

DIN EN ISO 27789

ICS 35.240.80

Ersatz für
DIN EN ISO 27789:2013-06**Medizinische Informatik –
Audit-Trails für elektronische Gesundheitsakten (ISO 27789:2021);
Englische Fassung EN ISO 27789:2021**

Health informatics –
Audit trails for electronic health records (ISO 27789:2021);
English version EN ISO 27789:2021

Informatique de santé –
Historique d'expertise des dossiers de santé informatisés (ISO 27789:2021);
Version anglaise EN ISO 27789:2021

Gesamtumfang 64 Seiten

DIN-Normenausschuss Medizin (NAMed)

Nationales Vorwort

Dieses Dokument (EN ISO 27789:2021) 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.

Für Deutschland hat hieran der Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ im DIN-Normenausschuss Medizin (NAMed) mitgearbeitet.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die Englische Fassung von EN ISO 27789:2021.

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

ISO 8601-1	siehe	DIN ISO 8601-1
ISO 12052	siehe	DIN EN ISO 12052
ISO 13940	siehe	DIN EN ISO 13940
ISO 21298	siehe	DIN EN ISO 21298
ISO 22600 (all parts)	siehe	DIN EN ISO 22600 (alle Teile)
ISO 27799:2016	siehe	DIN EN ISO 27799:2016-12
ISO/HL7 10781	siehe	DIN EN ISO 10781
ISO/IEC 27000:2018	siehe	DIN EN ISO/IEC 27000:2020-06
ISO/IEC 15408 (all parts)	siehe	DIN EN ISO/IEC 15408 (alle Teile)
ISO/TS 14265	siehe	DIN CEN ISO/TS 14265 (DIN SPEC 13265)

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

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

- a) Veröffentlichung in der englischen Fassung mit Bereitstellung der Einleitung, des Anwendungsbereichs und des Abschnitts „Begriffe“ in deutscher Sprache (siehe Nationaler Anhang NA);
- b) Harmonisierung zwischen Format des Auditeintrags und dem DICOM-Format;
- c) Überarbeitung des Inhalts in Anhang A;
- d) Überarbeitung des Diagramms in Anhang B;
- e) Aktualisierung der Literaturhinweise.

Frühere Ausgaben

DIN EN ISO 27789: 2013-06

Nationaler Anhang NA (informativ)

Nationale Hinweise

NA.1 Übersetzung der Einleitung

NA.1.1 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 benötigen, 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.

NA.1.2 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.

NA.1.3 Verwandte Normen zu Audit-Trails für elektronische Gesundheitsakten

Dieses Dokument stützt sich auf und steht im Einklang mit der Arbeit, die in RFC 3881 in Hinblick auf den Zugriff auf die elektronische Gesundheitsakte begonnen wurde. Dieses Dokument stützt sich ebenso auf und steht im Einklang mit dem Inhalt von ISO/TS 21089:2018.

NA.2 Übersetzung des Anwendungsbereiches

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, und jedes Mal einen sicheren Auditeintrag erstellen, wenn ein Benutzer über das System diese Informationen liest, sie erzeugt, aktualisiert oder archiviert.

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 (alle Teile) [9], behandelt.

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

NA.3 Übersetzung des Abschnitts 3 „Begriffe“

Die Benummerung der folgenden Begriffe ist identisch mit der Benummerung in der englischen Fassung.

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/TS 21089:2018 und 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 <https://www.iso.org/obp>

— IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1

Zugriffskontrolle

Mittel um sicherzustellen, dass der Zugang zu Werten aufgrund von Geschäfts- und Sicherheitsanforderungen befugt und eingeschränkt ist

[QUELLE: ISO/IEC 27000:2018, 3.1]

3.2

Zugriffsleitlinie

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

3.3

Rechenschaftspflicht

Zurechenbarkeit

Verpflichtung einer Person oder Organisation, über ihre Aktivitäten Rechenschaft abzulegen, eine Leistung oder Aufgabe zu erfüllen, die Verantwortung für diese Aktivitäten, Leistungen oder Aufgaben zu übernehmen und die Ergebnisse auf transparente Weise offenzulegen

