

DIN EN ISO 27789

ICS 35.240.80

**Medizinische Informatik –
Audit-Trails für elektronische Gesundheitsakten (ISO 27789:2013);
Deutsche Fassung EN ISO 27789:2013**

Health informatics –
Audit trails for electronic health records (ISO 27789:2013);
German version EN ISO 27789:2013

Informatique de santé –
Historique d'expertise des dossiers de santé informatisés (ISO 27789:2013);
Version allemande EN ISO 27789:2013

Gesamtumfang 58 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (EN ISO 27789:2013) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ erarbeitet und wird parallel im CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) abgestimmt. Der Fachbereich 7 „Medizinische Informatik“ und insbesondere die Mitarbeiter des Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ im Normenausschusses Medizin (NAMed) im DIN haben an der Erarbeitung mitgewirkt.

Für die in den Normativen Verweisungen zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 8601:2004	siehe	DIN ISO 8601:2006-09
ISO 27799:2008	siehe	DIN EN ISO 27799:2008-10

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO 8601:2006-09, *Datenelemente und Austauschformate — Informationsaustausch — Darstellung von Datum und Uhrzeit (ISO 8601:2004)*

DIN EN ISO 27799:2008-10, *Medizinische Informatik — Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2013); Deutsche Fassung EN ISO 27799:2008*

Deutsche Fassung

Medizinische Informatik —
Audit-Trails für elektronische Gesundheitsakten
(ISO 27789:2013)

Health informatics —
Audit trails for electronic health records
(ISO 27789:2013)

Informatique de santé —
Historique d'expertise des dossiers de santé informatisés
(ISO 27789:2013)

Diese Europäische Norm wurde vom CEN am 16. Februar 2013 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Symbole und Abkürzungen	10
5 Anforderungen an und Verwendung von Auditdaten	10
5.1 Ethische und formale Anforderungen	10
5.2 Verwendung von Auditdaten	11
6 Auslösende Ereignisse	12
6.1 Allgemeines	12
6.2 Einzelheiten zu den Ereignistypen und deren Inhalten	13
7 Einzelheiten zum Auditeintrag	14
7.1 Allgemeines Eintragsformat	14
7.2 Identifizierung von auslösenden Ereignissen	15
7.3 Benutzeridentifizierung	18
7.4 Identifizierung des Zugriffspunkts	22
7.5 Identifizierung der Auditquelle	23
7.6 Identifizierung des Teilnehmerobjekts	25
8 Auditeinträge für einzelne Ereignisse	31
8.1 Zugriffereignisse	31
8.2 Abfrageereignisse	34
9 Sichere Verwaltung von Auditdaten	36
9.1 Überlegungen zur Sicherheit	36
9.2 Sichern der Verfügbarkeit des Auditsystems	36
9.3 Anforderungen an die Aufbewahrung	36
9.4 Sicherung der Vertraulichkeit und Integrität von Audit-Trails	37
9.5 Zugriff auf Auditdaten	37
Anhang A (informativ) Auditszenarien	38
Anhang B (informativ) Auditprotokolldienste	46
Literaturhinweise	56

Vorwort

Dieses Dokument (EN ISO 27789:2013) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2013, und etwaige entgegenstehende nationale Normen müssen bis September 2013 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 27789:2013 wurde vom CEN als EN ISO 27789:2013 ohne irgendeine Abänderung genehmigt.

Einleitung

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.

Die vorliegende Norm 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 Bezeichnungen 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. Diese Norm 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 dieser Norm

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.

Diese Norm 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

Diese Norm stimmt mit den Anforderungen von ISO 27799:2008 überein, soweit sich diese auf Auditierung und Audit-Trails beziehen.

Einige Leser sind möglicherweise mit dem RFC 3881 [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 der vorliegenden ISO-Norm 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 diese ISO-Norm 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 der vorliegenden Norm 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.

1 Anwendungsbereich

Diese Internationale Norm 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.

