

DIN EN ISO 27789



ICS 35.240.80

Entwurf

Einsprüche bis 2020-05-20
Vorgesehen als Ersatz für
DIN EN ISO 27789:2013-06

**Medizinische Informatik –
Audit-Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2020);
Englische Fassung prEN ISO 27789:2020**

Health informatics –
Audit trails for electronic health records (ISO/DIS 27789:2020);
English version prEN ISO 27789:2020

Informatique de santé –
Historique d'expertise des dossiers de santé informatisés (ISO/DIS 27789:2020);
Version anglaise prEN ISO 27789:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-03-20 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an named@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Medizin (NAMed), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 59 Seiten

DIN-Normenausschuss Medizin (NAMed)

Nationales Vorwort

Dieses Dokument (prEN ISO 27789:2020) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ (Sekretariat: ANSI, USA) unter Beteiligung deutscher Experten erarbeitet und vom Technischen Komitee CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) übernommen.

Das zuständige deutsche Gremium ist der Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ im DIN-Normenausschuss Medizin (NAMed).

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von prEN ISO 27789:2020.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 12052:2017	siehe	DIN EN ISO 12052:2017-12
ISO 15489-1:2001	siehe	DIN ISO 15489-1:2002-12
ISO 21298:2017	siehe	DIN EN ISO 21298:2017-07
ISO 22600 (all parts)	siehe	DIN EN ISO 22600 (alle Teile)
ISO 27799	siehe	DIN EN ISO 27799
ISO/IEC 15408-2:2008	siehe	E DIN EN ISO/IEC 15408-2:2019-11
ISO/TS 14265:2011	siehe	DIN CEN ISO/TS 14265 (DIN SPEC 13265):2014-03

Änderungen

Gegenüber DIN EN ISO 27789:2013-06 wurden folgende Änderungen vorgenommen:

- a) Veröffentlichung in der englischen Fassung mit Bereitstellung des Anwendungsbereichs und des Abschnitts „Begriffe“ in deutscher Sprache (siehe Zusammenfassung im Nationalen Vorwort und Nationaler Anhang NA);
- b) Anpassung an die aktuellen Abschnittsbezeichnungen der ISO 27799;
- c) Anpassungen zwischen Format des Auditeintrags und dem DICOM-Format;
- d) Überarbeitung des Anhangs A „Auditszenarien“;
- e) Überarbeitung des Diagramms in Anhang B „Auditprotokolldienste“;
- f) Aktualisierung der Literaturhinweise;
- g) redaktionelle Überarbeitung der Norm.

Zusammenfassung

0.1 Allgemeines

Persönliche Gesundheitsinformationen gehören mit zu den vertraulichsten Arten von persönlichen Informationen überhaupt; die Wahrung ihrer Vertraulichkeit ist daher von entscheidender Bedeutung im Zusammenhang mit dem Schutz der Privatsphäre von behandelten Personen. Um die Konsistenz von Gesundheitsinformationen zu schützen, ist es außerdem wichtig, dass ihr gesamter Lebenszyklus vollständig auditierbar ist. Gesundheitsakten sollten so erstellt, verarbeitet und verwaltet werden, dass die Integrität und Vertraulichkeit ihres Inhalts garantiert ist und Behandelte die legitime Möglichkeit haben, die Art und Weise der Erstellung, Verwendung und Verwaltung ihrer Akte zu kontrollieren.

Um das Vertrauen in elektronische Gesundheitsakten herzustellen, sind physikalische und technische Sicherheitselemente sowie Datenintegritätselemente erforderlich. Zu den wichtigsten Sicherheitsanforderungen im Zusammenhang mit dem Schutz persönlicher Gesundheitsinformationen und der Integrität von Einträgen gehören die Anforderungen an Auditierung und Protokollierung. Diese helfen dabei sicherzustellen, dass die Zurechenbarkeit für die zu Behandelnden, die ihre Informationen eGA-Systemen (eGA = elektronische Gesundheitsakte) anvertrauen, erkennbar ist. Darüber hinaus tragen sie zum Schutz der Integrität der Einträge bei, da sie Benutzer dieser Systeme dazu anhalten, organisationsinterne Leitlinien zur Verwendung dieser Systeme einzuhalten.

