Designation: E 1986 – 98

An American National Standard

Standard Guide for Information Access Privileges to Health Information[1]

This standard is issued under the fixed designation E 1986; 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 process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organizational data in the healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.

1.2 This guide is based on long-term existing and established professional practices in the management of healthcare administrative and clinical data. Healthcare data, and specifically healthcare records (also referred to as medical records or patient records), are generally managed under similar professional practices throughout the United States, essentially regardless of specific variations in local, regional, state, and federal laws regarding rules and requirements for data and record management.

1.3 This guide applies to all individuals, groups, organizations, data-users, data-managers, and public and private firms, companies, agencies, departments, bureaus, service-providers, and similar entities that collect individual, group, and organizational data related to health care.

1.4 This guide applies to all collection, use, management, maintenance, disclosure, and access of all individual, group, and organizational data related to health care.

1.5 This guide does not attempt to address specific legislative and regulatory issues regarding individual, group, and organizational rights to protection of privacy.

1.6 This guide covers all methods of collection and use of data whether paper-based, written, printed, typed, dictated, transcribed, forms-based, photocopied, scanned, facsimile, telefax, magnetic media, image, video, motion picture, still picture, film, microfilm, animation, 3D, audio, digital media, optical media, synthetic media, or computer-based.

1.7 This guide does not directly define explicit disease-specific and evaluation/treatment-specific data control or access, or both. As defined under this guide, the confidential protection of elemental data elements in relation to which data elements fall into restrictive or specifically controlled categories, or both, is set by policies, professional practice, and laws, legislation and regulations.

2. Referenced Documents

2.1 *ASTM Standards:*

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

E 1633 Specification for Coded Values Used in Computer-Based Patient Record[2]

E 1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records[2]

E 1987 Guide for Individual Rights Regarding Health Information[2]

PS 101 Provisional Guide on Security Framework for Healthcare Information[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. **(E 1869)**

3.1.2 *access control*—the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2.1 *Discussion*—Access control counters the threat of unauthorized access to, disclosure of, or modification of data. **(ISO 7498-2)**

3.1.3 *accountability*—the property that ensures that the actions of an entity can be traced. **(ISO 7498-2)**

3.1.4 *audit trail*—data collected and potentially used to facilitate a security audit. **(ISO 7498-2)**

3.1.5 *authentication*—the corroboration that an entity is the one claimed. **(ISO 7498-2)**

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

Current edition approved Oct. 10, 1998. Published November 1998.

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

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. **(E 1869)**

3.1.7 *authorization—(1)* The granting of rights, which includes the granting of access based on access rights. *(2)* The mechanism for obtaining consent for the use and disclosure of health information. **(ISO 7498-2, CPRI, AHIMA)**

3.1.8 *confidential*—status accorded to data or information indicating that it is sensitive for some reason and needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorized individuals or organizations with an approved need to know. Private information which is entrusted to another with the confidence that unauthorized disclosure that will be prejudicial to the individual will not occur. **(E 1869)**

3.1.9 *confidentiality*—the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. **(ISO 7498-2)**

3.1.10 *database*—a collection of data organized for rapid search and retrieval. **(Webster's, 1993)**

3.1.11 *data element*—the combination of one or more data entities that forms a unit or piece of information, such as the social security number, a diagnosis, an address, or a medication.

3.1.12 *data entity*—a discrete form of data such as a number or word.

3.1.13 *disclosure (health care)*—the release of information to third parties within or outside the healthcare provider organization from an individual's record with or without the consent of the individual to whom the record pertains.

3.1.13.1 *Discussion*—Under this guide the definition is slightly modified to read: the release of information to an individual, group or organization from an individual's health information with or without the authorization of the individual to whom the health information pertains. **(CPRI)**

3.1.14 *emergency*—a sudden demand for action. Condition that poses an immediate threat to the health of the patient.

3.1.15 *healthcare data*—data which are input, stored, processed or output by the automated information system which support the business functions of the healthcare establishment. These data may relate to person identifiable records or may be part of an administrative system where persons are not identified. **(CEN)**

3.1.16 *health information*—any information, whether oral or recorded in any form or medium *(1)* that is created or received by a healthcare 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 payments 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. **(HIPAA, E 1869)**

3.1.17 *information*—data to which meaning is assigned, according to context and assumed conventions. **(National Security Council, 1991, E 1869)**

3.2 *Definitions of Terms Specific to This Standard:*

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

3.2.1.1 *external disclosure*—disclosure outside an organization.

3.2.1.2 *internal disclosure*—disclosure within an organization.

4. Significance and Use

4.1 The maintenance of confidentiality in paper-based, electronic, or computer-based health information requires that policies and procedures be in place to protect confidentiality. Confidentiality of information depends on structural and explicit mechanisms to allow persons or systems to define who has access to what, and in what situation that access is granted.

4.2 Confidential protection of data elements is a specific requirement. The classification of data elements into restrictive and specifically controlled categories is set by policies, professional practice, and laws, legislation, and regulations.

4.3 There are three explicit concepts upon which the use of and access to health information confidentiality are defined. Each of these concepts is an explicit and unique characteristic relevant to confidentiality, but only through the combination (convergence) of all three concepts can appropriate access to an explicit data element at a specific point in time be provided, and unauthorized access denied. The three concepts are:

4.3.1 The categorization and breakdown of data into logical and reasonable elements or entities.

4.3.2 The identification of individual roles or job functions.

4.3.3 The establishment of context and conditions of data use at a specific point in time, and within a specific setting.