Diese Internationale Norm 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.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 8601:2004, *Data elements and interchange formats - Information interchange - Representation of dates and times*

ISO 27799:2008, *Health informatics — Security management in health using ISO/IEC 27002*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1
Zugriffskontrolle
Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

[ISO/IEC 27000:2012, 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

[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

[ISO/IEC 27000:2012, Definition 2.8]

3.12

Autorisierung

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

ANMERKUNG 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

[ISO/IEC 27000:2012, Definition 2.10]

3.15

Vertraulichkeit

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

[ISO/IEC 27000:2012, Definition 2.13]

3.16

Koordinierte Weltzeit

UTC

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

[IEC 60050-713:1998]

3.17

Datenintegrität

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

[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

[ASTM E1769:1995]

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

[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

[ISO/IEC 27000:2012, Definition 2.30]

3.23

Integrität

Eigenschaft der Absicherung der Richtigkeit und Vollständigkeit von Werten

[ISO/IEC 27000:2012, Definition 2.36]

3.24

Objektbezeichner

OID

Weltweit, eindeutiger Bezeichner für ein Informationsobjekt

Anmerkung 1 zum Begriff: Der in dieser Internationalen Norm 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

[ISO/TS 22600]

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

[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 Rechtersicherheit befolgt wird

[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

[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

4 Symbole und Abkürzungen

eGA	elektronische Gesundheitsakte
HL7	Health Level Seven International
OID	Objektbezeichner
UTC	Koordinierte Weltzeit

5 Anforderungen an und Verwendung von Auditdaten

5.1 Ethische und formale Anforderungen

5.1.1 Allgemeines

Gesundheitsdienstleister müssen ihrer berufsethischen Verantwortung nachkommen. Diese umfasst unter anderem den Schutz der persönlichen Daten der behandelten Personen und die Dokumentation der Befunde und der im Rahmen der Erbringung der Gesundheitsdienstleistung ausgeführten Tätigkeiten. Die Beschränkung des Zugangs zu Gesundheitsakten und die Sicherstellung ihrer angemessenen Verwendung sind wesentliche Voraussetzungen im Gesundheitswesen, die in vielen Zuständigkeitsbereichen gesetzlich geregelt sind.

Sichere Audit-Trails zum Zugriff auf elektronische Gesundheitsakten können die Einhaltung berufsethischer Prinzipien, organisationsinterner Leitlinien und von Gesetzen unterstützen, sie reichen allein jedoch nicht aus, um die Vollständigkeit einer elektronischen Gesundheitsakte zu beurteilen.

5.1.2 Zugriffsleitlinie

Eine für die Führung eines Auditprotokolls verantwortliche Organisation muss die Zugriffsleitlinie angeben, der alle protokollierten Zugriffe unterliegen.

Die Zugriffsleitlinie muss in Übereinstimmung mit ISO 27799:2008, 7.8.1.2, Leitlinie für Zugriffssteuerung, sein.

ANMERKUNG 1 Es wird angenommen, dass die Zugriffsleitlinie eine eGA-Segmentstruktur definiert.

ANMERKUNG 2 Im Auditeintrag wird die Zugriffsleitlinie durch die Auditprotokollquelle angegeben.

Eine Anleitung für die Spezifizierung und Implementierung einer Zugriffsleitlinie kann man der ISO/TS 26000 [6] entnehmen. Ein Feld "Teilnehmerobjektzulassung Leitliniensatz (en: Participant object Permission PolicySet)" ist in 7.6.6 festgelegt, um das Referenzieren der aktuellen Leitlinien im Auditprotokoll zu unterstützen.

5.1.3 Eindeutige Identifikation der Benutzer von Informationssystemen

Die Audit-Trails müssen ausreichend Daten zur Verfügung stellen, um alle autorisierten Benutzer von Gesundheitssystemen eindeutig identifizieren zu können. Die Benutzer des Informationssystems können Personen, aber auch andere Entitäten sein.