[QUELLE: ISO/TS 21089:2018, 3.3.1]

3.4

Agent

Entität, die programmierte Aktionen ausführt, z. B. Software oder ein Gerät

[QUELLE: ISO/TS 21089:2018, 3.6.4]

3.5

Alarm

was gesendet wird, wenn der Überwachungsdienst feststellt, dass eine Reihe von Ereignissen einem Muster entspricht

3.6

Audit

unabhängige Überprüfung und Untersuchung von Aufzeichnungen und Aktivitäten, um die Angemessenheit der Systemkontrollen zu beurteilen, die Einhaltung etablierter Richtlinien und betrieblicher Verfahren sicherzustellen und um notwendige Änderungen der Kontrollen, Richtlinien oder Verfahren zu empfehlen

[QUELLE: ISO/TS 21089:2018, 3.20]

3.7

Auditarchiv

archivarische Sammlung von einem oder mehreren Auditprotokollen

3.8

Auditdaten

Daten aus einem oder mehreren Auditeinträgen

3.9

Auditprotokoll

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

3.10

Auditeintrag

Aufzeichnung eines spezifischen Ereignisses im Lebenszyklus einer elektronischen Gesundheitsakte

3.11

Auditsystem

Informationsverarbeitungssystem, das ein oder mehrere Auditprotokolle pflegt

3.12

Audit-Trail

chronologische Aufzeichnung der Systemaktivitäten, die ausreicht, um die Abfolge von Umgebungen und Aktivitäten, die eine Operation, ein Verfahren oder ein Ereignis in einer Transaktion umgeben oder zu ihr führen, von ihrem Beginn bis zu den endgültigen Ergebnissen zu rekonstruieren, zu überprüfen und zu untersuchen

[QUELLE: GCST]

3.13

Authentisierung

Sicherstellung, dass die von einer Entität behaupteten Eigenschaften richtig sind

[QUELLE: ISO/IEC 27000:2018, 3.5]

3.14

Autorisierung

Erteilung von Privilegien, wozu auch die Gewährung des Zugriffs basierend auf Zugriffsprivilegien gehört

[QUELLE: ISO/IEC 2382:2015: 2126256, modifiziert — Anmerkungen zum Begriff gelöscht]

3.15

Verfügbarkeit

Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

[QUELLE: ISO/IEC 27000:2018, 3.7]

3.16

Vertraulichkeit

Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird

[QUELLE: ISO/IEC 27000:2018, 3.10]

3.17**Koordinierte Weltzeit****UTC**

Zeitskala, welche die Grundlage für die abgestimmte Funkaussendung von Normalfrequenzen und Zeitsignalen bildet

Anmerkung 1 zum Begriff: UTC stimmt mit dem der Internationalen Atomzeit überein, ist aber ihr gegenüber um eine ganze Zahl von Sekunden verschoben.

[QUELLE: IEC 60050-713:1998, 05-20]

3.18**Datenintegrität**

Merkmal von Daten, deren Richtigkeit und Konsistenz unabhängig von vorgenommenen Änderungen erhalten bleiben

[QUELLE: ISO 2382:2015, 2126247, modifiziert — Anmerkungen zum Begriff gelöscht]

3.19**elektronische Gesundheitsakte****eGA**

Repository von (organisierten Sätzen von) Informationen über den Gesundheitszustand eines Pflegebedürftigen in computerverarbeitbarer Form

[QUELLE: ISO/TR 20514:2005, 2.11, modifiziert — Text in Anführungszeichen hinzugefügt]

3.20**elektronische Gesundheitsakte-Segment****eGA-Segment**

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

3.21**Identifizierung**

Prozess des Erkennens der Attribute, die das Objekt identifizieren

[QUELLE: ISO 16678:2014, 2.1.7]

3.22**Bezeichner**

ein oder mehrere Zeichen, die verwendet werden, um ein Datenelement zu identifizieren oder zu benennen und möglicherweise um bestimmte Eigenschaften dieses Datenelements anzugeben

[QUELLE: ISO/IEC 2382:2015, 2121623]

3.23**Informationssicherheit**

Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen^{N1}

[QUELLE: ISO/IEC 27000:2018, 3.28]

^{N1} Nationale Fußnote: Die Anmerkung 1 zum Begriff wurde weggelassen. In der englischen Fassung wurde dies nicht explizit erwähnt.

