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.

1.7 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)**.

---

[1] This specification 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 Nov. 10, 2001. Published February 2002.

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

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 retained, at a minimum, according to the statute governing medical records in the geographic area.

4.2 The purpose of audit access and disclosure logs is to document and maintain a permanent record of all authorized and unauthorized access to and disclosure of confidential

[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.

health care information in order that health care providers, organizations, and patients and others can retrieve evidence of that access to meet multiple needs. Examples are clinical, organizational, risk management, and patient rights' needs.

4.3 Audit logs designed for system access provide a precise capability for organizations to see who has accessed patient information. Due to the significant risk in computing environments by authorized and unauthorized users, the audit log is an important management tool to monitor, access retrospectively. In addition, the access and disclosure log becomes a powerful support document for disciplinary action. Audit logs are essential components to comprehensive security programs in health care.

4.4 Organizations are accountable for managing the disclosure of health information in a way that meets legal, regulatory, accreditation and licensing requirements and growing patient expectations for accountable privacy practices. Basic audit trail procedures should be applied, manually if necessary, in paper patient record systems to the extent feasible. Security in health information systems is an essential component to making progress in building and linking patient information. Successful implementation of large scale systems, the use of networks to transmit data, growing technical capability to address security issues and concerns about the confidentiality, and security provisions of patient information drive the focus on this topic. (See Guide E 1384.)

4.5 Consumer fears about confidentiality of health information and legal initiatives underscore disclosure practices. Patients and health care providers want assurance that their information is protected. Technology exists to incorporate audit functions in health information systems. Advances in security audit expert systems can be applied to the health care industry. Emerging off-the-shelf products will be able to use audit logs to enable the detection of inappropriate use of health information. Institutions are accountable for implementing comprehensive confidentiality and security programs that combine social elements, management, and technology.

5. Audit Functions in Health Information Systems

5.1 An audit log is a record of actions (queries, views, additions, deletions, changes) performed on data by users. Actions should be recorded at the time they occur. These actions include user authentication, user or system-directed signoff, health record access to view, and receipt of patient health record content from external provider/practitioner.

5.1.1 Health record content (transformation/translation via interfaces, interface engines, gateways between heterogeneous applications) should be maintained in the "before" and "after" form. For example, laboratory reports/data translated from laboratory forwarded to clinical repository storage.

5.2 Other database tables are needed to link the items in 5.1 and 5.1.1 to satisfy inquiries and to produce useful reports. Including unique user identification, for example, number, user name, work location, and employee status (permanent, contract, temporary) provides essential user information. While the audit log is a complete entity, data may be extracted from other systems for use in the audit log application.

5.3 The following functions should be performed when auditing:

5.3.1 Audits should identify and track individual users' access, including authentication and signoff, to a specific patient's or provider's data. This function should be done in real time and captured in audit logs. In the paper patient record, at a minimum, keep a permanent charge copy of all external releases. For example, an audit can be authorized by the patient or guardian, provided by law, or granted in an emergency. This may be a computer file.

5.3.2 Record or report type of access (authentication, signoff, queries, views, additions, deletions, changes). Complete records of the type of access and all actions performed on the data should be maintained. All changes to an individual patient's or provider's computer based health information should be retrievable. Changes, additions, and deletions to a patient's health information should be reported to the guardian/custodian/steward of patient/health information/medical records.

5.3.3 Record and maintain breach access flag. Flags should notify a security administrator and the guardian/custodian/steward of patient/health information/medical records that potential breaches may be occurring or have occurred. Organizations should be able to tailor flags to meet their requirements. For example, restricted health data may be flagged in one organization, high profile individuals' (that is, celebrity, employees, VIPs, providers) data may be flagged in another.

5.3.4 Maintain user identification data. Doing so should include a user identification code, full name, and employment status and the access authorization based on role and job function that is assigned by the organization.

5.3.5 Allow cross-reference to user employment, work location, or contract status with authorized access code.

5.3.6 Allow easy retrieval. Audit log queries must be efficient to operate and provide easy, on demand reporting within a reasonable time frame.