4.4 The overriding principle in preserving the confidentiality of information is to provide access to that information only under circumstances and to individuals when there is an absolute, established, and recognized need to access that data, and the information accessed should itself be constrained only to that information essential to accomplish a defined and recognized task or process. Information nonessential to that task or process should ideally not be accessible, even though an individual accessing that information may have some general right of access to that information.

5. Principles

5.1 The following principles are based upon U.S. state and federal laws, current European Economic Community initiatives and laws and regulations resulting from those initiatives, and professional practice within the U.S. and European healthcare domains.

5.2 Individuals, groups, and organizations retain rights over the specific, intermediate, and ultimate use of any data collected from them and about whom the data is retained and managed.

5.3 No individual, group, or organizational data shall be collected, used, maintained, released, or disclosed without the specific explicit informed consent of the individual, group, or

organization, unless specifically required for the protection of public health, and mandated by local, state, regional, or federal law.

5.4 Individual, group, or organizational data may only be used for the purpose for which it was collected. Explicit informed consent of the individual, group, or organization from which the data was collected is required if the data is to be used for any additional purpose. Organizational policies shall state the purposes for which data will be collected, maintained, and used.

5.5 All individuals, groups, organizations, data-users, data-managers, and public and private firms, companies, agencies, departments, bureaus, service-providers, and similar entities that collect individual, group and healthcare related data, are required to collect, manage, maintain, disclose, provide access to, or release that data only in strict compliance with the data access rules defined in this guide. If they are unable to adhere to this guide they will not retain data beyond its initial collection and use, or will securely and confidentially entrust that data to an authorized organization that can abide by the rules under this guide.

5.6 Data and data elements under this guide are defined at a discrete level. This is necessary in order to define data access and use rights down to discrete elemental data. This guide is established under the assumption that there is no such thing as "dis-identified data" in that as long as data exist as discrete elemental data they are ultimately identifiable with an individual. For example a diagnosis or a patient weight is not dis-identified within a population just because it does not have a name or other outward identifying information attached or linked to it. The average weight within a population or the incidence of a given disease, both calculated or derived from a population aggregate, may be dis-identified from an individual within a population, but might still predispose the population to identification or prejudice. For example an "abnormal" average weight might increase the health risk to a population, therefore providing valuable preventative and epidemiological data, but if that data is assumed to be dis-identified and generally available for review, then it might allow population-based prejudicial pricing for healthcare services or insurance. Disease incidence can also be used to target populations at health risk, but if considered dis-identified and generally available for review, disease incidence can also be used to identify populations as to race, religion, ethnicity, genetics, sexual preferences, and other prejudicial indicators. The protection of individual, group, and organizational data confidentiality under this guide is, therefore, absolute and is always based upon the connection of that data to the individual, group, or organization from which the data was collected and for or about whom the data is retained and managed. No data is releasable as discrete data or discrete data-types under any assumption that since another related data element (for example, name, age, sex, address, etc.) was not released, that the data is no longer individual, group, or organizational data, or can no longer be identified or connected to any individual, group, or organization.

5.7 All access shall be explicitly authorized. Unauthorized access is explicitly forbidden.

6. Data Elements

6.1 Data elements under this guide represent fragmentation (separation) of data into discrete entities. These entities (data elements) represent discrete elemental data types that can be reconstructed into complete data sets according to varying needs and requirements of access and use, by appropriate data-users, under appropriately defined and authorized roles. Data elements exist as discrete data in their own right or can be aggregated as data sets that represent data about a specific individual, provider, group, or organization, or they can be aggregated across individuals, providers, groups, or organizations.

6.2 Data elements and data entities under this guide are explicitly delineated and apply to healthcare related data in aggregate as well as discrete forms.

6.3 If data exist in aggregate form and cannot be broken down or protected from improper use or disclosure at the data element or entity level, then the aggregate data itself cannot be released for use or disclosure to any data-user other than those who meet the access privilege rules for the most confidential data within that aggregate.

6.3.1 *Example*—HIV data within a document, even if only a small fraction of the content of that document, makes the entire document subject to the rules of disclosure defined for HIV data, unless that HIV data (or any other data of that class) can be stripped (removed) from the document.

6.3.2 In addition, if aggregate data is stripped of any non-disclosable data for disclosure to a data-user, then the disclosed data can have no evidence, sign, or indication of the fact that it was stripped of non-disclosable data. An exception under this requirement should be granted only in the instance where it is impossible or impractical to screen or filter confidential data from the aggregate form in which it was entered into the health record, such as handwritten or dictated and transcribed physician notes or histories and physicals that contain data of differing levels of confidentiality. In the instance of hand written or dictated and transcribed data non-disclosable data should still be masked when these data are reviewed or accessed by data-users without appropriate authorization to review and access the most confidential elemental data within that data set.