Eine wirksame Auditierung und Protokollierung kann dazu beitragen, die missbräuchliche Verwendung von eGA-Systemen oder eGA-Daten aufzudecken und Organisationen und Behandelten dabei helfen, Schadenersatz gegen Benutzer einzufordern, die ihre Zugriffsrechte missbraucht haben. Für eine wirksame Auditierung müssen die Audit-Trails ausreichend Informationen enthalten, um eine Vielzahl von Szenarien abdecken zu können (siehe Anhang A).

Auditprotokolle stellen eine Ergänzung der Zugriffskontrolle dar. Sie bieten ein Mittel zur Bewertung der Einhaltung organisationsinterner Zugriffsleitlinien und können zur Verbesserung und Verfeinerung der Leitlinien selbst beitragen. Da die Leitlinien jedoch das Auftreten von unvorhergesehenen Fällen oder Notfällen berücksichtigen müssen, ist für diese Fälle die Auswertung der Auditprotokolle das wichtigste Mittel zur Sicherstellung der Zugriffskontrolle.

Dieses Dokument beschränkt sich ausschließlich auf die Protokollierung von Ereignissen. Es wird davon ausgegangen, dass Änderungen von Datenwerten in den Feldern einer elektronischen Gesundheitsakte nicht im Auditprotokoll, sondern im eGA-Datenbanksystem selbst aufgezeichnet werden. Dabei wird weiterhin davon ausgegangen, dass das eGA-System selbst sowohl den vorherigen als auch den aktualisierten Wert jedes Felds enthält. Dies entspricht den aktuellen „Point-in-time“-Datenbankarchitekturen. Für das Auditprotokoll wird angenommen, dass es außer den Bezeichnern und Verknüpfungen zum Eintrag keine persönlichen Gesundheitsinformationen enthält.

Die Einträge der elektronischen Gesundheitsakte einer einzelnen Person können in vielen unterschiedlichen Informationssystemen innerhalb einer Organisation oder auch organisations- oder sogar zuständigkeitsbereichsübergreifend liegen. Um die Übersicht über alle Aktionen zu behalten, die Einträge zu einer bestimmten behandelten Person betreffen, ist ein gemeinsamer Rahmen erforderlich. Dieses Dokument stellt einen derartigen Rahmen bereit. Für die Unterstützung domänenübergreifender Audit-Trails ist es wichtig, in diesem Rahmen auch auf die Leitlinien zu verweisen, die die Anforderungen innerhalb der jeweiligen Domäne festlegen, zum Beispiel Zugriffskontrollregeln und Aufbewahrungsfristen. Domänenleitlinien dürfen implizit durch Identifizierung der Auditprotokollquelle referenziert werden.

0.2 Vorteile der Anwendung dieses Dokuments

Die Normung von Audit-Trails im Zusammenhang mit dem Zugriff auf elektronische Gesundheitsakten erfüllt zwei Zwecke:

- Sicherstellung, dass die in einem Auditprotokoll erfassten Informationen ausreichend sind, um eine detaillierte Chronologie der Ereignisse zu rekonstruieren, die den Inhalt einer elektronischen Gesundheitsakte geformt haben;
- Sicherstellung, dass die Audit-Trails zu den Aktionen im Zusammenhang mit der Akte eines Behandelten zuverlässig nachvollzogen werden können, und zwar auch über Organisationsbereiche hinweg.

Dieses Dokument richtet sich an all jene, die für die Überwachung der Sicherheit bzw. den Schutz von Gesundheitsinformationen verantwortlich sind, sowie an Organisationen des Gesundheitswesens und sonstige Verwalter von Gesundheitsinformationen, die sich zu Audit-Trails informieren möchten, sowie an deren Sicherheitsreferenten, Berater, Auditoren, Lieferanten und Drittdienstleister.

0.3 Vergleich mit verwandten Normen zu Audit-Trails für elektronische Gesundheitsakten

Dieses Dokument stimmt mit den Anforderungen von ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*, überein, soweit sich diese auf Auditierung und Audit-Trails beziehen.

