Designation: E2147 – 18

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

This standard is issued under the fixed designation E2147; 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 secure audit data and logs for electronically stored health information. It specifies how to design the audit log to record all activities impacting a medical record, for example, creating a new record, entering data into a record, changing or deleting an existing record, and all additional user access data (for example, identification, location, and date and time) to patient-identifiable information maintained in computer systems. Such audit logs shall track not only data entry and modifications, but also simple access and viewing of the patient record, and whether any modifications are made during that access. This specification also includes principles for developing policies, procedures, and functions of health information logs to document all actions regarding identifiable health information for use in both manually entered (paper record) and computer systems.

1.2 The first purpose of this specification is to define the nature, purpose, and function of system access audit logs and their use in health information systems as a technical and procedural tool to help provide privacy and security oversight and produce a self-authenticating record that would, when maintained together with its audit logs, speak to and confirm its own integrity and accuracy of the medical and other data within the record. Moreover, in concert with organizational confidentiality and security policies and procedures, permanent audit logs can clearly identify all system application users who accessed and acted on patient identifiable information or both, and identify the location of the user, identify patient information accessed, and maintain a permanent record of actions taken by the user. Accomplishing the purpose of creating a trustworthy record thus requires the use of secure, automatic, computer-generated, time-stamped audit logs, which shall be used to independently record the identity of the user as well as the date, time, and location of user access, and also record all entries and actions that create, change, or delete electronic records or other patient information. Full transparency of modifications or deletions or both is mandatory. For example, record changes shall not obscure previously recorded information. Such audit data and documentation shall be retained for a period at least as long as that required for the subject paper and electronic records (together, "records"), including any time period required by evidence preservation or litigation hold requirements and applicable state or applicable federal laws pertaining to the subject records. In no event shall the audit data or medical records in hard copy or electronic format be destroyed in advance of that date prescribed by state, federal or other law or regulation, when such records may be legally destroyed; and in any case, not before ten years or, in the case of a minor child, before two years after that child's eighteenth birthday. If such records are for any reason maintained beyond this minimum requirement, then the audit logs, and the data contained therein, must be maintained as long as the records are maintained. Audit logs and healthcare information shall be provided when specifically requested by authorized healthcare providers; the patient, his personal representative, advocate, and/or designee; researchers; quality control personnel; and organizational managers or administrators or both; and other persons authorized to have access to patient records or patient-identifiable information or both in any form.

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, data entry, and data modification. Where the paper patient record and the computer-based patient record coexist in parallel, security oversight and access and data management shall address both environments with the underlying and unifying principle being transparency regarding the identity of the individual accessing or acting upon data in the record or both; the location of the individual when doing so; the time and date of such actions/entries; and clear visibility of modifications such as addenda, deletions, error corrections, and late entries.

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

[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 May 1, 2018. Published May 2018. Originally approved in 2001. Last previous edition approved in 2009 as E2147 – 01(2009) which was withdrawn March 2017 and reinstated in May 2018. DOI: 10.1520/E2147-18.

requires a comprehensive framework that incorporates both mandates and criteria for disclosing patient health information found in federal and state laws and rules and regulations and ethical statements of professional conduct. Accountability for such a framework shall be established through a set of standard principles that are applicable to all healthcare settings and health information systems.

1.5 The creation and preservation of logs used to audit and oversee health information access, actions made upon health information, and disclosure of health information are the responsibility of each healthcare provider, 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, institutional mandates, civil remedies by the patient or patient's family, and are also tied to authentication of medical data and a patient's right to obtain a complete, accurate, and transparent set of medical data and metadata (for example, audit logs).

1.6 When non-patient-specific healthcare data is sought (for example, analyses of aggregate patient data for internal or external reviews, research, or subsidies), healthcare providers and organizations need to also prescribe access requirements for such aggregate data and approve query tools that allow complete auditing capability or design data repositories that, in an active query, can limit inclusion of data in end-product aggregate form that reveals potential keys to identifiable data. In other words, endproduct aggregate-patient data shall not contain patient-identifying data or elements that, through analysis, can be used to identify individuals through inferences. For example, fields such as birth date, sex, race, or relevant demographics, and medical records numbers, or combinations thereof, are analyzed together for research purposes, using software that matches data elements across databases, thereby allowing identification of specific patients through inferencing, while preserving patient privacy. Audit data and logs can be designed to work with such applications, if the query functions are part of a defined retrieval application, but the end-product data is safeguarded to protect patient identity from release. This specification applies to the disclosure or transfer of health information (records) whether as individual files or in batches.

1.7 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

E1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records (Withdrawn 2017)[3]

E1986 Guide for Information Access Privileges to Health Information (Withdrawn 2017)[3]

2.2 *Federal Standards:*

21 CFR 11 Subpart B(e) Electronic Records

42 CFR, Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records

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.

3.1.2 *access report*—record that is a subset of the "clinical audit report" documenting the following information about each access of patient medical information: user identification (the person accessing the record); the date and time of the access (documenting both start and exit times spent on each record accessed); total duration of access; specific terminal, hardware, or location from which the access occurred; type of action (for example, copy, print, addition, modification, and deletion to the record, and when any access has been made, even when the user makes no entry or change); specific patient data accessed.