5.3.7 Provide search capability by user and patient identification, date range, type of data accessed, type of access (queries, views, additions, deletions, change). Doing so allows the capability to query access patterns to identify exceptions and allows programs to be written to generate exception reports related to known access patterns.

5.3.8 Provide the capability for predetermined flags to generate audit summary reports by designated schedule and ad-hoc reports within a reasonable time frame.

5.3.9 Provide highly restricted access to audit log and maintain security records of the audit log itself (date/time of operation, access, and use). Organizational measures and a specific security environment for the audit log device could support the required security level.

5.3.10 Prohibit use for other reasons than to enforce security and to detect security breaches in health information systems, for example, the audits are not to be used to explore activity profiles or movement profiles of employees.

5.3.11 Support real-time search and retrieval capabilities by storing audit log data in a database or transferring the data to a database.

5.3.12 Reconstruct data resulting from access to the health record content for any given historical date/time. Document the

chronology, continuity and completeness of the health record event by event for patient or provider.

6. Principles for Health Information Disclosure Oversight in Paper and Computer based Health Information Systems

6.1 Disclosure of health information should be made only by those appropriately trained and qualified to do so. Disclosures should be consistent with the organization's policies and procedures and federal and state statutes and regulations.

6.2 Disclosures of health information pursuant to patient authorization should be documented.

6.3 Disclosure of health information pursuant to subpoena or court order should be documented in the health record.

6.4 Disclosure of information relating to alcohol and drug abuse treatment should be made pursuant to the federal regulations (42 CFR, Part 2) **(7)**. The regulations require that each disclosure must be accompanied by a notice prohibiting redisclosure. The notice states the following:

> "This information has been disclosed to you from records whose confidentiality is protected by Federal law. Federal regulations (42 CFR, Part 2) prohibit you from making any further disclosure of it without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical or other information is *not* sufficient for this purpose."

6.5 In a medical emergency, the 42 CFR, Part 2 federal regulations do permit disclosure to medical personnel to treat a condition that "poses an immediate threat to the health of the patient." Such disclosure should be documented.

6.6 A verbal disclosure under 42 CFR, Part 2 should be documented and must be accompanied or followed by the required notice prohibiting redisclosure.

7. Audit Log Content

7.1 Audit log content is determined by regulatory initiatives, accreditation standards, and principles and organizational needs. Information is needed to adequately understand and oversee access to patient identifiable data in health information systems in order to perform security oversight tasks responsibly. Logs must contain the following minimum data elements:

7.2 *Date and Time of Event*—The exact date and time of the access event and the exit event.

7.3 *Patient Identification*—Unique identification of the patient to distinguish the patient and his/her health information from all others.

7.4 *User Identification*—Unique identification of the user of the health information system.

7.5 *Access Device (optional)*—Terminal or work station or device from which the user obtained access.

7.6 *Type of Action (additions, deletions, changes, queries, print, copy)*—Specifies inquiry, any changes made (with pointer to original data state), and a delete specification (with a pointer to deleted information).

7.7 *Identification of the Patient Data that is Accessed (optional)*—Granularity should be specific enough to clearly determine if data designated by federal or state law as requiring special confidentiality protection has been accessed. Specific category of data content, such as demographics, pharmacy data, test results, and transcribed notes type, should be identified.

7.8 *Source of Access (optional unless the log is combined from multiple systems or can be indisputably inferred)*—The identification of the application through which the access occurred.

7.9 *Reason for Access (optional)*—Reason for access may be assumed according to role delineation of the users typically identifiable by the system. The information may be derived from access control mechanisms or the security privileges used to gain access to the data. When the user's role does not match the information accessed, it may trigger an audit.

7.10 If capability exists, there should be recognition that both an electronic "copy" operation and a paper "print" operation are qualitatively different from other actions. Both of these activities initiate a new audit trail, which must follow the new copy of the information.