Einige Leser sind möglicherweise mit dem RFC 3881, *Security Audit and Access Accountability Message — XML Data Definitions for Healthcare Applications* [13], der Internet Engineering Task Force (IETF) vertraut. (Leser, die den IETF RFC 3881 nicht kennen, brauchen sich mit dem Dokument nicht vertraut zu machen, da sein Inhalt keine Voraussetzung für das Verständnis des vorliegenden Dokuments ist.) Der informative (Informational) RFC 3381 vom September 2004, der in der IETF-Datenbank nicht mehr als aktiv gelistet ist, war ein früher und nützlicher Versuch, den Inhalt von Auditprotokollen für das Gesundheitswesen festzulegen. Soweit möglich, stützt sich dieses Dokument im Hinblick auf den Zugriff auf die elektronische Gesundheitsakte auf die im RFC 3881 begonnene Arbeit.

0.4 Hinweis zur Terminologie

In Abschnitt 3 (Begriffe) sind einige eng miteinander verwandte Begriffe definiert. Ein *Auditprotokoll* ist eine chronologische Folge von *Auditeinträgen*; jeder Auditeintrag enthält einen Nachweis darüber, dass er unmittelbar zur Ausführung einer Prozess- oder Systemfunktion gehört und sich aus dieser ergibt. Da es sich bei eGA-Systemen um komplexe Aggregationen von Systemen und Datenbanken handeln kann, gibt es möglicherweise mehr als ein Auditprotokoll mit Informationen zu Systemereignissen, die zu einer Änderung in der elektronischen Gesundheitsakte eines Behandelten geführt haben. Zwar werden die Benennungen *Audit-Trail* und *Auditprotokoll* oft synonym verwendet, in dem vorliegenden Dokument bezeichnet *Audit-Trail* jedoch die Sammlung aller Auditeinträge aus einem oder mehreren Auditprotokollen, die sich auf einen bestimmten Behandelten, eine bestimmte elektronische Gesundheitsakte oder einen bestimmten Benutzer beziehen. Ein *Auditsystem* stellt alle Informationsverarbeitungsfunktionen bereit, die zur Führung eines oder mehrerer Auditprotokolle erforderlich sind.

0.5 Anwendungsbereich

Dieses Dokument legt einen gemeinsamen Rahmen für Audit-Trails für elektronische Gesundheitsakten (eGA), für die auslösenden Ereignisse eines Audits und für Auditdaten fest, um die Auditierbarkeit des vollständigen Satzes der persönlichen Gesundheitsinformationen über Informationssysteme und Zuständigkeitsbereiche hinweg aufrechtzuerhalten.

Sie ist anwendbar für Systeme die persönliche Gesundheitsinformationen verarbeiten, entsprechend ISO 27799, und jedes Mal, wenn ein Benutzer über das System auf diese Informationen zugreift, sie erzeugt, aktualisiert oder archiviert, einen sicheren Auditeintrag erstellen.

ANMERKUNG Bei diesem Auditeintrag handelt es sich mindestens um eine eindeutige Identifizierung des Benutzers, eine eindeutige Identifizierung des Behandelten, eine Angabe der vom Benutzer ausgeführten Funktion (Erzeugung, Zugriff auf, Aktualisierung eines Eintrags usw.) und die Aufzeichnung des Datums und der Uhrzeit, zu dem die Funktion ausgeführt wurde.

Dieses Dokument beschränkt sich auf an elektronischen Gesundheitsakten ausgeführte Aktionen, welche durch die Zugriffsleitlinien für die Domäne bestimmt werden, in der die elektronische Gesundheitsakte liegt. Sie enthalten abgesehen von Bezeichnern keinerlei persönliche Gesundheitsinformationen aus der elektronischen Gesundheitsakte. Der Auditeintrag enthält lediglich entsprechend den jeweiligen Zugriffsleitlinien definierte Verknüpfungen zu eGA-Segmenten.

Die Spezifikation und Anwendung von Auditprotokollen für die Systemverwaltung und Systemsicherheit, zum Beispiel zur Erkennung von Leistungsproblemen und Anwendungsfehlern oder zur Unterstützung einer Datenrekonstruktion, liegen außerhalb des Anwendungsbereichs dieses Dokuments. Diese Aspekte sind bereits in allgemeinen Normen zur IT-Sicherheit, zum Beispiel in ISO/IEC 15408-2 [9], behandelt.

