Designation: E 1869 – 97

An American National Standard

Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records[1]

This standard is issued under the fixed designation E 1869; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers the principles for confidentiality, privacy, access, and security of person identifiable health information. The focus of this standard is computer-based systems; however, many of the principles outlined in this guide also apply to health information and patient records that are not in an electronic format. Basic principles and ethical practices for handling confidentiality, access, and security of health information are contained in a myriad of federal and state laws, rules and regulations, and in ethical statements of professional conduct. Although there are many sources for guidance, there is no current national standard guide on this topic.

1.2 This guide includes principles related to:

	Section
Privacy	7
Confidentiality	8
Collection, Use, and Maintenance	9
Ownership	10
Access	11
Disclosure/Transfer of Data	12
Data Security	13
Penalties/Sanctions	14
Education	15

1.3 This guide does not address specific technical requirements. It is intended as a base for development of more specific standards.

2. Referenced Documents

2.1 *ASTM Standards:*

E 1384 Guide for the Content and Structure of the Computer-Based Patient Record[2]

E 1714 Guide for the Properties of Electronic Health Records and Record Systems[2]

E 1762 Guide for Electronic Authentication of Health Information[2]

E 1769 Guide for the Properties of Electronic Health Records and Record Systems[2]

3. Terminology

3.1 *Definitions:*

3.1.1 *access*—the provision of an opportunity to approach, inspect, review, retrieve, store, communicate with, or make use of health information system resources (for example, hardware, software, systems or structure) or patient identifiable data and information, or both.

3.1.2 *authentication*:

3.1.3 *authentication (data entry)*—to authorize or validate an entry in a record by: a signature including first initial, last name, and discipline or a unique identifier allowing identification of the responsible individual.

3.1.4 *authentication (data origin/sender)*—corroboration that the source/sender of data received is as claimed.

3.1.5 *authentication (user/receiver)*—the provision of assurance of the claimed identity of an entity/receiver.

3.1.6 *authorize*—the granting to a user the right of access to specified data and information, a program, a terminal, or a process.

3.1.7 *clinical data centers*—all computer-based (and manual) systems which handle and store patient records and health information, that is, solo practitioners, clinics, hospitals, state departments of health, data centers, and health maintenance organizations.

3.1.8 *clinical information*—data and information collected from the patient or patient's family by a healthcare practitioner or healthcare organization. A healthcare practitioner's objective measurement or subjective evaluation of a patient's physical or mental state of health, descriptions of an individual's health history and family health history, diagnostic studies, decision rationale, descriptions of procedures performed, findings, therapeutic interventions, medications prescribed, description of responses to treatment, prognostic statements and descriptions of socioeconomic factors, and environmental factors related to the patient's health.

3.1.9 *computer-based patient record*—see *patient record*.

3.1.10 *confidential*—status accorded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use,

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and are the direct responsibility of Subcommittee E31.20 on Data and System Security for Health Information.

Current edition approved April 10, 1997. Published April 1997.

[2] *Annual Book of ASTM Standards*, Vol 14.01.

or both, and must be disseminated only to authorized individuals or organizations with a need to know.

3.1.11 *data*—collection of elements on a given subject; things known, given, or assumed, as the basis for decision making; the raw material of information systems expressed in text, numbers, symbols and images; facts.

3.1.12 *data protection measure*—a planned operation, for example, procedure, policy, program, or technology, employed in the privacy system to prevent, detect, or sanction breaches of security.

3.1.13 *disclosure*—to release, transfer, or otherwise divulge confidential health information to any entity other than the individual who is the subject of such information.

3.1.14 *health care*—(*1*) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, public health, counseling, service, or procedure with respect to the physical or mental condition of an individual; or affecting the structure or function of the human body; or (*2*) any sale or dispensing of a drug, device, equipment, or other item to an individual, or for the use of an individual, pursuant to a prescription.

3.1.15 *health information*—any information, whether oral or recorded in any form or medium (*1*) that is created or received by a health care provider; a health plan; health researcher, public health authority, instructor, employer, school or university; health information service or other entity that creates, receives, obtains, maintains, uses, or transmits health information; a health oversight agency, a health information service organization, or (*2*) that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to a protected individual; and (*3*) that identifies the individual, with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

3.1.16 *inference*—refers to the ability to deduce the identity of a person associated with a set of data through "clues" contained in that information. This analysis permits determination of the individual's identity based on a combination of facts associated with that person even though specific identifiers have been removed, like name and social security number.

3.1.17 *information*—data that have been processed for use; human interpretation of data; data that have been processed into a meaningful form.