Die Audit-Trails müssen ausreichend Daten zur Verfügung stellen, um feststellen zu können, welche autorisierten Benutzer und externen Systeme auf die Daten einer Gesundheitsakte zugegriffen haben bzw. an welche autorisierten Benutzer und externen Systeme derartige Daten vom System gesendet wurden.

5.1.4 Benutzerrollen

Der Audit-Trail muss die Rolle des Benutzers zeigen, der die aufgezeichnete Aktion an der persönlichen Gesundheitsinformation ausgeführt hat.

Informationssysteme, die persönliche Gesundheitsinformationen verarbeiten, sollten einen rollenbasierten Zugriff unterstützen, der jeden Benutzer einer oder mehreren Rollen und jede Rolle einer oder mehreren Systemfunktionen zuweisen kann, wie es in ISO 27799:2008, 7.8.2.2, Privilegienmanagement, gefordert wird.

Funktionelle und strukturelle Rollen sind in ISO/TS 21298 [4] dokumentiert. Zusätzliche Anleitungen zum Privilegienmanagement im Gesundheitswesen sind in ISO/TS 22600 (alle Teile) [6], angegeben.

5.1.5 Sichere Auditeinträge

Sichere Auditeinträge müssen jedes Mal, wenn auf persönliche Gesundheitsinformationen zugegriffen wird bzw. diese erzeugt, aktualisiert oder archiviert werden, erstellt werden, entsprechend ISO 27799:2008, 7.7.10.2, Auditprotokollierung. Die Auditeinträge müssen mit Hilfe einer sicheren Schriftgutverwaltung gepflegt werden.

5.2 Verwendung von Auditdaten

5.2.1 Lenkung und Überwachung

Die Audit-Trails müssen Daten zur Verfügung stellen, um den zuständigen Autoritäten die Bewertung der Einhaltung der organisationsinternen Leitlinien und die Beurteilung der Wirksamkeit dieser Leitlinien zu ermöglichen.

Dies umfasst:

- das Erkennen eines unberechtigten Zugriffs auf Gesundheitsakten;
- die Beurteilung des Notfallzugriffs;
- das Erkennen eines Missbrauchs von Berechtigungen

sowie die Unterstützung der

- Dokumentation eines domänenübergreifenden Zugriffs und
- der Beurteilung der Zugriffsleitlinien.

ANMERKUNG Eine vollständige Bewertung der Einhaltung der organisatorischen Leitlinien kann zusätzlich Daten benötigen, welche nicht im Auditeintrag enthalten sind, wie Benutzerinformationen, Zulassungstabellen oder Einträge über physikalische Eintritte in gesicherte Räume. Siehe Anhang B für Auditprotokolldienste.

Die Audit-Trails müssen ausreichend Daten zur Verfügung stellen, um alle Zugriffe ermitteln zu können, die ein bestimmter Benutzer in einem festgelegten Zeitraum auf die Einträge zu einer behandelten Person vorgenommen hat.

Die Audit-Trails müssen ausreichend Daten zur Verfügung stellen, um alle in einem festgelegten Zeitraum erfolgten Zugriffe auf die Einträge zu einer behandelten Person ermitteln zu können, bei denen ein erhöhtes Risiko einer Datenschutzverletzung besteht und die als Einträge mit einem derartigen Risiko gekennzeichnet sind.

5.2.2 Wahrnehmung von Rechten durch die behandelten Personen

Die Audit-Trails müssen ausreichend Daten zur Verfügung stellen, um Behandelten Folgendes zu ermöglichen:

- Feststellen, welche autorisierten Benutzer zu welchem Zeitpunkt auf die Gesundheitsakte des/der Behandelten zugegriffen haben;
- Feststellen, wer für den Inhalt des Eintrags verantwortlich ist;
- Ermitteln, ob die Vorgaben des Behandelten im Hinblick auf seine Zustimmung zum Zugriff auf seine Daten bzw. deren Offenbarung eingehalten wurden und
- Ermitteln des Notfallzugriffs (sofern zutreffend), der von einem Benutzer in Bezug auf die Akte des Behandelten gewährt wurde, einschließlich der Identifizierung des Benutzers, des Zeitpunkts des Zugriffs und des Ortes, von dem aus der Zugriff erfolgte.