Anhang A enthält Beispiele für verschiedene Auditszenarien. Anhang B gibt einen Überblick über Dienste für eine Auditprotokollverwaltung.

Nationaler Anhang NA (informativ)

Begriffe

Reihenfolge und Inhalt der folgenden Begriffe sind identisch mit denen in Abschnitt Begriffe der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

Zugriffskontrolle

Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

[QUELLE: ISO/IEC 27000:2009, Definition 2.1]

3.2

Zugriffsleitlinie

Definition der Pflichten, die Voraussetzung für die Gewährung des Zugriffs auf eine Ressource sind

3.3

Rechenschaftspflicht

Zurechenbarkeit

Grundsatz, demzufolge natürliche Personen, Organisationen und die Gesellschaft für ihre Handlungen verantwortlich und rechenschaftspflichtig sind

[QUELLE: ISO 15489-1:2001, Definition 3.2]

3.4

Audit

systematische und unabhängige Prüfung von Zugriffen auf, Ergänzungen zu oder Änderungen in elektronischen Gesundheitsakten, um zu ermitteln, ob die Aktivitäten und Daten in Übereinstimmung mit den organisationsinternen Standardarbeitsanweisungen und Leitlinien, der guten klinischen Praxis und den geltenden behördlichen Anforderungen ausgeführt bzw. erfasst, verwendet, aufbewahrt oder offenbart wurden

3.5

Auditarchiv

archivarische Sammlung von einem oder mehreren Auditprotokollen

3.6

Auditdaten

Daten aus einem oder mehreren Auditeinträgen

3.7

Auditprotokoll

chronologische Folge von Auditeinträgen, die jeweils Daten zu einem bestimmten Ereignis enthalten

3.8

Auditeintrag

Aufzeichnung eines spezifischen Ereignisses im Lebenszyklus einer elektronischen Gesundheitsakte

3.9

Auditsystem

Informationsverarbeitungssystem, das ein oder mehrere Auditprotokolle pflegt

3.10

Audit-Trail

Sammlung von Auditeinträgen aus einem oder mehreren Auditprotokollen, die sich auf eine bestimmte behandelte Person oder eine bestimmte elektronische Gesundheitsakte beziehen

3.11

Authentisierung

Sicherstellung, dass die von einer Einheit behauptete Eigenschaft korrekt ist

[QUELLE: ISO/IEC 27000:2009, Definition 2.5]

3.12

Autorisierung

Erteilung von Privilegien, wozu auch die Erteilung von Privilegien auf Zugriffsdaten und -funktionen gehört

Anmerkung 1 zum Begriff: Unterschiedlich zu ISO 7498-2: Erteilung von Privilegien, wozu auch die Gewährung des Zugriffs basierend auf Zugriffsprivilegien gehört

3.13

Autorität

Entität, die für die Ausgabe von Zertifikaten verantwortlich ist

3.14

Verfügbarkeit

Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein

[QUELLE: ISO/IEC 27000:2009, Definition 2.7]

3.15

Vertraulichkeit

Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

[QUELLE: ISO/IEC 27000:2009, Definition 2.9]

3.16

Koordinierte Weltzeit

UTC

Zeitskala, welche die Grundlage für die abgestimmte Funkaussendung von Normalfrequenzen und Zeitsignalen formatiert; ihr Gang stimmt mit dem der Internationalen Atomzeit überein, ist aber ihr gegenüber um eine ganze Zahl von Sekunden verschoben.

[QUELLE: IEC 60050-713:1998]

3.17

Datenintegrität

Merkmal, dass Daten nicht in unautorisierter Art und Weise verändert oder zerstört wurden

[QUELLE: ISO 7498-2:1998, Definition 3.3.21]

3.18

elektronische Gesundheitsakte

eGA

umfassender, strukturierter Satz von klinischen, demographischen, umweltbezogenen, sozialen und finanziellen Daten in elektronischer Form, der die für eine bestimmte Person erbrachte Gesundheitsdienstleistung dokumentiert

[QUELLE: ASTM E 1769:1995]

3.19

eGA-Segment

Teil einer eGA, der eine eindeutig abgegrenzte Ressource für die Zugriffsleitlinie darstellt

3.20

Identifizierung

Durchführung von Prüfungen, um einem Datenverarbeitungssystem die Erkennung von Entitäten zu ermöglichen