3.24

Integrität

Eigenschaft der Richtigkeit und Vollständigkeit

[QUELLE: ISO/IEC 27000:2018, 3.36]

3.25

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.

3.26

Policy

Leitlinie

Satz von Regeln für einen bestimmten Zweck

Anmerkung 1 zum Begriff: Eine Regel kann als Verpflichtung, Autorisierung, Erlaubnis oder Verbot ausgedrückt werden.

[QUELLE: ISO 19101-2:2018, modifiziert — Anmerkung 1 zum Begriff hinzugefügt]

3.27

Privileg

Berechtigung

Fähigkeit, die einer Entität von einer Autorität zugewiesen wird

3.28

Aufzeichnungsverwaltung

Bereich des Managements, der für die Kontrolle der Erstellung, des Erhalts, der Pflege, der Verwendung und der Verfügung von Aufzeichnungen verantwortlich ist, einschließlich der Prozesse zur Erfassung und Pflege von Nachweisen und Informationen über Geschäftsaktivitäten und Transaktionen in Form von Aufzeichnungen

[QUELLE: ISO 15489-1:2016, 3.15, modifiziert]

3.29

Rolle

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

3.30

Sicherheitsrichtlinie

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

[QUELLE: ISO/IEC 2382:2015, 2126246, modifiziert — Anmerkungen zum Begriff gelöscht]

3.31

Sensibilität

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

3.32

behandelte Person zu Behandelnder

Person oder definierte Personengruppen, die Gesundheitsleistungen beziehen oder als anspruchsberechtigt gemeldet sind oder Gesundheitsleistungen erhalten haben

Anmerkung 1 zum Begriff: Zum Beispiel ein Patient, Klient, Kunde oder Mitglied eines Gesundheitsplans.

[QUELLE: ISO/TS 17975:2015, modifiziert — Anmerkung zum Begriff hinzugefügt]

3.33

Benutzer

Person oder andere Entität, die von einem Anbieter autorisiert wurde, einige oder alle Dienste des Anbieters zu nutzen

Anmerkung 1 zum Begriff: Auch ein Mensch, der das System verwendet, um Anfragen an Objekte auszugeben, um sie dazu zu bringen, Funktionen in dem System in seinem/ihrer Namen auszuführen.

[SOURCE: COACH; OMG]

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN CEN ISO/TS 14265 (DIN SPEC 13265), *Medizinische Informatik — Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen*

DIN EN ISO 10781, *Medizinische Informatik — HL 7 Funktionales Modell für ein elektronisches Gesundheitssystem (EHRS FM), Ausgabe 2*

DIN EN ISO 12052, *Medizinische Informatik — Digitale Bildverarbeitung und Kommunikation in der Medizin (DICOM) inklusive Workflow und Datenmanagement*

DIN EN ISO 13940, *Medizinische Informatik — Begriffssystem zur Unterstützung der Kontinuität der Versorgung*

DIN EN ISO 21298, *Medizinische Informatik — Funktionelle und strukturelle Rollen*

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

DIN EN ISO 27799:2016-12, *Medizinische Informatik — Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2016); Englische Fassung EN ISO 27799:2016*

DIN EN ISO/IEC 15408 (alle Teile), *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit*

DIN EN ISO/IEC 27000:2020-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*

DIN ISO 8601-1, *Datum und Uhrzeit — Darstellung für den Informationsaustausch — Teil 1: Grundlegende Regeln*

English Version

Health informatics -
Audit trails for electronic health records
(ISO 27789:2021)

Informatique de santé -
Historique d'expertise des dossiers de santé
informatisés (ISO 27789:2021)

Medizinische Informatik -
Audit-Trails für elektronische Gesundheitsakten
(ISO 27789:2021)

This European Standard was approved by CEN on 15 August 2021.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO 27789:2021) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2022, and conflicting national standards shall be withdrawn at the latest by April 2022.

