the course of medical attendance, or the deficiencies he may observe in the character of patients, unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or of the community."

The confidentiality of physician-patient communications is desirable to assure free and open disclosure by the patient to the physician of all information needed to establish a proper diagnosis and attain the most desirable clinical outcome possible. Protecting the confidentiality of the personal and medical information in such medical records is also necessary to prevent humiliation, embarrassment, or discomfort of patients.

At the same time, patients may have legitimate desires to have medical information concerning their care and treatment forwarded to others. The increasing incidence of personal injury litigation and the expanding use of life, accident and health insurance, for example, are major factors which have operated to multiply the number of persons who have a legitimate interest in the information. It may, for instance, be desirable for a patient to have certain information transmitted directly to third parties concerned with the payment of the patient's bill, to a workmen's compensation commission, to the patient's attorney, to a succeeding attending physician, to a physician with a professional or academic interest in the type of case, to a law enforcement agency, to military authorities, to a prospective employer, or to others. Patient authorization for release of information to a third party payor that has legal liability for the payment of any part of the charges for the medical care and treatment provided may be the most commonly encountered instance in which the patient's expectation of authorized release should be honored.

In summary, both the protection of confidentiality and the appropriate release of information in records is the rightful expectation of the patient. A physician should respect the patient's expectations of confidentiality concerning medical records that involve the patient's care and treatment, but the physician should also respect the patient's authorization to provide information from the medical records to those whom the patient authorizes to inspect all or a part of it for legitimate purposes.

(Joint Report)

Discussion

Resolution 38 (A-77), as amended, requested the development of guidelines applicable to information from a physician's office records that is made part of a computerized data system. The transfer of such information would, generally, be expected to occur when a computer service bureau contracts with a physician to store data on patient billing or on the care and treatment provided the physician's patients. Although computerized data concerning patient care and treatment could involve many other data systems, such as that used by peer review bodies, Health Systems Agencies, third party insurance carriers and intermediaries, and PSROs, the guidelines presented in this report will be limited primarily to the situation of computerized office records, in keeping with the major thrust of amended Resolution 38.

There are three primary issues that need to be addressed to assure the maintenance of confidentiality of information from medical records stored in computerized data banks by computer service bureaus. These three related issues are privacy, confidentiality, and security. The issue of privacy concerns the obligation to withhold personal information from revelation. There is certain information, such as may be kept in a medical record, that a patient may not want disclosed solely for personal reasons. The issue of confidentiality concerns an agreement between individuals to limit the extent of revelation of such personal information. The patient's expectations of confidentiality arise from the obligation to protect the patient's privacy and from the clinical desirability of such an agreement to allow a free flow of information between the physician and the patient. As has been noted above, there may be limitations on a patient's expectations of confidentiality. The third issue, security, concerns a responsibility to protect personal information from revelation so as to preserve confidentiality.

Computer technology permits the accumulation, storage, and analysis of an unlimited quantum of medical information. The fact that the data bases are increasing substantially is evidence of increased pressure to obtain medical data for clinical, administrative, and archive purposes. Although the concepts of privacy, confidentiality, and security apply to all medical data regardless of collection or storage method, the ability of the computer to store vast amounts of medical data has resulted in public and private scrutiny of this technology to guard against its accidental or intentional misuse. Such misuse may occur because of inadequate security policies or improper training of personnel. The harm that results from the misuse of such data may be felt by the patient, whether the misuse is accidental or intentional.

Because of the technological growth of medical data acquisition mechanisms, the fundamental need to protect the confidentiality of information from medical records has been intensified. The fact that such data may reside in a computerized data bank does not alter this need.

The possibility of access to information is greater with a computerized data system than with information stored in the traditional written form in a physician's office. Accordingly, the guidelines noted below are offered to assist computer service organizations and physicians in maintaining the confidentiality of information in medical records when that information is stored in computerized data bases. Commentary on specific guidelines is also included to show the need for certain particular rules and standards for computerized medical information.

The Council on Medical Service and the Judicial Council, therefore, recommend that the House of Delegates adopt the following guidelines addressing the issues spoken to by amended Resolution 38 (A-77).

(Joint Report)

I. GUIDELINES ON PROCEDURES FOR THE MANAGEMENT OF A COMPUTERIZED DATA BASE

Introduction

Management of computerized data bases involves the planning, organization and control of activities or programs directed towards satisfying an established set of operational objectives. With respect to the management of a computerized data base holding medical information, guidelines have been requested by the House of Delegates in order to assure the maintenance of confidential treatment and management of essentially private patient data. The management guidelines noted below reflect concepts desirable from a medical viewpoint related to computer technology capable of storing confidential medical information. It should be recognized that specific procedures adapted from application of these concepts may vary depending upon the nature of the organization processing the data as well as the appropriate and authorized use of the stored data.

1. PREFACE: Medical information maintained on a patient's behalf is often used as the basis for important clinical or administrative decisions affecting the patient. Accordingly, only specifically authorized individuals should be permitted to submit additions, changes, or deletions to the computerized data base holding medical information.