[QUELLE: ISO/IEC 2382-8:1998, Definition 08.04.12 (wie Identität der Authentisierung, Identität der Validierung)]

3.21

Bezeichner

Information, die vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator verwendet wird, um eine Identität zu beanspruchen

3.22

Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

[QUELLE: ISO/IEC 27000:2009, Definition 2.19]

3.23

Integrität

Eigenschaft der Absicherung der Richtigkeit und Vollständigkeit von Werten

[QUELLE: ISO/IEC 27000:2009, Definition 2.25]

3.24

Objektbezeichner

OID

weltweit eindeutiger Bezeichner für ein Informationsobjekt

Anmerkung 1 zum Begriff: Der in diesem Dokument verwendete Objektbezeichner bezieht sich auf Codesysteme. Diese Codesysteme können in Normen und Standards oder lokal durch eine Implementierung definiert sein. Der Objektbezeichner wird durch Verwendung der Notation für darstellungsunabhängige Syntax Eins (ASN.1) beschrieben, welche in ISO/IEC 8824-1 und ISO/IEC 8824-2 festgelegt ist.

3.25

Policy

Leitlinie

Satz von rechtlichen, politischen, organisationsinternen, funktionellen und technischen Pflichten im Hinblick auf Kommunikation und Kooperation

[QUELLE: ISO/TS 22600-1:2006, Definition 2.22]

3.26

Privileg

Berechtigung

Fähigkeit, die einer Entität von einer Autorität zugewiesen wird

3.27

Schriftgutverwaltung

als Führungsaufgabe wahrzunehmende effiziente und systematische Kontrolle und Durchführung der Erstellung, Entgegennahme, Aufbewahrung, Nutzung und Aussonderung von Schriftgut einschließlich der Vorgänge zur Erfassung und Aufbewahrung von Nachweisen und Informationen über Geschäftsabläufe und Transaktionen in Form von Akten

[QUELLE: ISO 15489-1, Definition 3.16]

3.28

Rolle

Satz von Zuständigkeiten und/oder Leistungen, die mit einer Aufgabe verbunden sind

3.29

Sensibilität

Maß für das Potential oder wahrgenommene Potential, das zur Schädigung oder zum Missbrauch von Daten führt

3.30

Sicherheitsrichtlinie

Aktionsplan oder -ablauf, der zum Zweck der Rechnersicherheit befolgt wird

[QUELLE: ISO/IEC 2382-8:1998, Definition 08.01.06]

3.31

behandelte Person zu Behandelnder

Person, die für den Empfang von Gesundheitsdienstleistungen vorgesehen ist, diese erhält oder bereits erhalten hat

[QUELLE: ISO 18308:2011, Definition 3.47]

3.32

Benutzer

Person, Gerät oder Programm, die/das ein eGA-System zur Datenverarbeitung oder zum Austausch von Gesundheitsinformationen verwendet

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN CEN ISO/TS 14265 (DIN SPEC 13265):2014-03; *Medizinische Informatik — Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen (ISO/TS 14265:2011); Deutsche Fassung CEN ISO/TS 14265:2013*

DIN EN ISO 12052:2017-12, *Medizinische Informatik — Digitale Bildverarbeitung und Kommunikation in der Medizin (DICOM) inklusive Workflow und Datenmanagement (ISO 12052:2017); Englische Fassung EN ISO 12052:2017*

DIN EN ISO 21298:2017-07, *Medizinische Informatik — Funktionelle und strukturelle Rollen (ISO 21298:2017, korrigierte Fassung 2017-04); Deutsche Fassung EN ISO 21298:2017*

DIN EN ISO 22600 (alle Teile), *Medizinische Informatik — Privilegienmanagement und Zugriffssteuerung*

DIN EN ISO 27799, *Medizinische Informatik — Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002*

DIN ISO 15489-1:2002-12, *Information und Dokumentation — Schriftgutverwaltung — Teil 1: Allgemeines (ISO 15489-1:2001)*

E DIN EN ISO/IEC 15408-2:2019-11, *Informationstechnik — Sicherheitstechniken — Bewertungskriterien für die IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2008); Englische Fassung prEN ISO/IEC 15408-2:2019*