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

This document supersedes EN ISO 27789:2013.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 27789:2021 has been approved by CEN as EN ISO 27789:2021 without any modification.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 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	6
5.1.4 User roles	6
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	7
5.2.3 Evidence and retention requirements	7
6 Trigger events	7
6.1 General	7
6.2 Details of the event types and their contents	8
6.2.1 Access events to the personal health information	8
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	10
7.2.1 Event ID	10
7.2.2 Event action code	11
7.2.3 Event date and time	11
7.2.4 Event outcome indicator	12
7.2.5 Event type code	12
7.3 User identification	12
7.3.1 User ID	12
7.3.2 Alternative user ID	13
7.3.3 User name	13
7.3.4 User is requestor	13
7.3.5 Role ID code	13
7.3.6 Purpose of use	14
7.4 Access point identification	15
7.4.1 Network access point type code	15
7.4.2 Network access point ID	16
7.5 Audit source identification	16
7.5.1 Overview	16
7.5.2 Audit enterprise site ID	17
7.5.3 Audit source ID	17
7.5.4 Audit source type code	17
7.6 Participant object identification	18
7.6.1 Overview	18
7.6.2 Participant object type code	19
7.6.3 Participant object type code role	19
7.6.4 Participant object data life cycle and record entry lifecycle events	20
7.6.5 Participant object ID type code	22
7.6.6 Participant object Permission PolicySet	22

7.6.7	Participant object sensitivity.....	23
7.6.8	Participant object ID.....	24
7.6.9	Participant object name.....	24
7.6.10	Participant object query.....	24
7.6.11	Participant object detail, Participant object description.....	24
8	Audit records for individual events.....	25
8.1	Access events.....	25
8.2	Query events.....	26
9	Secure management of audit data.....	28
9.1	Security considerations.....	28
9.2	Securing the availability of the audit system.....	28
9.3	Retention requirements.....	29
9.4	Securing the confidentiality and integrity of audit trails.....	29
9.5	Access to audit data.....	29
	Annex A (informative) Audit scenarios.....	30
	Annex B (informative) Audit log services.....	36
	Bibliography.....	45

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

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

The main changes are as follows:

- harmonization between audit record format and DICOM format;
- review of the content in Annex A;
- review of the chart in Annex B;
- bibliography update.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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 to maintain the privacy of subjects of care. 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 conformity with organizational access policy and can contribute to improving and refining the policy itself. But as such a policy needs 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 can 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;
- 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 Related standards on electronic health record audit trails

This document builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR. This document also builds upon and is consistent with the content in ISO/TS 21089:2018.

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 that create a secure audit record each time a user reads, creates, updates, or archives personal health information via the system.

NOTE Such audit records at a minimum uniquely identify the user, uniquely identify the subject of care, identify the function performed by the user (record creation, read, 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 (all parts)^[9].

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*

ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

ISO/TS 21089:2018, *Health informatics — Trusted end-to-end information flows*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 21089:2018 and the following terms and definitions apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://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 27000:2018, 3.1]

3.2
access policy
definition of the obligations for authorizing access to a resource

3.3
accountability
obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner

[SOURCE: ISO/TS 21089:2018, 3.3.1]

3.4
agent
entity that takes programmed actions, such as software or a device

[SOURCE: ISO/TS 21089:2018, 3.6.4]

3.5
alert
what is sent when the monitor service notices that a series of events matches a pattern

3.6
audit
independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures

[SOURCE: ISO/TS 21089:2018, 3.20]

3.7
audit archive
archival collection of one or more audit logs

3.8
audit data
data obtained from one or more audit records

3.9
audit log
chronological sequence of audit records, each of which contains data about a specific event

3.10
audit record
record of a single specific event in the life cycle of an electronic health record

3.11
audit system
information processing system that maintains one or more audit logs