3.1.18 *informed consent*—informed consent requires that individuals be informed, in advance, of the information being collected from them, or generated, and the purposes for which it will be used; and be given an opportunity to accept, reject, or modify the terms presented. Central to the principle of informed consent is providing individuals with the ability to control the use of information once collected. The general rule is that information collected for one purpose must not be used for another purpose without the individual's consent. In practice, this requires that no use or disclosure occur, except to a documented request by, or with the prior consent of, the individual to whom the record pertains. Under some circumstances a guardian or designee may consent on behalf of the individual.

3.1.19 *informational privacy*—(*1*) a state or condition of controlled access to personal information. (*2*) The ability of an individual to control the use and dissemination of information that relates to himself or herself. (*3*) The individual's ability to control what information is available to various users and to limit redisclosures of information.

3.1.20 *patient record*:

3.1.21 *longitudinal patient record*—a permanent, coordinated patient record of significant information. It is a birth-to-death synopsis of significant demographic, genetic, clinical, and environmental facts and events.

3.1.22 *patient health record*—(*1*) a set of information for a single individual's encounter with the healthcare system. It contains data and information generated across care settings and from different health care interactions. The set of data may be viewed in various ways, like brief summary or emergency data. (*2*) It is the primary legal record documenting the healthcare services provided to an individual.

3.1.23 *Discussion—patient health record* is used to refer to: medical record, patient care record, hospital record, clinical record, client record, resident record, electronic medical record, and computer-based patient record. The term includes routine clinical or office records, hospital records, records of care in any health-related setting, research protocols, preventive care, life style evaluation, special study records, and various clinical databases.

3.1.24 *patient record system*—the set of components that form the mechanism by which patient records are created, used, stored, and retrieved. A patient record system is usually located within a healthcare provider setting. It includes people, data, rules and procedures, processing and storage devices (for example, paper and pen, hardware and software), and communications and support function. The system supports users by providing access to complete and accurate data, alerts, reminders, clinical decision support systems, links to medical knowledge, and other aids.

3.1.25 *secondary patient record*—a record that is derived from the primary health record and contains selected data elements to aid in providing, supporting, evaluating, or advancing patient care. Patient care provision refers to practitioner access to a coordinated database containing limited information (for example, immunization data, problem list, medication record, lab results). Patient care support refers to administration, regulation, and payment functions. Patient care evaluation refers to quality management activities including: quality improvement, quality assurance, patient satisfaction, utilization management, and audits examining specific aspects of patient care. Patient care advancement refers to research. Secondary record data are often combined to form a secondary database, for example, an immunization tracking database, a disease index, a trauma registry, and an emergency department log.

3.1.26 *personally identifiable health information*— health information which contains an individual's identifiers (name, social security number) or contains a sufficient number of variables to allow identification of an individual.

3.1.27 *practitioner (licensed/certified)*—an individual at any level of professional specialization who requires a public license to deliver health care to individuals. An individual at

any level of professional specialization who is certified by a public agency or professional organization to provide health services to individuals. A practitioner may also be a provider.

3.1.28 *privacy*—the right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property. It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference. See also *informational privacy*.

3.1.29 *privilege*—the individual's right to hold private and confidential the information given to a healthcare provider in the context of a professional relationship. The individual may, by overt act of consent or by other means, waive the right to privilege. For example, if a patient brings a lawsuit against a facility and the records are needed to present the facility's case, the privilege is waived.

3.1.30 *provider*—a business entity which furnishes health care to a consumer; it includes a professionally licensed practitioner who is authorized to operate a healthcare delivery system.

3.1.31 *security*:

3.1.32 *data security*—the result of effective data protection measures; the sum of measures that safeguard data and computer programs from undesired occurrences and exposure to: (*1*) accidental or intentional access or disclosure to unauthorized persons, or a combination thereof, (*2*) accidental or malicious alteration, (*3*) unauthorized copying, (*4*) loss by theft or destruction by hardware failures, software deficiencies, operating mistakes; physical damage by fire, water, smoke, excessive temperature, electrical failure or sabotage; or a combination thereof. Data security exists when data are protected from accidental or intentional disclosure to unauthorized persons and from unauthorized or accidental alteration.

3.1.33 *system security*—security is the totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. Security protects both the system and the information contained within from unauthorized access from without and from misuse from within. Security enables the entity or system to protect the confidential information it stores from unauthorized access, disclosure, or misuse; thereby protecting the privacy of the individuals who are the subjects of the stored information.