6.4 This guide does not put any explicit restrictions on the type or format of health information content. An example set of data elements to illustrate the breakdown or partitioning of health information into confidential data sets that warrant differing levels of access are listed in Table 1. The presence of a data element or entity in that list is explicitly not a suggestion, requirement, or mandate to collect, store, or maintain that data element or entity. In fact, in the maintenance of confidentiality and privacy it is important to keep the minimum amount of data required to accomplish the specific tasks for which the data is being collected, disclosed, stored, and maintained. Also, please note that data elements and entities in that list are not specifically in each instance of use necessarily defined as healthcare data. The list is comprised of data elements and entities that may, but are not required to be

collected, utilized, stored, or maintained, or a combination thereof, in the process of providing healthcare administrative and clinical services.

TABLE 1 Data Elements Warranting Differing Levels of Access Control

- Unique ID
- Unique ID to Number Mapping(s)
- Address(es)
- Phone(s)
- Electronic Mail Address(es)
- Photograph(s)
- Biometric Token(s) (fingerprint, retinal image, handwriting, signature, etc.)
- Passwords, IDs, Authentication Data
- Insurance (discretely defined by type)
  - Health
  - Auto
  - Workman's Compensation
  - Disability
- Employment
- Relatives
- Genetic Data (discretely defined by type)
- Blood Type
- Family Health History
- Race/Nationality/Ethnicity
- Citizenship
- Political Affiliation
- Religion
- Diet or Dietary Preferences
- Sexual Preference
- Personal Habits (discretely defined by type)
- Immunizations
- Advanced Directives
- Power(s) Of Attorney
- Living Wills
- Allergies (discretely defined by type)
- Adverse Reactions (discretely defined by type)
- Diagnoses (discretely defined by type)
- Problems (discretely defined by type)
- Procedures (discretely defined by type)
- Injuries (discretely defined by type)
- Mental Health Problems/Diseases/Diagnoses (discretely defined by type)
- Clinical Symptoms
- Clinical Findings
- Substance Use/Abuse
- Health Care Encounter(s)
  - Encounter Type
  - Reason For Encounter
  - Disposition
  - Provider Identification
  - Procedure(s)
  - Problems(s)
  - Diagnosis(es)
  - Appointment(s)
  - Provider Encounter Record/SuperBill
  - Bill For Services
  - Claim Form(s)
  - Clerical Billing Process Documentation
  - Payment Form
  - Payment
  - Denial
  - Receipt Request
  - Receipt
  - Remittance Advice
  - Remittance
  - Financial Transaction
  - Request for Clarification
  - Adjudication
- Consent Forms
  - Treatment/Admission
  - Procedure
  - Photography
  - Health Plan Membership
  - Data Rights, Ownership, and Disclosure (Data or Disclosure Request Forms)
  - Research
  - Protocol
  - Public Health Disclosure
  - Publication
- Electronic Mail Messages
- Fax(es)
- Documentation
  - Triage Note(s)
    - Administrative
    - Physician
    - Non-physician Provider
    - Nursing
    - Pharmacy
    - Ancillary Services
    - Social Services
    - Ambulance (Transport) Run Sheet
    - Health Plan/Insurer
  - Telephone Note(s)
    - Administrative
    - Physician
    - Non-physician Provider
    - Nursing
    - Pharmacy
    - Ancillary Services
    - Social Services
    - Out-sourced Service Provider
    - Third Party Intermediary
    - Claims Clearing House
    - Health Plan/Insurer
  - Telephone Messages
    - To Administrative Personnel
    - To Physician(s)
    - To Non-physician Provider(s)
    - To Nursing
    - To Pharmacy
    - To Ancillary Services
    - To Social Services
    - Out-sourced Service Provider
    - Third Party Intermediary
    - Claims Clearing House
    - To Health Plan/Insurer
    - Coordinator Of Care / Services
      - Behavioral Health
      - Home Health
  - Correspondence
    - To Administrative Personnel
    - To Physician(s)
    - To Non-physician Provider(s)
    - To Nursing
    - To Pharmacy
    - To Ancillary Services
    - To Social Services
    - To Out-sourced Service Provider
    - Third Party Intermediary
    - To Claims Clearing House
    - To Health Plan/Insurer
    - To Billing Intermediary
    - To Government Agencies
    - To Accrediting Agencies
    - To Employers
    - To Schools and Educational Institutions
    - To Regulatory Agencies
    - Consent, Access and Disclosure Notifications
  - Outpatient Nursing Note(s)
  - Inpatient Nursing Note(s)
  - Home Health Nursing Note(s)
  - Outpatient Pharmacy Note(s)
  - Inpatient Pharmacy Note(s)
  - Home Health Pharmacy Note(s)
  - Outpatient Physician Note(s)
  - Inpatient Physician Note(s)
  - Home Health Physician Note(s)
  - Outpatient Non-physician Provider Note(s)
  - Inpatient Non-physician Provider Note(s)
  - Home Health Non-physician Provider Note(s)
  - Outpatient Ancillary Service Note(s)
  - Inpatient Ancillary Service Note(s)
  - Home Health Ancillary Service Note(s)
  - Dictations and Transcriptions

- Dictation(s)
- Dictation Media
- Transcription(s)
- Transcriptionist's Notes
- Administrative Notes

Procedure Note(s)
- Physician Procedure Note(s)
- Non-physician Provider Procedure Note(s)
- Nursing Procedure Note(s)
- Ancillary Service Procedure Note(s)
- Pharmacy Procedure Note(s)