8. Disclosure Log Content

8.1 The date, name, and address of the individual or entity to which the information is sent; description of information sent, including patient identity; reason for disclosure; and the identity of the individual handling the disclosure should be logged. For routine or basic disclosure, the following are required:

8.1.1 Date and time of disclosure.

8.1.2 Reason for disclosure.

8.1.3 Description of information disclosed.

8.1.4 Identity of person requesting access.

8.1.5 Identity and verification of the party receiving the information.

8.1.6 Identity of the party disclosing the information.

8.1.7 Verification method of requesting the party's identity.

8.2 *Legal Disclosure*—The court docket number, names of the parties, the name and location of the court where the proceeding is held, and a description of the documents provided should be provided. Details are as follows:

8.2.1 Date and time of disclosure.

8.2.2 Reason for disclosure.

8.2.3 Description of information disclosed.

8.2.4 Identity and verification of the party receiving the information.

8.2.5 Identity of the party disclosing the information.

8.2.6 Verification method of requesting the party's identity.

8.2.7 Court docket number.

8.2.8 Names of the parties.

8.2.9 Name and location of the court.

8.3 Records of disclosures for emergency purposes must be maintained according to Guide E 1986. All emergency accesses should follow standard auditing procedures. Patient's name and case number include the following information:

8.3.1 Date and time of disclosure.

8.3.2 Description of circumstances that required emergency disclosure.

8.3.3 Description of information disclosed.

8.3.4 Identity of person requesting access.

8.3.5 Identity and verification of the party receiving the information.

8.3.6 Identity of the party disclosing the information.

8.3.7 Verification method of requesting party's identity.

9. Audit Log Reports

9.1 Standard access and disclosure reports should be provided to security officers or privacy officers and designated individuals such as data custodians, data stewards, and work area managers. These reports should include but not be limited to periodic random samples of all who seek information to identify individuals who have accessed patient identifiable data.

9.2 Ad hoc reports should be available for authorized parties, such as privacy or security officers or managers.

9.3 *Variation*—Reports should be available to report access variations for individuals and for departments. This should include the capability of an authorized requester to query the application to generate a report on a unscheduled basis. This feature is called for so that prompt response can be provided for incidents that are identified as a potential security breach. Managers should be able to specify queries that arise from patient, provider, or employee complaints, or a combination thereof.

9.4 On-demand reports (requests that are made with a reasonable time frame) to providers and patients should be available to provide the record of access to confidential health information. Reports should include identification of the individual who accessed the information, date of access, and the reason for access if the reason for access is maintained.

9.5 An audit log should be able to be used to determine the following:

9.5.1 For a given patient, determine the users who viewed data on this person including their identity, the date/time of access, etc.

9.5.2 For a given user, determine which data content categories that are viewed.

9.5.3 Determine the changes that are made to this patient record (over a given time frame.)

9.5.4 If technical capability permits, determine how many copies of a specific set of data have been made and the circumstances of each copy.

9.6 Patients and providers should have access to the permanent record of disclosures of health information to external users.

10. Sanctions

10.1 Enterprise sanctions should be invoked when audit log inquiry reveals that confidentiality has been breached. Organizations must have policies and procedures regarding disciplinary actions and sanctions, which are communicated to all employees, agents, and contractors. Examples of sanctions include verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties (Guide E 1869).

10.2 In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information.

10.3 Employees, agents, and contractors must be made aware that violations may result in notification to law enforcement officials and regulatory, accreditation and licenser organizations.

REFERENCES

(**1**) The Privacy Act of 1974.
(**2**) Public Law 104–191.
(**3**) Health Insurance Portability and Accountability Act of 1996, Public Law 104–191.
(**4**) National Research Council, "For the Record-Protecting Electronic Health Information Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure," National Academy Press, Washington, DC, 1997, pp. 97–99.
(**5**) Office of Technology Assessment, "Protecting Privacy in Computerized Medical Information," OTA-TCT-576, Washington, DC, U.S. Government Printing Office, 1993.
(**6**) Computer-based Patient Record Institute, Managing Information Security Programs at Organizations Using Computer-based Patient Records, Bethesda, MD, CPRI, 1996.
(**7**) Federal Regulations Governing the Confidentiality of Substance Abuse Treatment, 42 CFR, Part 2, 1983.