   GUIDELINE: Procedures should be developed to insure that confidential medical information entered into the computerized data base is verified as to authenticity of source.

2. PREFACE: Once a physician has released a patient's confidential medical information on the patient's authorization, subsequent use of that information is out of the physician's effective control. The physician should be advised about the destination of medical information released from his control.

   GUIDELINE: Procedures should be developed to advise the patient and physician about the existence of computerized data bases in which the patient's medical information is stored. Such information should be communicated to the physician and patient prior to the physician's release of the medical information.

3. PREFACE: Due to the ease with which information can be produced from a computer, it is important to identify and trace all reports on which is printed identifiable patient data.

   GUIDELINE: Procedures should be developed for notifying both the physician and patient of the distribution of all reports reflecting identifiable patient data prior to distribution of the reports by the computer facility.

4. PREFACE: Too often an unwarranted assumption may be made that the data coming from a computerized data base is correct. Management of the computerized medical data must, therefore, include mechanisms to maintain the patient data in an as accurate a state as possible.

   GUIDELINE: Procedures should be developed for adding to or changing data on the computerized data base. The procedures 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.

(Joint Report)

5. PREFACE: Due to the large storage capacity of computers, there exists the possibility that once data is entered into the data base it will not be subsequently removed even if the data has no contemporary or historical value.

   GUIDELINE: 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.

6. PREFACE: Once a computerized data base is physically linked to the computer, it becomes relatively easy to gain access to that data base. Care should, therefore, be taken not to connect the data files to the computer except as necessary to perform legitimately defined processing.

   GUIDELINE: The computerized medical data base should be on-line to the computer only when authorized computer programs requiring the medical data are being used.

7. PREFACE: To prevent misuse of data, it is advisable to permit only authorized computer service personnel to enter or work in the physical facility in which processing is done and the computer files are stored.

   GUIDELINE: Stringent security procedures for entry into the immediate environment in which the computerized medical data base is stored and/or processed should be developed and strictly enforced.

8. PREFACE: Procedures for the maintenance of the confidentiality of medical data should be communicated to employees involved in activities related to the computerized medical data base. It is equally important that employees be advised of administrative remedies for breaches of confidentiality which may place in peril the confidential patient data.

   GUIDELINE: (a) Specific guidelines concerning behavior of employees handling or otherwise having access to confidential medical information should be developed and be made generally available to affected employees.

   (b) All terminated or former employees in the data processing environment should have no access to data from the medical records concerning patients.

   (c) Employees working in the data processing environment in which data from medical records concerning patients are processed and who are involuntarily terminated should immediately upon termination be removed from the computerized medical data environment.

II. GUIDELINES ON PROCEDURES WHICH CONTROL ACCESS TO CLINICAL DATA AND LIMIT ACCESS TO THE COMPUTERIZED DATA BASE

Introduction

In general, the recorded instances of theft or misuse of computerized data are few compared to those instances in which information maintained in conventional, non-computerized data repositories are misused or stolen. The recorded instances of computerized data misuse, however, suggest that when such an occurrence takes place, it involves exceptionally large segments of information. Such misuse may be more extensive than realized, since it may not be reported or

may remain cloaked due to the technical abilities of those involved in the misuse of data. The recounting of such occurrences of misuse suggests that the problem is generally not one of access by unauthorized individuals, but stems from the misuse of computerized data (either consciously or inadvertently) by those who have authorized access to the data. Hence, with respect to computerized data bases holding medical data, emphasis should be placed upon controlling the mechanism for authorized access to medical data as well as defining the limits of such permissible authorized access.

1. PREFACE: Once an individual or organization has gained physical access to the computer data base, either via remote computer terminal or other means, it becomes extremely difficult, if not virtually impossible, to prevent access to those portions of the data base which have not been authorized for release.

   GUIDELINE: Individuals and organizations external to the clinical facility should not be provided on-line access to a computerized data base containing identifiable data from medical records concerning patients.

2. PREFACE: The patient and physician should be cognizant of those individuals or organizations that will have access to the computerized files of medical information concerning the patient. Such safeguards are important in a computer environment because of the relative ease with which large segments of data can be transferred from one computer to another.

   GUIDELINE: Procedures should be developed to obtain the approval by the physician and patient prior to the release of patient-identified clinical and administrative data to individuals or organizations external to the medical care environment.

3. PREFACE: Due to the complexity of the health care environment, secondary and tertiary users of medical data are becoming more prevalent. Increasingly prolific dispersion of computerized medical data endangers the confidentiality of these data.

   GUIDELINE: As a corollary to Guideline Number 2, procedures should be developed to provide the patient with advance notification of any agency or individual with access to patient-identifiable medical data.

4. PREFACE: The probability of leakage of confidential medical data increases the longer the data is external to the controlled access data base environment. In addition, the probability of the data being used for unauthorized purposes increases.