4. Significance and Use

4.1 Many U.S. healthcare and health information systems leaders believe that electronic health information systems that include computer-based patient records will improve health care. To achieve this goal these systems will need to protect individual privacy of patient data, provide appropriate access, and use adequate data security measures. Sound information policies and practices must be in place prior to the wide-scale deployment of health information systems. Strong enforceable privacy policies must shape the development and implementation of these systems.

4.2 The purposes of patient records are to document the course of the patient's illness or health status during each encounter and episode of care; to furnish documentary evidence of the course of the patient's health evaluation, treatment and change in condition; to document an individual's health status; to provide data for preventive care; to document communication between the practitioner responsible for the patient's care and any other healthcare practitioner who contributes to the patient's care; to assist in protecting the legal interest of the patient, the health care facility and the responsible practitioner; to provide continuity of care; to provide data to substantiate insurance claims; to provide a basis for evaluating the adequacy and appropriateness of care; and to provide data for use in continuing education and research.

4.3 Health information is a broad concept. It includes all information related to an individual's physical and mental health, the provision of health care generally, and payment for health care. The patient record is a major component of the health information system. The creation of electronic databases and communication protocols to transfer data between systems presents new opportunities to implement more effective systems for health information, to enhance patient care, reduce the cost of health care, and improve patient outcomes. National standards will guide all who have responsibilities for records and information systems containing person identifiable health data and information.

4.4 This guide also acknowledges the large and growing list of health information databases already in existence. These databases have been assembled to pay for services rendered (insurance), to validate the appropriate use of patient services (utilization management), to support policy (national levels), to gather data for research/tracking of specific problems (registries—such as tumor, trauma, birth defects, mental health case management), to prevent the spread of disease (required reporting of communicable diseases such as tuberculosis, gonorrhea, AIDS), and to respond to new uses which are proposed each year.

4.5 National standards delineating principles and practices in the areas of confidentiality, privacy, access, and data security will provide a guide for policy, law, and systems development and a base for standards for electronic health information regardless of its location.

5. Description of Standards

5.1 The Privacy Act, although applicable only to federal agencies and federal contractors, outlines basic tenets useful for any group, facility, or individual that maintains records on individuals. These tenets should be incorporated into policies and practices for computer-based patient record systems and health information systems. The basic tenets are:

5.1.1 The individual has the right to know that identifiable, personal information is available in a record system and to know what that information is used for.

5.1.2 The individual may have access to the records, has a right to have a copy made, and has the right to amend or correct the records.

5.1.3 The data may not be used for any use beyond that for which the data are collected (as specified by law or regulation).

5.1.4 Written consent of the individual shall be obtained for all other uses (beyond those specified by law or regulation).

NOTE 1—Technology provides means for electronic forms of consent and authentication.

5.1.5 The data shall be collected and used only for a necessary and lawful purpose.

5.2 The computer-based patient record and many electronic health information systems provide flexibility in collecting, organizing, and disseminating data. It is possible to segment data and provide only needed data to legitimate users both within and external to a healthcare facility, for example, lab technician, business office, switchboard, third party payer, or workmen's compensation agency. This same technology allows easier linking of data. This guide does not address the specifics of data linkage. However, the value of appropriate data linkage and its potential uses are recognized.

5.2.1 Computer-based patient record systems and other health information systems should facilitate access to patient information by authorized healthcare practitioners during the active phase of treatment. The needs of emergency care situations should be given special attention and procedures.

5.2.2 This guide is intended to provide a base for construction of laws, regulations, systems, and policies for health information systems and computer-based patient records systems by all entities that use, handle, or store health information pertaining to individuals, or a combination thereof. The focus of this standard is primarily the individual recipient of healthcare; however, in some principles the privacy and confidentiality interests of practitioners and the confidentiality interests of providers are also recognized. While not developed in this standard it is recognized that patients are responsible for certain aspects of their care. This responsibility may include collecting and communicating personal health data. This data may reside in a health information system database or record.

6. Principles

6.1 The following statements of principles are organized into categories. Each category lists principles and provides a discussion related to the principle. The categories are:

6.1.1 Privacy.
6.1.2 Confidentiality.
6.1.3 Collection, Use, and Maintenance.
6.1.4 Ownership.
6.1.5 Access.
6.1.6 Disclosure/Transfer of Data.
6.1.7 Data Security.
6.1.8 Penalties/Sanctions.
6.1.9 Education.