5.2.3 Ethischer oder rechtlicher Aktionsnachweis von Gesundheitsdienstleistern

Die Audit-Trails müssen ausreichend Daten bereitstellen, um den Gesundheitsdienstleistern einen dokumentierten Nachweis darüber zu bieten, welche Informationen angesehen und welche Aktionen wann und von wem ausgeführt wurden (Erzeugen, Nachschlagen, Lesen, Korrigieren, Aktualisieren, Extrahieren, Ausgeben, Archivieren usw.).

Die Aufbewahrungsdauer der Auditeinträge sollte den im jeweiligen Zuständigkeitsbereich geltenden rechtlichen Vorgaben zur Zurechenbarkeit entsprechen.

Siehe auch HL7 EHR Records Management & Evidentiary Support (RM-ES).

6 Auslösende Ereignisse

6.1 Allgemeines

Die Auditereignisse (auslösende Ereignisse), die das Auditsystem zur Erstellung von Auditeinträgen veranlassen, werden entsprechend der Bemessung und dem Zweck sowie dem Inhalt der Datenschutz- und Sicherheitsleitlinien jedes Gesundheitsinformationssystems definiert. Da der Anwendungsbereich dieser Norm auf den Zugriff auf persönliche Gesundheitsinformationen beschränkt ist, sind hier nur zugriffsbezogene auslösende Ereignisse festgelegt.

Für die Erstellung von Auditeinträgen, die die Anforderungen von Abschnitt 5 (Anforderungen an und Verwendung von Auditdaten) erfüllen, d. h. „wann“, „wer“, „wessen“, sind folgende zwei Ereignistypen obligatorisch:

- a) Zugriffereignisse auf persönliche Gesundheitsinformationen;
- b) Abfrageereignisse zu persönlichen Gesundheitsinformationen.

Beispiele für Ereignisse, die außerhalb des Anwendungsbereichs liegen:

- Start- und Stoppereignisse des Anwendungsprogramms;
- Authentisierungsereignisse, die die Benutzerauthentisierung einschließen;
- Eingabe- und Ausgabeereignisse in die/aus der externen Umgebung;
- Zugriffereignisse auf andere Informationen als persönliche Gesundheitsinformationen;
- Sicherheitswarnereignisse im Zusammenhang mit den Anwendungsprogrammen;
- Zugriffereignisse auf das in den Anwendungsprogrammen aufbewahrte Auditprotokoll;
- vom Betriebssystem, der Middleware usw. generierte Ereignisse;
- durch Verwendung von Systemprogrammen generierte Zugriffereignisse;
- Verbindungs-/Trennungereignisse zwischen Geräten und Netzwerk;
- Start-/Stoppereignisse der Schutzsysteme, zum Beispiel Virenschutzsysteme;
- Softwareaktualisierungereignisse, die eine Softwaremodifikation oder Patches umfassen.

6.2 Einzelheiten zu den Ereignistypen und deren Inhalten

6.2.1 Zugriffereignisse auf persönliche Gesundheitsinformationen

In dieser Norm wird der Zugriff auf die persönlichen Gesundheitsinformationen als das Auditereignis betrachtet. „Zugriff“ bedeutet in diesem Fall das Erzeugen, Lesen, Aktualisieren und Löschen von Daten. Beim Inhalt des Auditprotokolls handelt es sich um die Zugriffsinformationen „wann“, „wer“ und „Zugriff auf wessen“ zu schützende Daten. Siehe Tabelle 1.