   GUIDELINE: Procedures should be developed to limit the dispersion of confidential medical data only to those individuals or agencies with a bona fide use for the data. 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.

5. PREFACE: The organization should designate an individual who is directly accountable for the manner in which and the success with which defined confidentiality procedures are implemented. This requirement may help to minimize errors of omission or commission with respect to observance of confidentiality procedures.

   GUIDELINE: The organization should designate a "security officer" with the duty to implement and monitor confidentiality procedures and policies.

6. PREFACE: Once confidential medical information is released to other organizations, effective control over subsequent use of the data is greatly diminished. Accordingly, organizations receiving such medical data should be sensitized to the data's confidential nature and limitations on its use.

   GUIDELINE: Data release limitations should be specifically stated for organizations or individuals receiving confidential medical data, such as PSROs, peer review bodies, Health Systems Agencies, and third party insurance intermediaries. 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.

7. PREFACE: Since individuals and organizations authorized to have access to computer data bases will have differing needs for access to the computer for legitimate purposes, the level of access to the data needed by the individual or organizations involved should be specified.

   GUIDELINE: All individuals and organizations with some form of access to computerized data bank, and level of access permitted, should be specifically identified.

III. ACCREDITING GUIDELINES FOR COMPUTER SERVICE BUREAUS

Introduction

An increasing number of computer service bureaus are expanding their services to include provision of data processing support for physicians who wish to automate their patient billing and for production of insurance reports for third party intermediaries. In the performance of this activity, the computer service bureau maintains computerized medical data bases which include medical information (e.g., diagnosis, service provided) used to produce the items noted above. As much of the data maintained by a computer service bureau is sensitive, it is important that these organizations establish explicit confidentiality procedures to protect against intentional or inadvertent release of confidential medical information to individuals or organizations not authorized to receive it.

The guidelines noted below are not intended to serve in the same manner as standards established by a voluntary accreditation agency. The guidelines are intended to suggest procedures to preserve the confidentiality of medical data the computer service bureau maintains when providing service for physicians and the patients they serve.

1. PREFACE: Only authorized computer service bureau personnel are to be permitted within the area in which computerized medical data base information is processed or stored so as to prevent unauthorized disclosures.

   GUIDELINE: The computer service bureau should specifically identify a physical security procedure to prevent access to the computer facility by unauthorized personnel.

2. PREFACE: In the event that unauthorized disclosure of medical data does take place, it is important to be able to identify the source of the disclosure so as to prevent repeated occurrences.

   GUIDELINE: Personnel audit procedures should be developed to establish a record in the event of unauthorized disclosure of medical data. A roster of past and present service bureau personnel with specified levels of access to the medical data base should be maintained.

3. PREFACE: A computer-generated report for one client may reflect a segment of data maintained on behalf of a different client. This generally arises either because all client data is maintained on a central data base or because client reports are the product of one continuous computer run and a segment of one client's report is inadvertently combined with that of another client. In the case of medical data, such an error would represent a serious breach of confidentiality.

   GUIDELINE: Procedures should be developed to prevent the commingling of a physician's computerized records with those of other service bureau clients. In addition, procedures should be developed to protect against inadvertent mixing of client reports or segments thereof.

4. PREFACE: Inadvertent release of patient-identified medical data to unauthorized recipients should be avoided at all costs. Hence specific individuals or organizations to whom information is to be sent should be qualified as authorized data recipients prior to forwarding the information.

   GUIDELINE: Information on a physician's computerized medical data base should under no circumstances be released without the express permission of the physician and the patient. This stipulation should appear in any agreement between the computer service bureau and the physician which addresses work to be performed for the physician.

5. PREFACE: In addition to management personnel, it is important that other computer service bureau employees be made aware of the sensitive nature of medical data and the proper conduct for handling such data.

   GUIDELINE: Procedures should be developed to advise computer service bureau employees of the confidential nature of the medical data processed. These procedures should explicitly address employee responsibilities. Specific administrative sanctions should exist to prevent employee breaches of confidentiality and security procedures.

6. PREFACE: The computer service bureau agreements with some physician clients may be terminated. Upon such termination of services, the disposition of the computerized medical data maintained for the physician is important. Under no circumstances should the medical information be retained by the computer service bureau after services for the physician have ceased.

   GUIDELINE: Upon termination of computer service bureau services for a physician, those computer files maintained for the physician should be physically turned over to the physician or destroyed (erased). In the event of file erasure, the computer service bureau should verify in writing to the physician that the erasure has taken place.

7. PREFACE: As the preservation of confidentiality is of significant importance to both the patient and physician, the computer service bureau should, upon request, notify the physician and the patient about the procedures taken to keep confidential the medical data on patients.

   GUIDELINE: The computer service bureau is strongly encouraged to make available to physicians and patients a brochure or other written document, which, in specific terms, outlines the procedures the computer service bureau uses to protect the confidentiality of patient-identifiable medical data processed by the facility.