7. Privacy

7.1 Individuals have privacy rights related to how information about them is collected, used, and disclosed.

7.1.1 Privacy is the right of an individual to be left alone. It includes freedom from intrusion or observation into one's private affairs and the right to maintain control over certain personal information. Individuals share personal information with healthcare providers and practitioners in the care process. However, individuals are entitled to expect the healthcare system and those involved to respect the individual's privacy.

7.1.2 Respect for individual privacy is demonstrated in the way the health information is collected, used, and disclosed. For individuals who are receiving health services the process of data collection, whether through interview, examination, or testing should respect the individual's privacy. The use of the information must be appropriate and respect the individual's privacy. Disclosures of information shall be sensitive to an individual's privacy and either be allowed by law or involve the consent of the individual or his or her designated representative.

7.2 Individuals have a right to know that identifiable, personal information is available in a health record, health information system, or other information system and to know to whom the information is available and the use of that information.

7.2.1 Those who collect data and maintain record systems should notify individuals of the types of information collected and generally how the information will be used and, if known, specific uses and locations of health information databases which will contain a patient's information, especially those that go beyond the boundaries of the provider healthcare organization. Examples of databases outside the provider organization are: regional registries for cancer, trauma, and implants; the Medical Information Bureau; third party payers; health data organizations; state and regional data systems; and research databases.

7.3 Healthcare organizations, practitioners, and others with access to health information shall respect an individual's right to privacy and provide appropriate protections to identifiable data and information.

7.3.1 Computer-based patient record systems and health information systems shall protect individual privacy. These systems should be capable of providing this protection to patients, practitioners and organizations. More extensive protections of data are typically required in the areas of mental health, sexually transmitted disease, obstetrics and drug/alcohol treatment. For example, drug/alcohol treatment regulations protect an individual's privacy by requiring that the facility not acknowledge an admission except to those individuals designated by the patient.

8. Confidentiality

8.1 Personally identifiable health information shall be treated confidentially.

8.1.1 Individuals and organizations that handle the health information shall not disclose it without patient consent, unless otherwise permitted or directed by law. Individuals expect that health information will be handled in a confidential manner. Individuals must be able to trust the healthcare systems with this sensitive information or they will forego care, withhold information, or provide inaccurate information.

8.2 All organizations or individuals who possess or have access to identifiable health information have a responsibility to protect the confidentiality of such information.

8.2.1 The complexities of the current healthcare system may require that a multitude of individuals, practitioners, and organizations within and outside the direct care process have access to an individual's health information. Each individual or entity, or both, with access to the information must respect its

confidentiality. Maintaining confidentiality acknowledges the individual's right to privacy and to control disclosure of personal information.

8.2.2 The responsibility for confidentiality includes the responsibility to use, disclose, or release such information with the knowledge and consent of the individual(s) identified.

8.2.3 In certain cases laws or regulations may require limited disclosure without consent (public health, law enforcement, etc.) or a specific detailed authorization to disclose health information (HIV status, mental health and drug treatment, etc.)

8.3 Appropriate means and mechanisms should be used to protect identifiable health information.

8.3.1 Health information protection methods and measures are available and should be used. A personal identifier which is not readily linkable to other non-health related databases helps to protect privacy of the individual. This identifier is not intended to preclude appropriate linkage but to discourage the development of mailing lists or cross referencing of health data with other private, governmental, public, or semi-public databases.

8.3.2 Encryption should be used when needed to protect the confidentiality of the data, for example, during transmission from one location to another or when it is important to link episodes of care but not disclose the identity of the individual.

8.3.3 Agreements with vendors and other business partners reinforce the commitment to protect the confidentiality of health information. Organizations may also use confidentiality agreements with staff to reinforce commitment to maintaining the confidentiality of health information.

8.3.4 Network systems should use measures to protect the confidentiality of health information. For example, access and dissemination controls, downloading of data to personal computers, combining of data files, off site linkage, and hardware placement.

9. Collection, Use, and Maintenance

9.1 Health information shall be collected and used only for a necessary and lawful purpose. Health information may not be used for purposes other than those for which it is collected.

9.1.1 The purposes for collecting health information should be related to the provision of health care or improving/protecting the health of individuals. Health information databases, especially those with identifiable or linkable patient data should only be used for appropriate purposes, for example, provision of care, health research, and related legally mandated purposes. These databases should not be used for other non-related purposes.

9.2 Organizations and individuals who collect, process, handle, or maintain health information should provide individuals and the public with a notice of information practices.

9.2.1 The notice of information practices should include: the scope and purpose of information collection; a description of the rights of individuals, including the right to inspect and copy information and the right to seek amendments; a description of the procedures for authorization and revoking authorizations; a description of the types of uses and disclosures that are permitted or required by law without the individual's authorization; the organization's policies regarding data storage, duration of retention of data and disposal thereof; a description of the general categories of uses to be made of data; and the point of contact for the health information system.