Operative Reports
- Physician Operative Report(s)
- Non-physician Provider Operative Report(s)
- Nursing Operative Report(s)
- Ancillary Service Operative Report(s)
- Pharmacy Operative Report(s)

Medication Related Requests and Notes
- Medication Name(s)
- Written Orders
- Vebal Orders
- Written Prescriptions
- Verbal Prescriptions
- Medication Administration Note(s) (MAR)
- Medication Dispensing Note(s)
- Medication Allergy/Adverse Reaction Note(s)
- Medication Adverse Drug Event (ADE)
- Medication Preparation Note(s)
- Medication History
- Pharmacy Claim

Orders and Requests (representing orders/requests from provider or patient, where provider can be physician, advanced practice registered nurse, nurse, pharmacist, ancillary service, administration, or other)
- Written Orders/Requests
- Verbal Orders/Requests

Clinical Guidelines
Clinical Protocols
Treatment Plans
Admission Notes
- Nursing
- Non-physician Provider
- Physician
- Pharmacy
- Ancillary Service
- Administrative

Discharge Notes
- Nursing
- Non-physician Provider
- Physician
- Pharmacy
- Ancillary Service
- Administrative

Social Service Notes
Death Certificate
Coroner Request/Wrongful Death Notification
Request For Autopsy
Coroner's Report
Bereavement Notes
Clinical Specimens, Data and Findings
- Specimen Labels (with patient name or identifying data)
- Images
  - Diagnostic Images
  - Documentation of Injury
  - Documentation of Procedure
- Sound/Audio Records
- Graphics
- Biometric/Waveform Tracings
- Clinical Device Output
- Laboratory Results
- Specimens
- Result Requests, Labels and Forms
- Laboratory Department Specimen Data
- Toxicology Reports

Quality Assurance Data
- Related to Patient
- Related to Providers
- Related to Department
- Related to Institution/Organization

Utilization Data
- Related to Patient
- Related to Providers

Comparative Practice/Provision of Care Data
- Related to Patient
- Related to Providers

Medical Malpractice Data

7. Data-User Roles

7.1 Data-user roles are defined under this guide to represent all potential data-users within the healthcare clinical and administrative domain. It is explicitly stated under this guide that no one outside of defined user roles (defined by specific role or class within a healthcare setting or organization providing healthcare clinical or administrative services) is to be allowed any data access or disclosure to confidential health data about an individual, group, or organization.

7.2 This guide does not put any explicit restrictions on the specific roles defined for any organization. The intent is to require organizations to classify all data-users of health information into categories that clearly define each data-user or each data-user type's access privileges.

7.3 Under this guide a given data-user can have multiple roles, but each of the roles shall be manifest for that individual discretely, one at a time, with separate discrete user authentication (data use or log-on), audit and access/disclosure logging for each instance of data access/disclosure. Explicitly, a given user can have more than one role, but can function in only one role and capacity at a time.

7.4 An example set of roles to illustrate the breakdown or partitioning of healthcare personnel that warrant differing levels of access are listed in Table 2. The presence of a role on that list is explicitly not a suggestion, requirement, or mandate to provide health information access to personnel in that role in a specific organization. In fact, in the maintenance of confidentiality and privacy it is important to allow access to data only to individuals who need to accomplish specific tasks. Also, please note that roles in that list are not specifically in each instance of use necessarily defined as healthcare providers. The list is comprised of roles that may, but are not required to provide healthcare administrative and clinical services.

TABLE 2 Healthcare Personnel that Warrant Differing Levels of Access Control

Licensed Health Care Providers
- Physician (MD/Allopath, Osteopath, Chiropractic, Naturopath, Homeopath)
- Advanced Practice Registered Nurse (NP, NM, CAN, CNS)
- Physician Assistant (PA)
- Midwives
- Registered Nurse (RN)
- Pharmacist (DP)
- Licensed Vocational Nurse (LVN)
- Non-western Medicine Providers
- Ancillary Service Providers
  - Occupational Therapy
  - Physical Therapy
  - Cast Technicians
  - Prosthetic Technicians
  - Speech Therapy
  - Respiratory Therapy
- Technician
  - Procedure-based (OR, Cath Lab, etc.)
  - Departmental
  - Specialty
  - General