Tabelle 1 — Zugriffereignisse

Ereignis	Inhalt
Zugriffereignisse auf die persönliche Gesundheitsinformation	Wann Wer Zugriff auf wessen

6.2.2 Abfrageereignisse zu den persönlichen Gesundheitsinformationen

Die Abfrage eine eGA-Datenbank zur Gewinnung persönlicher Gesundheitsinformationen gilt als ein auditierbares Ereignis. Dabei ist die Abfrageaktion selbst das Abfrageereignis, während die sich aus der Abfrage ergebende Verweisung auf die persönliche Gesundheitsinformation das Zugriffereignis darstellt. Beim Inhalt des Auditeintrags handelt es sich um die Abfrageinformationen „wann“, „wer“ und „welche Abfragebedingung“. Siehe Tabelle 2.

Tabelle 2 — Abfrageergebnisse

Ereignis	Inhalt
Abfrageereignisse zu der persönlichen Gesundheitsinformation	Wann
	Wer
	Welche Abfragebedingung

7 Einzelheiten zum Auditeintrag

7.1 Allgemeines Eintragsformat

Tabelle 3 beschreibt das allgemeine Format der Auditeinträge. Zum Eintragsinhalt der einzelnen Ereignisse siehe Abschnitt 8. Das Eintragsformat ist in Übereinstimmung mit RFC 3881 [13] und DICOM [11] definiert, mit den zusätzlichen optionalen Feldern "Verwendungszweck (en: PurposeOfUse)" und "Teilnehmerobjekt Leitliniensatz (en: ParticipantObjectPolicySet)".

Tabelle 3 — Allgemeines Format der Auditeinträge

Typ	Feldname	Optionalität	Beschreibung	Weitere Informationen
Ereignis-bezogen (1)	EventID	M	ID des auditierten Ereignisses	siehe 7.2
	EventActionCode	M	Art der während des auditierten Ereignisses durchgeführten Aktion	
	EventDateTime	M	Datum/Uhrzeit des Auftretens des auditierten Ereignisses	
	EventOutcomeIndicator	U	Erfolg oder Misserfolg des Ereignisses	
	EventTypeCode	U	Ereigniskategorie	
Benutzer-bezogen (1..2)	UserID	M	ID der Person oder des Prozesses	siehe 7.3
	AlternateUserID	U	alternative ID des Benutzers oder Prozesses	
	UserName	U	Benutzer- oder Prozessname	
	UserIsRequestor	U	Indikator dafür, dass der Benutzer der Anfragende ist/nicht der Anfragende ist	
	RoleIDCode	U	Spezifikation der Rolle, die der Benutzer bei der Ausführung des Ereignisses innehat	
	PurposeOfUse	U	Code für den Verwendungszweck des Datenzugriffs	
	NetworkAccessPointTypeCode	U	Art des Netzwerkzugriffspunkts	siehe 7.4
	NetworkAccessPointID	U	ID des Netzwerkzugriffspunkts	

Tabelle 3 (fortgesetzt)

Typ	Feldname	Optionalität	Beschreibung	Weitere Informationen
Audit-system-bezogen (1)	AuditEnterpriseSiteID	U	Standort-ID des Auditunternehmens	siehe 7.5
	AuditSourceID	M	eindeutige ID der Auditquelle	
	AuditSourceTypeCode	U	Typcode der Auditquelle	
Teilnehmer-objekt-bezogen (0..N)	ParticipantObjectTypeCode	M	Code des Teilnehmerobjekttyps	siehe 7.6
	ParticipantObjectTypeCodeRole	M	Objekttypcode der Rolle	
	ParticipantObjectDataLifeCycle	U	Bezeichner für die Lebenszyklusphase der Daten des Teilnehmerobjekts	
	ParticipantObjectIDTypeCode	M	Typcode der Teilnehmerobjekt-ID	
	ParticipantObjectPolicySet	U	Leitliniensatz für die Zulassung für Teilnehmerobjekt-ID	
	ParticipantObjectSensitivity	U	durch die Leitlinie definierte Sensibilität der ParticipantObjectID (Teilnehmerobjekt-ID)	
	ParticipantObjectID	M	identifiziert eine bestimmte Instanz des Teilnehmerobjekts	
	ParticipantObjectName	U	Objektname des Teilnehmers, zum Beispiel der Name einer Person	
	ParticipantObjectQuery	M/U	Inhalt der Abfrage für das Teilnehmerobjekt	
	ParticipantObjectDetail	U	Einzelheiten zum Teilnehmerobjekt	
Multiplizität:		Optionalität:		
(1)		M	obligatorisch	
(0..1)	0 oder 1 existiert	MC	bedingt obligatorisch	
(1..2)	1 oder 2 existiert (existieren)	U	optional	
(0..N)	0 bis N existiert (existieren)	M/U	obligatorisch oder optional in Bezug auf Ereignisse	