10. Ownership

10.1 The practitioner, provider, or organization that creates the patient record owns the record. The individual who supplies or is the subject of the health information has rights in the information.

10.1.1 The patient record is a business record for the practitioner, healthcare organization, or provider which creates the record. A variety of media may be used to store records (paper, microfiche, laser disk, computer disk). The business record describes and documents the healthcare services provided and is subject to applicable laws. Health information concerning an individual is intended primarily to foster and enhance the health of that individual with other uses (for example, billing, quality review, research) being secondary.

10.1.2 Individuals' and organizations' rights and responsibilities should be agreed upon, including the rights of practitioners who contribute to an organization's patient records and the rights of patients who are the subjects of the records.

10.1.3 The individual who is the subject of the health information typically has rights of access and disclosure. Those rights are subject to laws and regulations but usually allow an individual to access his or her health information or record, to amend the record by adding information and to consent to disclosures.

10.1.4 Society also retains an interest in using the health information for the public good, for example, public health.

11. Access

11.1 An individual shall be given reasonable access to his or her health information and may amend his or her record.

11.1.1 The patient or his or her designated personal representative has access rights to the data and information in his or her health record and other health information databases except as restricted by law. An individual should be able to inspect or see his or her health information or request a copy of all or part of the health information, or both.

11.1.2 An individual has a right to amend by adding information to his or her record or database to correct inaccurate information in his or her patient record and in secondary records and databases which contain patient identifiable health information. The request for amendment should include a timely review and response by the provider, practitioner, or other organization responsible for patient records or databases, or both.

11.1.3 Access to a record or file by the individual or the individual's representative, or both, shall be documented.

11.1.4 Response time for a request for information from an individual who is the subject of the health information or that individual's designated representative should be reasonable, either to produce the data or notify the requestor that the information does not exist or cannot be found. Appropriate staff should be available at reasonable times to assist an individual in reviewing his or her health information. The holder of the record or database should develop procedures

which address the form of the request, the hours of business, and any charge for services.

11.1.5 Access to all or part of a record or database can be denied the patient under certain circumstances. These circumstances vary by state. For example, a healthcare practitioner may limit access to information if knowledge of the information would be injurious to the patient's health. In this instance the information is released to a designated third party. Another example is access to information that could endanger the life or safety of another person or access to the name of an individual who filed a report in confidence.

11.1.6 Individuals should be notified of a change of custodian for their health information when health information is transferred to, stored in, or shared with a site, individual, or organization other than that of the original custodian. For example, hospital *A* closes and all patient records are transferred to hospital *B*. A notice in the local newspaper could provide reasonable notice of a change in custodian.

11.1.7 Not all information maintained by healthcare providers and other health-related organizations is accessible by an individual patient even though portions of that information may refer to an individual. Examples include organizational activities designed to perform peer review, engage in quality improvement, and review administrative procedures. The information used in these activities is not considered part of an individual's health record or health information database.

11.2 Providers, practitioners, and other organizations shall adopt systems which address the appropriate use and availability of health information.

11.2.1 Providers, practitioners, and healthcare organizations shall use systems which support the appropriate use of health information. Reasonably accurate, complete, legible, and timely information is needed for patient care and other related purposes. Some holders of health information will have summary information while others may hold detailed information. Use and availability over a lifetime could be provided by longitudinal patient records kept by patients or maintained in components by providers or in clinical data centers.

11.2.2 The computer-based patient record system and other health information databases should allow users and managers of health information systems to classify data for access purposes. The data classification process may address data by related data groups or by individual data elements. The system/database use should be supported by policies and procedures which identify users/roles authorized to read, enter, modify, amend, or download data.

11.2.3 The computer-based patient record system and other health information systems should be designed to verify the identity of the user and record each access to the record/database and the action taken (for example, read, copy, update, print, download, transfer). In addition to documenting the access by time, date, and individual it is also recommended that the purpose of the access be documented. Many authorizations contain a purpose statement which could be related to access. Internal organizational users should provide a purpose by category (for example, patient treatment, patient billing, utilization management, etc.).

11.2.4 The organization should periodically review the assignment of access privileges based on job duties, roles, and requirements. Inappropriate browsing of the system by authorized system users and others who attempt to access the system should be prohibited by policy and reviewed to prevent this activity.