- Non-Licensed Health Care Providers
  - Nurse's Aide
  - Orderly
  - Phlebotomist
  - Bereavement Counselor
  - Volunteer
  - Technician
  - Patient Transportation Personnel
  - Specimen Transportation Personnel
  - Health Record Transportation Personnel
- Emergency Services
  - Paramedic
  - EMT
  - EMS
  - Ambulance Drivers
  - Air Transport Pilots
- Secular Services (Priest, Rabbi, Pastoral Care, etc.)
- Patient Advocate
- Interpreters
- Clerical and Administrative Personnel
  - Encounter Registration Clerk
  - Admission Clerk
  - Ward/Unit/Clinic Clerk
  - Departmental Clerk
    - Clinical Services
    - Laboratory Services
    - Imaging Services
    - Pharmacy Services
    - Social Services
    - Ancillary Services
- Disposition/Discharge Clerks
- Administrative Support Staff and Services
  - Physician Office
  - Non-physician Provider Office
  - Clinical Department
  - Administrative Department
  - Health Records (Medical Records)/Health Information Management Department
  - Quality Assurance
- Transcription Personnel
  - Transcriptionist
  - Proofreader
  - QA Personnel
  - Clerks
  - Students
  - Supervisors/Managers
  - Vendors
  - Maintenance and System Support Personnel
- File Clerk
  - Clinical Department
  - Administrative Department
  - Health Records (Medical Records)/Health Information Management Department
  - Quality Assurance
- Supervisory Personnel
  - Clinical Department
  - Administrative Department
  - Health Records (Medical Records)/Health Information Management Department
  - Quality Assurance
- Health Records (Medical Records)/Health Information Management Department
  - Administration
  - Administrative Support
  - File Clerks
  - Information Management Personnel
- Information Services
  - Database Administrator
  - Network Administrator
  - Security Administrator
  - Trainer (of end-users)
  - Help Desk
  - Operations Support
  - System Administrator
  - Applications Support
  - Business Analyst
  - Programmers
  - Third Party Support (Vendors and Consultants)
- Financial Services, Billing and Claims
  - Billing File Clerk
  - Billing Personnel
  - Claims Personnel
  - Coders/Reimbursement Specialists
  - Administrative Support Personnel
  - Collections Personnel
  - Cost and Quality Analysts
- Quality Assurance
- Utilization Review
- Discharge Planning
- Infection Control
- Risk Management
- Health Plan/Insurer
  - Claims File Clerk
  - Claims Review Personnel
  - Claims Adjudication Personnel
  - Internal Quality Assurance Personnel
  - Health Care Provision Quality Assurance Personnel
  - Internal Utilization Review Personnel
  - Health Care Provision Utilization Review Personnel
  - Administrative Support Personnel
- Medical Malpractice
  - Health Records File Clerk
  - Health Records Supervisor
  - Lawyer/Judge
  - Legal Aide
  - Legal Secretary
  - Expert Witness
  - Governmental File Clerk
- Accrediting and Regulatory Agencies
  - JCAHO Auditors
  - NCQA Auditors
  - Local, State and Federal Agencies
  - Local, State and Federal Surveyors
- Administrative Management
  - Executive Officers
  - Board of Trustees
  - Medical Staff Administration
  - Administrative Support Staff

8. Data Access and Use Privileges

8.1 Data access, disclosure, and use privileges under this guide are allowed only under authorization of the individual, group, or organization from whom the data was collected and for or about whom the data is retained and managed.

8.2 Aside from specifically defining data elements and user roles and the associated access and disclosure rules for a specific data element and user role, all data, in all instances of use, access, and disclosure that do not need to be uniquely identified as to a specific individual (patient, provider), group, or organization, should be stripped of uniquely identifying characteristics at the time of use, access, and disclosure. Explicitly, data should be uniquely identified with an individual, group, or organization only when specifically required for performance of a defined task, or when absolutely required for patient or individual safety.

8.2.1 *Example(s)*—Lab specimens should be labeled with the patient's name for safety reasons, but once the results are obtained and verified from that specimen, there is no need for any but specifically approved lab personnel to associate results with an individual patient.

8.2.2 Note this is specifically where unique and encrypted patient, provider, group and organizational unique ID numbers can best be utilized to uniquely, but safely dis- identify data. This is where a number (encrypted or dis-identified) would be used in place of a name, preserving the correct association of data with the individual, but removing all direct identifying characteristics.

8.3 Once disclosed, data are to be used only in the direct provision of clinical, administrative, and legal services as defined by the user role of the individual to whom confidential data has been disclosed. If data is to be stored and retrieved for re-use, such as for the collection and maintenance of a longitudinal record, or for epidemiological or other data tracking or aggregate uses, all provisions under Section 5 of this guide must be met, including but not limited to obtaining explicit informed consent, otherwise, once used, all data and all appropriate copies of the data are to be returned to the individual, group, or organization who provided disclosure or destroyed. Destruction of data at the completion of use is preferred under this guide versus storage in readable or otherwise disclosable form while not under the protection of the individual, group, or organization who provided disclosure. The only information under this guide that can be maintained, unless specific authorization has been obtained from the individual, group, or organization about whom the data will be maintained, is that data which are essential for the support of business practices and are maintained as business records. These business records, however, shall be maintained as confidential, under the provisions of this guide if they contain confidential health information as defined under this guide.

8.4 Under this guide quality assurance or utilization review data, or both, is to be considered non-disclosable and undiscoverable, unless explicitly used to gauge, judge, rate, or review the use of clinical or administrative services, or the quality of service or clinical care provided by an individual, group or organization. If, and only if quality assurance or utilization review data, or both, is used to gauge, judge, rate, or review the use of clinical or administrative services, or the quality of service or clinical care provided by an individual, group, or organization, then, and only then, is it disclosable, and then only to the individual, group, or organization being gauged, judged, rated, or reviewed. Quality assurance and utilization review data under this guide are disclosable only with the authorization of the individual, group, or organization from whom, or about whom the data was collected or generated, or both, and for or about whom the data is retained.

8.5 The overriding constraint on data users is to use (access and disclose) the minimum data needed to provide service to the individual patient, provider, group, or organization and to allow data users access to individual patient, provider, group, or organizational data only to those individuals and entities to whom they are providing direct, consult, referral clinical care or advice, or administrative services or review. Administrative review is allowed only when there is authorization to provide quality, financial, or utilization review.

