Designation: E 2147 – 01

An American National Standard

Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems[1]

This standard is issued under the fixed designation E 2147; 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 specification is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1).[2]

1.2 The first purpose of this specification is to define the nature, role, and function of system access audit logs and their use in health information systems as a technical and procedural tool to help provide security oversight. In concert with organizational confidentiality and security policies and procedures, permanent audit logs can clearly identify all system application users who access patient identifiable information, record the nature of the patient information accessed, and maintain a permanent record of actions taken by the user. By providing a precise method for an organization to monitor and review who has accessed patient data, audit logs have the potential for more effective security oversight than traditional paper record environments. This specification will identify functionality needed for audit log management, the data to be recorded, and the use of audit logs as security and management tools by organizational managers.

1.3 In the absence of computerized logs, audit log principles can be implemented manually in the paper patient record environment with respect to permanently monitoring paper patient record access. Where the paper patient record and the computer-based patient record coexist in parallel, security oversight and access management should address both environments.

1.4 The second purpose of this specification is to identify principles for establishing a permanent record of disclosure of health information to external users and the data to be recorded in maintaining it. Security management of health information requires a comprehensive framework that incorporates mandates and criteria for disclosing patient health information found in federal and state laws, rules and regulations and ethical statements of professional conduct. Accountability for such a framework should be established through a set of standard principles that are applicable to all health care settings and health information systems.

1.5 Logs used to audit and oversee health information access and disclosure are the responsibility of each health care organization, data intermediary, data warehouse, clinical data repository, third party payer, agency, organization or corporation that maintains or provides, or has access to individually-identifiable data. Such logs are specified in and support policy on information access monitoring and are tied to disciplinary sanctions that satisfy legal, regulatory, accreditation and institutional mandates.

1.6 Organizations need to prescribe access requirements for aggregate data and to approve query tools that allow auditing capability, or design data repositories that limit inclusion of data that provide potential keys to identifiable data. Inferencing patient identifiable data through analysis of aggregate data that contains limited identifying data elements such as birth date, birth location, and family name, is possible using software that matches data elements across data bases. This allows a consistent approach to linking records into longitudinal cases for research purposes. Audit trails can be designed to work with applications which use these techniques if the query functions are part of a defined retrieval application but often standard query tools are not easily audited. This specification applies to the disclosure or transfer of health information (records) individually or in batches.

[1] This specification is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.25 on Healthcare Data Management, Security, Confidentiality, and Privacy.

Current edition approved Nov. 10, 2001. Published February 2002.

[2] The boldface numbers in parentheses refer to the list of references at the end of this standard.

1.7 This specification responds to the need for a standard addressing privacy and confidentiality as noted in Public Law 104–191 (2), or the Health Insurance Portability and Accountability Act of 1996 (3).

2. Referenced Documents

2.1 *ASTM Standards:*

E 1384 Guide for Content and Structure of the Electronic Health Record (EHR)[3]

E 1633 Specification for Coded Values Used in the Electronic Health Record[3]

E 1762 Guide for Electronic Authentication of Health Care Information[3]

E 1869 Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer Based Patient Records[3]

E 1902 Guide for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records[3]

E 1986 Guide for Information Access Privileges to Health Information[3]

2.2 *Other Health Informatics Standards:*

Health Level Seven (HL7) Version 2.2[4]

ANSI ASC X12 Version 3, Release 3[5]

ISO/TEC 15408

3. Terminology

3.1 *Definitions:*

3.1.1 *access*, *n*—the provision of an opportunity to approach, inspect, review, retrieve, store, communicate with, or make use of health information resources (for example, hardware, software, systems or structure) or patient identifiable data and information, or both. **(E 1869)**

3.1.2 *audit log*, *n*—a record of actions, for example, creation, queries, views, additions, deletions, and changes performed on data.

3.1.3 *audit trail*, *n*—a record of users that is documentary evidence of monitoring each operation of individuals on health information. Audit trails may be comprehensive or specific to the individual and information (4). For example, an audit trail may be a record of all actions taken by anyone on a particularly sensitive file (5).

3.1.4 *authentication*, *n*—the provision of assurance of the claimed identity of an entity, receiver or object. **(E 1762, E 1869, CPRI)**

3.1.5 *authorize*, *v*—the granting to a user the right of access to specified data and information, a program, a terminal or a process. **(E 1869)**

3.1.6 *authorization*, *n*—the mechanism for obtaining consent for the use and disclosure of health information. **(CPRI, AHIMA)**

3.1.7 *certificate*, *n*—certificate means that a Certificate Authority (CA) states a given correlation or given properties of persons or IT-systems as true. If the certificate is used to confirm that a key belongs to its owner, it is called key certificate. If the certificate is used to confirm roles (qualifications), it is called authentication certificate.

3.1.8 *confidential*, *n*—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, 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 which would be prejudicial to the individual will not occur (6). **(E 1869; CPRI)**

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

3.1.10 *database security*, *n*—refers to the ability of the system to enforce security policy governing access, creation, modification, or destruction of information. Unauthorized creation of information is an important threat.

3.1.11 *disclosure*, *n*—to access, release, transfer, or otherwise divulge health information to any internal or external user or entity other than the individual who is the subject of such information. **(E 1869)**

3.1.12 *health information*, *n*—any information, whether oral or recorded in any form or medium 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, 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, 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).

3.1.13 *information*, *n*—data to which meaning is assigned, according to context and assumed conventions. **(E 1869)**

3.1.14 *transaction log*, *n*—a record of changes to data, especially to a data base, that can be used to reconstruct the data if there is a failure after the transaction occurs, in other words, a means of ensuring data integrity and availability.

3.1.15 *user*, *n*—a person authorized to use the information contained in an information system as specified by their job function. The patient may be designated an authorized user by statute or institutional policy. A user also may refer to internal and external systems that draw data from an application.

3.1.16 *user identification (user ID)*, *n*—the combination name/number biometric assigned and maintained in security procedures for identifying and tracking individual user activity.

3.1.17 *view*—a designated configuration for data/information extracted from information system(s) and presented through a workstation.

4. Significance and Use

4.1 Data that document health services in health care organizations are business records and must be archived to a secondary but retrievable medium. Audit logs should be

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

[4] Available from HL7, Mark McDougall, Executive Director, 900 Victors Way, Suite 122, Ann Arbor, MI 48108.

[5] Available from American National Standards Institute, 11 W. 42nd St., 13th Floor, New York, NY 10036.