11.2.5 The system should automatically record any apparent inappropriate access or breach of level of authorized access by a user and automatically notify the system's data security officer.

12. Disclosure/Transfer of Data

12.1 The basis for disclosure of protected health information is informed consent.

12.1.1 Identifiable health information should not be disclosed without the informed consent of the identified individual(s) except as required by law or for communication between the patient's current health care provider team. (See also 7.1.1, 8.1.1, 8.2.1, 8.2.3.)

12.1.2 In the healthcare setting where the individual is receiving service/treatment the consent may be implied or expressed. It is implied if the individual presents for care and then proceeds to share data and information with the provider. Consent is also implied in an emergency treatment situation. Consent is expressed when the agreement to share information is in writing. The implied or express consent extends to all members of the healthcare provider team. In the healthcare environment authorizations are used to obtain consent for the use and disclosure of health information. The purpose of the authorization is to protect personal privacy.

12.1.3 Information is disclosed for different purposes. Authorizations for treatment and authorizations for payment of treatment should be separated and presented in clear, simple language. For example, as a part of the general contract for payment of services an individual may have agreed to disclose to the third party payer relevant health information sufficient to pay a claim. However, most healthcare facilities verify this understanding by having the individual sign a specific authorization to release health information on a particular episode of care to the third party payer.

12.1.4 *Authorizations should contain*:

12.1.4.1 Subject individual's full name, address, phone number, and date of birth.

12.1.4.2 Name of person or institution that is to release the information.

12.1.4.3 Name of each individual or institution that is to receive the information.

12.1.4.4 Purpose or need for the information.

12.1.4.5 Specific designation of information to be disclosed, subject to restrictions by the patient to disclosure of a specific medical condition, injury, time period (dates of treatment), and/or any other type of specific information.

12.1.4.6 Specific date, event, or condition upon which the authorization will expire unless revoked earlier.

12.1.4.7 Statement that the authorization can be revoked or amended, but not retroactive to the release of information made in reliance on the authorization by the provider, practitioner, or other organization.

12.1.4.8 Signature of patient or person legally authorized to act on the patient or individual's behalf, and the date the consent is signed, where electronic, dated, and authenticated.

12.1.4.9 Statement that the recipient may not further disclose such information, unless further disclosure is expressly permitted in the authorization or is implicit in the purposes of the authorization.

12.1.4.10 Statement that the recipient may not use the information for any other purpose unless further disclosure is expressly permitted in the authorization or is implicit in the purposes of the authorization.

12.1.5 Implied consent to release or share treatment information between organizations/providers is assumed in continuity of care situations and in emergency treatment situations. In these situations an authorization may be processed after the treatment event.

12.1.6 Practitioners, providers, and other organizations should inform the individual of information uses, required reporting, and voluntary information sharing practices.

12.1.7 It is understood that a number of laws require reporting or disclosure. These laws are primarily laws which have been enacted to protect the public good. Reporting does not make the information public information. The information may only be used for the stated purpose, like communicable disease, elder abuse, and related regulations.

12.1.8 External reviews such as those for provider licensure or accreditation require the review of patient records or health information. Many of these external reviews are not focused on an individually identified person or patient. In a computerized environment a facility should produce a record without patient identifiers or with pseudo-identifiers for review purposes.

12.1.9 Organizations should review other uses of health information, for example, vendors, contractors, consultants and service personnel to see if identifiable information is needed and to develop agreements to protect the health information available during these service activities.

12.1.10 With an individual's consent or by law, clinical data centers and health data organizations may accumulate data on individuals over time from a variety of sources. An individual should be able to have some form of access to the aggregate record and authorize all or part of its release to another party. Typically an individual will authorize release of his or her complete record to a healthcare provider. There may, however, be occasions when the individual chooses to release only a portion of his or her record. For example, an ophthalmologist will not need to know that an individual had an abortion 20 years ago in order to perform an eye exam. Individuals should recognize the information.

12.1.11 When information is released pursuant to the individual's authorization the party receiving the health information shall not further redisclose the information without the individual's consent to disclose the health information except in an emergency treatment situation.

12.2 Research and analysis of data shall be conducted in a manner which protects an individual's privacy and the confidentiality of their health information.

12.2.1 Data should be made available to promote progress in prevention and treatment of disease and planning, evaluation, and policy development in health care. The provider, practitioner, organization, or data center, or a combination thereof, with health information must have a system in place which evaluates each request for data, determines its appropriateness, and places the necessary constraints on the requestor's access to and use of the data. The data may be used to meet research, planning, prevention, and policy development needs. Health information, which identifies persons, should be disclosed only with the consent of the persons identified or through an organizational review process that imposes confidentiality requirements on the requestor.