8.6 Role-based disclosure within an overall access matrix can be further defined by a set of role-specific, case-specific, situation-specific, and policy-specific parameters defined as follows:

Clinical Case Specific
Encounter Specific (inclusive of outpatient, inpatient, home health)
Billing/Claim Event Specific
Registration Specific (inclusive of health plan registration, encounter registration, admission)
Problem Specific (inclusive of Diagnosis Specific, Disease Specific, Disorder Specific)
Department Specific
Departmentally Generated (images without reports)
Test Specific
Result Specific
Procedure Specific
Specimen Specific
Shift Specific
Workgroup Specific
Education/Training Specific
Therapeutic Agent Specific
Diagnostic Agent Specific
Dis-Uniquely Identified Only

8.6.1 These parameters should be applied, where and when appropriate, to specific data elements and specific user roles. An example is a clinical provider giving care to a patient during a shift should be granted access to specific data elements he or she needs to carry out the assigned clinical function in taking care of the patient during that shift. At the end of the shift, however, access to that patient's health information should end. This is defined in an access matrix as "Shift Specific" access. Another example is "Department Specific," where a provider or individual working in a specific department might have access to health information generated by that department only and no other data, even if the same data element type, similar to those data element types generated by that department, is in a given health record. For example, a given clinical lab could look at its own results in a patient chart but not those generated by other labs that are part of the historical record.

8.7 In addition to role-based disclosure under this guide, data access, disclosure and use privileges are additionally subject to definition by type-masks and exclusions from disclosure under the following categorizations:

Problem
Procedure
Diagnosis
Diagnostic Test or Result
Race
Religion
Nationality
Citizenship
Country/Region of Data Origin
Sexual Preference
Genetic Data or Profile

8.8 These type-mask specific data element and data value exclusions from disclosure additionally cover any related or revealing data that can allow the assumption or proof of a problem, diagnosis, race, religion, nationality, citizenship, country/region of data origin, sexual preference, genetic data or profile, or a combination thereof. These type-mask specific categories are called out uniquely under this guide as they have the highest level of risk for misuse, unauthorized access, and disclosure. They also represent, along with drug, alcohol, and mental health information, the highest adverse risk for discrimination and discriminatory policies against individuals.

8.9 All data access, disclosure, and use privileges for any healthcare data will in no instance be less restrictive then the laws and professional standards of practice of the country or region of origin. This explicitly refers to the laws and professional standards of practice between two countries that have different disclosure policies regarding health information. What is legally and procedurally allowable for disclosure in one country is not disclosable to another country, or within

another country, without explicit authorization from the individual, group, or organization about whom the data is maintained. If an individual travels to another country, then new data collected on that individual under appropriate authorization while in that other country falls within the rules of access and disclosure for that other country.

8.10 Data cannot cross legal boundaries and lose or have a change in the professional practice and legal protections under which the data are or were collected without the explicit informed consent of the individual, group or organization from and about whom the data are collected, retained, or managed.

9. Data Protection Between Disclosure and Return or Destruction

9.1 Data protection from wrongful disclosure under this guide includes the entire timeframe within which the data are accessed, disclosed, evaluated, and reviewed, up to and including its return or destruction. To fulfill this requirement for data protection, rights to print, send facsimile, telefax, photocopy, copy to mechanical, optical or magnetic media, or to electronically transmit data and any occurrences of printing, facsimile, telefax, photocopy, copy to mechanical, optical, digital, synthetic, or magnetic media or electronic transmission of data shall be explicitly documented and permanently maintained for audit.

9.2 Furthermore, under this guide, all disclosed data is required to be protected during transport with a secure cover to prevent unauthorized access and wrongful disclosure.

9.3 Destruction of confidential healthcare data shall be done in a manner that continues to protect to confidentiality of the data during the timeframe from disposal to destruction. Specifically:

9.3.1 Paper shall be stored in a secure environment/container and shall be shredded or recycled under confidential and secure restrictions.

9.3.2 Non-paper medium shall be destroyed under secure and confidential restrictions. Destruction methods for non-paper medium shall ensure absolute non-recoverability (for computer disks, for example, erasure alone may not be adequate erased, unless erasure provides absolute assurance of non-recoverability).

9.3.3 Specimens and specimen containers shall be destroyed under secure and confidential restrictions, or shall be absolutely dis-identified or de-labeled prior to release for disposal or destruction, or both.

10. Data Access and Disclosure Under Healthcare Malpractice and Any Legal Disputes or Litigation Involving or Requiring the Use of Health Information as Evidence

10.1 Data access and disclosure under healthcare malpractice and any legal disputes or litigation involving or requiring the use of health information as evidence is only to individuals to whom authorization has been provided by the patient, or in case the patient is deceased their direct family or guardian. Such disclosure under healthcare malpractice and any legal disputes or litigation involving or requiring the use of health information as evidence is for the encounter or case under direct legal review and action only unless otherwise mandated by court order or local, regional, state, or federal law. Under this provision individuals, groups, or organizations cannot refuse authorization to opposing attorneys or legal representatives if their own attorneys or legal representatives are granted access.