7.2 Identifizierung von auslösenden Ereignissen

7.2.1 Ereignis-ID (en: Event ID)

Beschreibung: Eindeutiger Bezeichner eines bestimmten auditierten Ereignisses, z. B. eines Menüpunkts, eines Programms, einer Regel, einer Leitlinie (Policy), eines Funktionscodes, eines Anwendungsnamens oder einer URL (en: uniform resource locator). Die Ereignis-ID identifiziert die ausgeführte Funktion.

Optionalität: Obligatorisch.

Format/Werte: Kodierte Werte, definiert entweder durch die Systemimplementierer oder als Verweisung auf ein Normvokabular. Das „code“-Attribut muss eindeutig sein und darf nur einmal vorkommen, zumindest innerhalb der ID der Auditquelle (siehe 7.5). Beispiele für Ereignis-IDs sind Programmname, Methodenname oder Funktionsname.

ANMERKUNG Die Kodierung ist nach IHE ITI TF-1 und TF-2 [12] und ISO 12052 [1] sowie DICOM Supplement 95 [11] modelliert.

Für implementierungsdefinierte kodierte Werte oder Verweisungen auf Normen definiert das XML-Schema in RFC 3881 die in Tabelle 4 gezeigten optionalen Attribute.

Tabelle 4 — Attribute bezogen auf die Ereignis-ID

Attribut	Wert
CodeSystem	OID-Referenz
CodeSystemName	Name des Kodierungssystems; für lokal definierte Codevorräte wird eine Wertfestlegung dringend empfohlen
CodeValue	der spezifische Code innerhalb des Kodierungssystems
DisplayName	der in Anzeigen und Berichten zu verwendende Wert
OriginalText	Eingangswert, der in den Code übersetzt wurde

Um die Forderung einer eindeutigen Ereignisidentifizierung unterstützen zu können, dürfen nicht mehrere Werte festgelegt werden.

Begründung: Identifiziert die auditierte Funktion. Bei Auditeinträgen zu Ereignisaktionscodes mit dem Wert „E“ (Ausführen) wird hierdurch die ausgeführte Anwendungsfunktion identifiziert.

Obligatorisch ist mindestens CodeSystem (OID) oder CodeSystemName.

7.2.2 Ereignisaktionscode (en: Event Action Code)

Beschreibung: Indikator für die Art der im Auditereignis ausgeführten Aktion.

Optionalität: Obligatorisch.

Format/Werte: Aufzählung entsprechend Tabelle 5.

Tabelle 5 — Ereignisaktionscode

Wert	Bedeutung	Beispiele
C	Erzeugen (en: Create)	Erzeugen eines neuen Datenbankobjekts, zum Beispiel „Aufgeben einer Bestellung“
R	Lesen/Ansehen/Drucken/Abfragen (en: Read/View/Print/Query)	Daten – zum Beispiel eine Diagnose – anzeigen oder drucken
U	Aktualisieren (en: Update)	Daten aktualisieren, zum Beispiel „Persönliche Gesundheitsinformationen überarbeiten“
D	Löschen (en: Delete)	Zugriff auf Elemente unmöglich machen
E	Ausführen (en: Execute)	Ausführen einer System- oder Anwendungsfunktion, zum Beispiel Suchen oder Extrahieren oder Anwendung der Methode eines Objekts