12.3 Health information may not be redisclosed without the authorization of the individual(s) who is the subject of the information.

12.3.1 Generally recipients of identified or identifiable health information may not rerelease the information without the authorization of the individual(s) or someone authorized to act on behalf of the individual(s). This prohibition is clear in some areas of the law but not in others. As the sharing of data is facilitated through electronic means it is important to address this issue and develop guidelines and policies in this area. (See also 12.1.11.)

12.4 The sharing and transfer of data shall be in a manner that ensures privacy, confidentiality, integrity, quality, and security of the information.

12.4.1 Organizations and individuals should ensure that the quality and integrity of data is not lost in an internal or external data transfer process. Controls should be used to limit the transmission of data to authorized recipients. For example, encryption should be used when the transmission between systems/sites is not secure; fax machines and other devices used to transmit/receive identifiable health information or copy identifiable health information, or both, should be in secure areas.

12.4.2 Copies, faxes, printouts, or any medium containing health information should be destroyed after use or retained in a secure location. Transmitted material should be accompanied by a statement of confidentiality and responsibility. The receiving party is then responsible for the security and confidentiality of the transmitted/copied health information.

13. Data Security

13.1 Policies and procedures shall be in place to ensure that the confidentiality, integrity, quality, and security of an individual's health information shall not be compromised.

13.1.1 A wide variety of tools, policies, and procedures should be used by healthcare providers and other individuals and organizations to achieve the goals of confidentiality, data security, data quality, and data integrity. Examples include:

13.1.1.1 Audit and control procedures to ensure appropriate use of data by authorized handlers and users as well as detection of unauthorized individuals.

13.1.1.2 Audit and control procedures to protect data from unauthorized accidental or intentional disclosure.

13.1.1.3 Procedures to deny access to employees, medical staff members, and others who no longer have authority to access and a need to know information.

13.1.1.4 Routine backup of data.

13.1.1.5 Secure storage of data in a manner that will withstand deterioration, corruption, and unauthorized destruction.

13.1.1.6 Documentation of the data storage process and media used.

13.1.1.7 Procedures to protect programs from unauthorized modification and inspection.

13.1.1.8 Physical security for appropriate components of information systems including computer rooms, printers, network components, data archives, health record areas, printed reports, downloaded data, the documentation on computer programs, and remote devices.

13.1.1.9 Alarms/alerts for hardware failures.

13.1.1.10 Safeguards to minimize/limit data loss and downtime.

13.1.1.11 Backup plan for system downtime.

13.1.1.12 Testing of new programs and communication interfaces with existing programs/system components to avoid introducing errors into an existing system.

13.1.1.13 Procedures to monitor and evaluate the security of the data systems.

13.1.1.14 Verification of data entries using quality control measures.

13.1.1.15 Maintenance for a reasonable time of a directory of data users (current and past). This directory contains demographic information on the user, the user's position in or relation to the organization, level of authorized use, and other data security information.

13.1.1.16 Maintenance for a reasonable time of a directory of the system's developers (current and past).

13.1.1.17 Secure storage of authentication data/information, for example, passwords, biometrics.

13.1.1.18 Mechanisms and policies introduction of viruses or any unauthorized changes in the system.

13.1.1.19 Monitoring and audit procedures to check data consistency and data plausibility.

13.1.1.20 Mechanisms to identify the source of each datum in the database.

13.1.1.21 Safeguards to prevent the allocation of data to the wrong patient.

13.1.1.22 Mechanisms to label reports as to their status, (for example, interim document, draft document, final document, amended document) and to hold a report/document until it is ready for release to the patient record or for other purposes. Procedure to retain any report or results disseminated as well as the final report. (Clinical decisions may have been made based on data available.)

13.1.1.23 Mechanisms to amend patient record and health information. (Once data items are "placed" in the patient record they can only be changed using an amendment process. The individual amending the record must have authorization to amend the record. The most current version, the amended version, should be the version retained in the active record with reference to any previous versions.)

13.1.1.24 Authentication.

13.1.1.25 Encryption of data.

13.1.1.26 Digital signatures.

13.1.1.27 Internal audits to monitor organizational compliance with policies.

14. Penalties/Sanctions

14.1 Violation of organizational and individual confidentiality and privacy contracts and policies shall have enforced sanctions.

14.1.1 All organizations and individuals shall adopt and use sanctions to deter inappropriate access, misuse of data, unauthorized release of data and sharing of access mechanisms. Organizations and individuals can reinforce their commitment to appropriate use of identifiable health information by developing sanctions for employees and others with whom they have business relationships.