10.2 Quality assurance and utilization data are considered non-disclosable and undiscoverable under this guide.

10.3 Rules under this guide for return or destruction, or both, of any and all confidential data accessed or disclosed explicitly apply under healthcare malpractice and any legal disputes or litigation involving or requiring the use of health information as evidence. Accessed or disclosed confidential healthcare data can be retained in healthcare malpractice cases and any legal disputes or litigation involving or requiring the use of health information as evidence only if it is explicitly and directly part of established public legal evidence, otherwise it shall be returned or destroyed. No confidential health information can be maintained in legal files without the authorization of the individual, group or organization from whom or about whom the data was collected, and for or about whom the data are retained, unless part of a specific legal case and kept as specific legal or historical records for that case. These legal or historical records, however, shall be maintained as confidential, under this guide, if they are confidential health information as defined under this guide.

11. Data Access and Disclosure For Clinical and Administrative Health Research and Public Health

11.1 Data access and disclosure under this guide for the purposes of clinical and administrative health research or public health shall be consistent with all guidelines under this guide and is allowed only under authorization of the individual, group, or organization from whom or about whom the data were collected and for or about whom the data are retained. There are only two exceptions under this provision:

11.1.1 One exception is where local, regional, state, or federal law explicitly requires specific access or disclosure for the explicit purposes of protecting public health. This exception applies only to disease, injury, or clinically relevant events where public health is placed at risk. This exception does not, and can not, apply to genetic data, race, religion, nationality, citizenship, sexual preference, political affiliation, personal habits, diet or dietary preferences, mental health, toxicology, or substance use or abuse.

11.1.2 The second exception allows for explicit and documented approval and authorization of an organization's healthcare specific institutional review board. Such approval and authorization shall come from an institutional review board meeting all ethical and professional standards for healthcare institutional review boards. The approval and authorization shall have been granted only after detailed peer-review, analysis, and approval of a written proposal for access to health information that includes a description of how confidentiality will be maintained during this approved access that is consistent with the provisions of this guide. Any authorization for access granted by an organization's institutional review board under this exception does not, however, release the organization from direct responsibility to maintain the confidentiality of accessed health information to which such access approval has

been granted. It is specifically the granting organization's direct responsibility to supervise and audit all access under this exception.

12. Access Priviledges and Disclosure of Health Information in an Emergency Treatment Event

12.1 This section provides specific guidelines for the disclosure of identifiable patient health information for emergency treatment of the identified individual. These provisions apply when an individual patient needs emergency health care, and timely access to health information concerning that patient is of critical importance. Under these emergency treatment conditions, and *only* under such conditions, regular administrative protocols for disclosure of identifiable health information may be temporarily suspended or deferred. The objective in an emergency is to quickly obtain information that may assist the healthcare provider and healthcare provider team. In addition, emergency treatment is often rendered at a site and by an organization other than where an identified individual would usually receive healthcare services.

12.2 In an emergency treatment situation a patient may be physically or mentally incapacitated and unable to provide authorization for disclosure of his or her health information, therefore healthcare providers have traditionally relied on an implied authorization for access to that patient's health information. If emergency disclosure is provided it is traditionally done in a confidential manner and is followed by a request for authorization so that it can be obtained as soon as the patient, direct family, or legal guardian is reasonably able to provide authorization. These principles and practices are maintained under this guide.

12.3 An emergency treatment event is one in which the patient needs care immediately. The event may be life-threatening. The patient is either too sick or unable to provide authorization for disclosure of previous health information. If the emergency site or the emergency treatment provider or provider team deems it potentially useful, an attempt should be made to obtain relevant health information.

12.4 The emergency site staff should contact the custodian(s) of the health information at previous treatment site(s). If a previous site is a hospital or major healthcare organization or large clinic the custodian is usually a health information manager. The health information manager, or another designated individual(s) within an organization shall be responsible either directly or through trained staff to respond to emergency requests for information. Each organization shall have a set of policies and procedures to cover the emergency access to and disclosure of health information. These policies and procedures shall be crafted to provide consistency in response to requests for emergency disclosures and to meet regulatory requirements.

12.5 A request for health information on an emergency patient can be made by telephone, facsimile, or via computer.

12.6 A request for health information on an emergency patient should contain the patient's name (correctly spelled), the patient's date of birth, the patient's address, and any other relevant identifying data to assist in a search for the correct information. The requester shall also provide his/her name, position, organization and how he/she can be contacted for verification of identity and authenticity and for transmission and receipt of requested health information. A timeframe regarding the length of time in which the information will be useful should also be provided. For example, if the custodial site stores records off site and a minimum of 2 h is required to retrieve the record, the response may be of no value. The request should also consider the most appropriate means of responding to the request. Is a return phone call appropriate? Would it best serve the emergency treatment site if the information were sent by facsimile or sent by other electronic means?

12.7 In order to responsibly disclose information the custodial site should know that the request is legitimate. If there is an ongoing working relationship between healthcare organizations in a community individuals involved in providing emergency care may be known to staff at the custodial site. In most instances it will take more than 2 min to verify that information is available on a particular individual and to begin to reply to a request for information. Therefore, the one form of verification of the legitimacy of the request is a callback procedure to the requesting emergency department. A list of emergency department phone numbers should be assembled and readily available for health information management staff in any custodial site. A similar list of legitimate and verified facsimile numbers and electronic mail or domain addressed should also be readily available.

12.8 *Phone Response*— A phone response should usually be limited to specific information that can quickly and easily provided by phone. For example, "What was the surgical procedure performed during the last hospitalization?" or "Is there a history of heart problems?" If a history was extensive then a decision could be made to transmit certain key documents by facsimile or other electronic means.