3.1.2.1 *Discussion*—The above access information is an indispensable part of the medical record because it is clinically relevant and does not appear in certain iterations of the record. All accesses shall be recorded, and the entire access record shall be provided when an access record is requested.

3.1.3 *audit data, n*—complete historical record of entries regarding patient care information automatically collected and stored by electronic health records (EHR) software or, in the case of paper records, collected and stored as a matter of industry standard and related policy and procedure.

3.1.3.1 *Discussion*—This data collection includes information entered or altered (changed or deleted) by users or processes and information concerning all users who accessed or who made, changed, or caused entries to be made into the EHR or paper medical record. In the case of EHR, this collection includes, but is not limited to, information regarding demographic data about the user and facts about access and actions taken by the user, such as date, time, location, and area of record accessed/actions taken, and the actions taken by the user or process in the record, such as creation, queries, views, additions, modifications, deletions, and so forth.

3.1.4 *authentication, n*—confirmation that a record is what it purports to be, an accurate depiction of a patient's medical care and data; the act of establishing a record, or other document, as

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] The last approved version of this historical standard is referenced on www.astm.org.

genuine, trustworthy and official; the provision of such assurance of the record's authenticity is possible only because of the audit log and data associated therewith.

3.1.4.1 *Discussion*—Authentication of the record is possible only when the associated audit data relating to the record is made an indispensable part of the medical record. **(1),**[4]

3.1.5 *authorization, n*—the mechanism for obtaining consent for the use and disclosure of health information. **((1), AHIMA)**

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

3.1.7 *certificate, n*—certificate authority (CA) states a given correlation or given properties of persons or information technology (IT) systems are true.

3.1.7.1 *Discussion*—If the certificate is used to confirm that a key belongs to its owner, it is called a key certificate. If the certificate is used to confirm roles (qualifications), it is called an authentication certificate.

3.1.8 *change, v*—to alter or edit information previously recorded in health information technology, for example, by addition or deletion.

3.1.8.1 *Discussion*—Information previously recorded shall not be changed without the retention of prior value(s). Change shall be retained as an audited event and in a viewable format that identifies the previous (and now changed) information in a patient's record (similar to how one might see changes represented by redlining in a word-processing application). How such changes are displayed or produced or both in exported electronic or printed form is a design decision left to EHR technology developers.[5]

3.1.9 *clinical audit report, n*—report created using audit data collected and stored within the EHR.

3.1.9.1 *Discussion*—Audit data can be aggregated into reports used to respond to a particular query or user's activity in the EHR. Audit data can also be aggregated into reports, commonly called "audit logs" or "audit trails" drawn from entire collections of data that have been automatically collected in the course of patient healthcare. An "access report" is one example of a report that can be generated to respond to the questions of which users have gained access to an individual's health information and what such users did during such access.

3.1.10 *confidential, adj*—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 patient—designated individuals or organizations with an approved need to know (**1**).

3.1.11 *data dictionary, n*—description in ordinary language of every table, data object, classification, or category of data, or combinations thereof, contained in the database, including the properties of each table, data object, and data classification, as well as an ordinary language description of any abbreviations or coded information recorded in the database.

3.1.11.1 *Discussion*—The data dictionary serves as a legend by which the information in the database can be queried and through which reports can be decoded. The data dictionary also explains the connections and dependencies of the tables within the database.

3.1.12 *database, n*—collection of data organized for rapid search and retrieval (**2**).

3.1.13 *database security, n*—refers to the ability of the system to enforce security policy governing access, creation, modification, or destruction of information.

3.1.13.1 *Discussion*—Unauthorized creation or destruction of information is an important and substantial threat that shall be addressed via proactive database security measures.

3.1.14 *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.

3.1.15 *health information, n*—any information relating to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payments (for example, coding and billing) for the provision of healthcare 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. This information may exist in any form or medium, which 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, such as a health oversight agency, a health information service organization or other (**2**).

3.1.16 *information, n*—data to which meaning is assigned, according to context and assumed conventions.

3.1.17 *integrity, n*—as it relates to health information, it means that the information/record is accurate, complete, and immutable in that all actions taken with respect to the record are transparent.

3.1.17.1 *Discussion*—The integrity of a record containing health information is verified as trustworthy and authentic by maintaining all audit data, which shall be enabled by default (that is, turned on), immutable (that is, unable to be changed, overwritten, or deleted), and able to record not only which action(s) occurred, but more specifically the electronic and other health information to which the action applies.

3.1.18 *privacy and security audit report*—intended to capture a forensic reconstruction of events that occurred on a patient record.

3.1.18.1 *Discussion*—One important audience of the privacy and security audit report is security officers and privacy officers who are relying on the privacy and security audit report to determine if inappropriate use or disclosure of patient data occurred. When a user performs a create, access, update,

[4] American Health Information Management Association.

[5] https://www.federalregister.gov/d/2012-20982/p-157