14.1.2 Intentional violations should be penalized more severely. Response to negligent, inadvertent, or accidental violations should include the reeducation of the individual as well as a review of related policies and procedures. Penalties should be adjusted to fit the situation ranging from dismissal from the job or loss of contract to lesser sanctions.

14.1.3 Organizations and individuals should both be able to bring civil actions against wrongdoers.

14.1.4 Individuals shall be informed of known breaches of their privacy and confidentiality.

15. Education

15.1 Any individual or organization which handles or stores personally identifiable health information has the obligation to educate their staff and others with whom they have business relationships regarding the privacy, confidentiality, access and data security principles, and policies of the organization.

15.1.1 Users and handlers of health information, for example, providers, practitioners, payers, patients, third party payers, analysts, system developers and others, must be educated regarding the appropriate use of health information. These individuals and their organizations have responsibilities related to the information. Programs to educate and periodically remind individuals of their obligations support the overall goal of protecting the confidentiality of health information. Systems must use security mechanisms but it is knowledgeable, ethical staff and business owners who ultimately are responsible for achieving the goal of maintaining the confidentiality of health information. Ethical, knowledgable staff also contribute significantly to this goal.

NOTE 2—Irrespective of any case, instance, circumstance, law, or regulation that may invalidate, make illegal, or make unenforceable any principle or provision of this standard, the validity, legality, and enforceability of the remaining principles and provisions shall not in any way be affected or impaired thereby. In particular the specific provisions concerning ownership, confidentiality, consent for disclosure, and notification should be honored and considered as valid principles, whose guidelines should be followed, irrespective of whether or not there is a legal necessity to do so. For instance, concerning laws for public health disclosure, notification to the individual whose information is being disclosed and released should be given, irrespective of the fact that there is no legal requirement that such notification be given.

ADDITIONAL MATERIAL

(**1**) Abdelhak, Mervat, Grostick, Sara, Hanken, Mary Alice, Jacobs, Ellen, *Health Information: Management of a Strategic Resource*, W.B. Saunders, Philadelphia, 1996.

(**2**) Brandt, Mary, *Maintenance, Disclosure and Redisclosure of Health Information*, American Health Information Management Association, Chicago, IL, 1995.

(**3**) Bruce, JoAnne, *Privacy and Confidentiality of Health Care Information*, 2nd Edition, American Hospital Publishing, American Hospital Association, Chicago, IL, 1988.

(**4**) Donaldson, Molla, and Lohr, Kathleen, *Health Data in the Information Age: Use, Disclosure and Privacy*, Institute of Medicine, National Academy Press, Washington, DC, 1994.

(**5**) Fitzmaurice, Michael, *Putting the Information Infrastructure to Work: Health Care and the National Information Infrastructure*, AHCPR/NIST, Publication 857, 1994, pp. 41–55.

(**6**) Gabrieli, Elmer, *Ethical Tenets for Clinical Data Centers*, 1980.

(**7**) Gostin, Lawrence, Turek-Brezina, Joan, et al. "Privacy and Security of Personal Information in a New Health Care System," *JAMA*, November 24, 1993, Vol 270, No. 20, pp. 2487–2492.

(**8**) Information System Security and Confidentiality, *In Confidence*, American Health Information Management Association, July, 1994, pp. 5–7.

(**9**) Medical Records Confidentiality Act of 1995—Proposed legislation.

(**10**) Privacy Act, 5 U.S.C. 552a, 1996.

(**11**) "Protecting Privacy in Computerized Medical Information," Office of Technology Assessment, Government Printing Office, 1993. (S/N 052-003-01345-2).

(**12**) "Toward a National Health Information Infrastructure," Report of the Workgroup on Computerization of Patient Records to the Secretary of the U.S. Department of Health and Human Services, April 1993.

(**13**) Waller, Adele, and Fulton, Deborah, "The Electronic Chart: KeepingIt Confidential and Secure," *Journal of Health and Hospital Law*, April 1993, Vol 26, No. 4, pp. 104–109. Washington Administrative Code (WAC 248-18-001 (7)).

(**14**) Westin, Alan, *Computers, Health Records and Citizens Rights*, U.S. Department of Commerce, National Bureau of Standards, 1976.

(**15**) Wright, Benjamin, "Law of Electronic Commerce, Chapter 21," *Electronic Health Care Information: Recordkeeping and Privacy Aspects*, Little, Brown and Company, Boston, 1993.