12.9 *Facsimile (fax) Response*—If the request is to send information to the treating site by facsimile, the custodial site should limit the transmission to what is needed to provide the emergency care. A cover letter shall accompany each facsimile transmission and include the following:

12.9.1 The current date and time.

12.9.2 The name, phone number and fax number of the receiving facility, and the name of the individual to receive the fax.

12.9.3 The sending facility's name, address, phone number, fax number, and the sender's name.

12.9.4 A request to send an authorization for disclosure signed by the patient if and when the patient becomes able to do so.

12.9.5 The number of pages transmitted including the cover page.

12.9.6 A statement that the information in the fax is confidential and shall not be disclosed to anyone other than the requesting individual and the emergency treatment providers and any other providers providing direct clinical care.

12.9.7 Instructions for a misdirected fax and for destruction of the fax if misdirected, or retrieved in whole or part by anyone other than the targeted site and recipient.

12.9.8 A request for confirmation that the fax was received, such as a phone call or return notice by fax.

12.10 Faxes should be encrypted during transmission whenever possible.

12.11 For the department/site initiating the request, the request should ask for the fax to be sent to a machine in the department/site or at least supervised by an individual trained in confidentiality procedures. Fax documents that contain confidential health information should be removed from the receiving fax machine as soon as possible after transmission. The individual receiving the fax should verify that all pages were received and notify the sender of any problems or that the fax was received. Faxed documents should then immediately be delivered to the clinical staff treating the patient.

12.12 If electronic means other than telephone or facsimile are used to transmit an individual's health information, all of the requirements under this section shall be applied. If information is transmitted over public channels, intranets, extranets, or the Internet, point-to-point encryption shall be utilized.

12.13 Post-emergency event authorization for disclosure shall be obtained in a timely manner. If and when a patient improves or is stabilized and is able to provide authorization, then the facility providing the emergency treatment shall obtain authorization for access and disclosure and forward it to the custodial site from whom disclosure was obtained.

12.14 When an organization or practitioner discloses information on an individual in an emergency situation, the following information should be recorded:

12.14.1 A brief description of the circumstances that required the emergency disclosure.

12.14.2 The patient's name and identification number.

12.14.3 The date and time of the request and any subsequent disclosure.

12.14.4 A description of the information requested and of the information disclosed.

12.14.5 The identity of the party receiving the information.

12.14.6 The identity of the party disclosing the information.

12.14.7 Date and time receipt requested and received.

12.14.8 This information may be recorded in a disclosure log or into a computer database designed to accept this information. Patient records may have additional sections for related material which include the disclosure requests and releases. If the patient record is not in electronic form, it may be necessary to record information in more than one location in order to clearly show the activity of disclosure with the record and to track the overall administrative disclosure activity within of a hospital or clinic or other entity.

12.15 This guide explicitly prohibits re-disclosure of health information released in an emergency event without authorization from the patient, patient family, or legal guardian to anyone other than another healthcare facility receiving the emergency case in transfer, or direct and continuing care healthcare providers.

12.16 This guide explicitly requires that all health information accessed and disclosed in an emergency treatment event, once disclosed, be treated as confidential health information and that it is subject to all other requirements under this guide, including, but not limited to, the return, continued confidential management or destruction of disclosed health information once an emergency treatment event is no longer active.

13. Keywords

13.1 access; access privileges; confidentiality; health data; health information; healthcare records

REFERENCES

(**1**) Computer-based Patient Record Institute, "Glossary of Terms Related to Information Security for Computer-based Patient Record Systems," CPRI Workgroup on Confidentiality, Privacy, and Security, July 1996.

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

(**3**) Donaldson, M. S., and Lohr, K. N., eds., "Health Data in the Information Age: Use, Disclosure, and Privacy," National Academy Press, Washington, DC, 1994.

(**4**) Public Law 104-191, "The Health Insurance Portability and Accountability Act of 1996," Section 264.

(**5**) U.S. Congress, Office of Technology Assessment, "Protecting Privacy in Computerized Medical Information," OTA-TCT-576, U.S. Government Printing Office, Washington, DC, September 1993.

(**6**) American Health Information Management Association, *Health Information Model Legislative Language*, 1993.

(**7**) JCAHO, Joint Commission on Accreditation of Healthcare Organizations, Accreditation Manual for Hospitals, 1997 ed.

(**8**) National Academy of Sciences, *For The Record, Protecting Electronic Health Information*, National Academy Press, Washington, DC 1997.

(**9**) Privacy Act of 1974, USC 552a Public Law 93-079.

(**10**) Health Care Financing Administration, "Conditions of Participation: Medical Record Services," 42 CFR, Chapter 4, 482.24.

(**11**) American Medical Association, "Code of Medical Ethics: Current Opinions, Confidentiality Statement," pp. 25–27.

(**12**) Tomes, Jonathan P. J. D., "Compliance Guide to Electronic Medical Records," Faulkner & Gray, 1997.

(**13**) Joint Commission on Accreditation of Healthcare Organizations, Accreditation Manual for Hospitals, 1997 ed.

(**14**) European Committee for Standardization, CEN/TC 251/WG6 European Prestandard, Draft, Security Categorisation and Protection for Healthcare Information Systems