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	5
5 Requirements and uses of audit data	5
5.1 Ethical and formal requirements	5
5.1.1 General	5
5.1.2 Access policy	5
5.1.3 Unambiguous identification of information system users	5
5.1.4 User roles	5
5.1.5 Secure audit records	6
5.2 Uses of audit data	6
5.2.1 Governance and supervision	6
5.2.2 Subjects of care exercising their rights	6
5.2.3 Healthcare provider's ethical or legal proof of action	6
6 Trigger events	7
6.1 General	7
6.2 Details of the event types and their contents	7
6.2.1 Access events to the personal health information	7
6.2.2 Query events to the personal health information	8
7 Audit record details	8
7.1 The general record format	8
7.2 Trigger event identification	9
7.2.1 Event ID	9
7.2.2 Event action code	10
7.2.3 Event date and time	10
7.2.4 Event outcome indicator	11
7.2.5 Event type code	11
7.3 User identification	11
7.3.1 User ID	11
7.3.2 Alternative user ID	12
7.3.3 User name	12
7.3.4 User is requestor	12
7.3.5 Role ID code	12
7.3.6 Purpose of use	13
7.4 Access point identification	15
7.4.1 Network access point type code	15
7.4.2 Network access point ID	15
7.5 Audit source identification	15
7.5.1 Overview	15
7.5.2 Audit enterprise site ID	16
7.5.3 Audit source ID	16
7.5.4 Audit source type code	16
7.6 Participant object identification	17
7.6.1 Overview	17
7.6.2 Participant object type code	18
7.6.3 Participant object type code role	18
7.6.4 Participant object data life cycle	19
7.6.5 Participant object ID type code	20
7.6.6 Participant object Permission PolicySet	20

7.6.7	Participant object sensitivity.....	21
7.6.8	Participant object ID.....	21
7.6.9	Participant object name.....	21
7.6.10	Participant object query.....	21
7.6.11	Participant object detail.....	22
8	Audit records for individual events.....	22
8.1	Access events.....	22
8.2	Query events.....	24
9	Secure management of audit data.....	26
9.1	Security considerations.....	26
9.2	Securing the availability of the audit system.....	26
9.3	Retention requirements.....	26
9.4	Securing the confidentiality and integrity of audit trails.....	26
9.5	Access to audit data.....	27
Annex A (informative) Audit scenarios.....		28
Annex B (informative) Audit log services.....		34
Bibliography.....		43

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 27789 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO/TS 27789:2013), which has been technically revised.

The main changes compared to the previous edition are as follows:

- update ISO27799 chapter titles to the latest
- match between audit record format and DICOM format
- review the content of Annex A audit scenarios
- review the chart of Annex B audit log services
- update bibliography.

Introduction

0.1 General

Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential if the privacy of subjects of care is to be maintained. In order to protect the consistency of health information, it is also important that its entire life cycle be fully auditable. Health records should be created, processed and managed in ways that guarantee the integrity and confidentiality of their contents and that support legitimate control by subjects of care in how the records are created, used and maintained.

Trust in electronic health records requires physical and technical security elements along with data integrity elements. Among the most important of all security requirements to protect personal health information and the integrity of records are those relating to audit and logging. These help to ensure accountability for subjects of care who entrust their information to electronic health record (EHR) systems. They also help to protect record integrity, as they provide a strong incentive to users of such systems to conform to organizational policies on the use of these systems.

Effective audit and logging can help to uncover misuse of EHR systems or EHR data and can help organisations and subjects of care obtain redress against users abusing their access privileges. For auditing to be effective, it is necessary that audit trails contain sufficient information to address a wide variety of circumstances (see Annex A).

Audit logs are complementary to access controls. The audit logs provide a means to assess compliance with organizational access policy and can contribute to improving and refining the policy itself. But as such a policy has to anticipate the occurrence of unforeseen or emergency cases, analysis of the audit logs becomes the primary means of ensuring access control for those cases.

This document is strictly limited in scope to logging of events. Changes to data values in fields of an EHR are presumed to be recorded in the EHR database system itself and not in the audit log. It is presumed that the EHR system itself contains both the previous and updated values of every field. This is consistent with contemporary point-in-time database architectures. The audit log itself is presumed to contain no personal health information other than identifiers and links to the record.

Electronic health records on an individual person may reside in many different information systems within and across organisational or even jurisdictional boundaries. To keep track of all actions that involve records on a particular subject of care, a common framework is a prerequisite. This document provides such a framework. To support audit trails across distinct domains it is essential to include references in this framework to the policies that specify the requirements within the domain, such as access control rules and retention periods. Domain policies may be referenced implicitly by identification of the audit log source.

0.2 Benefits of using this document

Standardization of audit trails on access to electronic health records aims at two goals:

- ensuring that information captured in an audit log is sufficient to clearly reconstruct a detailed chronology of the events that have shaped the content of an electronic health record, and
- ensuring that an audit trail of actions relating to a subject of care's record can be reliably followed, even across organizational domains.

This document is intended for those responsible for overseeing health information security or privacy and for healthcare organizations and other custodians of health information seeking guidance on audit trails, together with their security advisors, consultants, auditors, vendors and third-party service providers.

0.3 Comparison with related standards on electronic health record audit trails

This document conforms to the requirements of ISO 27799, *Health informatics — Security management in health using ISO/IEC 27002*, insofar as they relate to auditing and audit trails.

Some readers may be familiar with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3881 *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*.^[13] (Readers not already familiar with IETF RFC 3881 need not refer to that document, as familiarity with it is not required to understand this document). Informational RFC 3881, dated 2004-09 and no longer listed as active in the IETF database, was an early and useful attempt at specifying the content of audit logs for healthcare. To the extent possible, this document builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR.

0.4 A note on terminology

Several closely related terms are defined in Clause 3 (Terms and definitions). An *audit log* is a chronological sequence of *audit records*; each audit record contains evidence of directly pertaining to and resulting from the execution of a process or system function. As EHR systems can be complex aggregations of systems and databases, there may be more than one audit log containing information on system events that have altered a subject of care's EHR. Although the terms *audit trail* and *audit log* are often used interchangeably, in this document the term *audit trail* refers to the collection of all audit records from one or more audit logs that refer to a specific subject of care or specific electronic health record or specific user. An *audit system* provides all the information processing functions necessary to maintain one or more audit logs.

- Entwurf -

Health informatics — Audit trails for electronic health records

1 Scope

This document specifies a common framework for audit trails for electronic health records (EHR), in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains.

It is applicable to systems processing personal health information which, complying with ISO 27799, create a secure audit record each time a user accesses, creates, updates, or archives personal health information via the system.

NOTE Such audit records at minimum uniquely identify the user, uniquely identify the subject of care, identify the function performed by the user (record creation, access, update, etc.), and record the date and time at which the function was performed.

This document covers only actions performed on the EHR, which are governed by the access policy for the domain where the electronic health record resides. It does not deal with any personal health information from the electronic health record, other than identifiers, the audit record only containing links to EHR segments as defined by the governing access policy.

It does not cover the specification and use of audit logs for system management and system security purposes, such as the detection of performance problems, application flaw, or support for a reconstruction of data, which are dealt with by general computer security standards such as ISO/IEC 15408^[9].

Annex A gives examples of audit scenarios. Annex B gives an overview of audit log services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 27799:2016, *Health informatics — Information security management in health using ISO/IEC 27002*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1

access control

means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2009, definition 2.1]

3.2

access policy

definition of the obligations for authorizing access to a resource

3.3

accountability

principle that individuals, organizations, and the community are responsible for their actions and may be required to explain them to others

[SOURCE: ISO 15489-1:2001, definition 3.2]

3.4

audit

systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).

3.5

audit archive

archival collection of one or more audit logs

3.6

audit data

data obtained from one or more audit records

3.7

audit log

chronological sequence of audit records, each of which contains data about a specific event

3.8

audit record

record of a single specific event in the life cycle of an electronic health record

3.9

audit system

information processing system that maintains one or more audit logs

3.10

audit trail

collection of audit records from one or more audit logs relating to a specific subject of care or a specific electronic health record

3.11

authentication

provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2009, definition 2.5]

3.12

authorization

granting of privileges, which includes the granting of privileges to access data and functions

Note 1 to entry: derived from ISO 7498-2: the granting of rights, which includes the granting of access based on access rights

3.13

authority

entity responsible for issuing certificates