

DIN EN ISO 27789

ICS 35.240.80

Einsprüche bis 2011-03-10

Entwurf**Medizinische Informatik –****Audit-Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2010);
Deutsche Fassung prEN ISO 27789:2010**

Health informatics –

Audit trails for electronic health records (ISO/DIS 27789:2010);

German version prEN ISO 27789:2010

Informatique de santé –

Pistes d'audit concernant les enregistrements électroniques touchant à la santé
(ISO/DIS 27789:2010);

Version allemande prEN ISO 27789:2010

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2011-01-10 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an named@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de, sofern dort wiedergegeben;
- oder in Papierform an den Normenausschuss Medizin (NAMed) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 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 56 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (prEN ISO 27789:2010) 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 NA 063-07-04 AA „Sicherheit“ des Normenausschusses Medizin (NAMed) im DIN haben an der Erarbeitung mitgewirkt.

Das Ausgabedatum des Europäischen Norm-Entwurfs stand zum Zeitpunkt der Veröffentlichung dieses DIN-EN-ISO-Entwurfs noch nicht fest; der prEN ISO wird jedoch vom CMC unter der angegebenen prEN-Nummer demnächst zur CEN-Umfrage verteilt. Um der deutschen Öffentlichkeit eine möglichst lange Einspruchsfrist einzuräumen, wurde dieser Norm-Entwurf vorab veröffentlicht.

Für die in den Normativen Verweisungen zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO 27799:2008 siehe DIN EN ISO 27799:2008

Nationaler Anhang NA (informativ)

Literaturhinweise

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

Medizinische Informatik — Audit-Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2010)

*Informatique de santé — Pistes d'audit concernant les enregistrements électroniques touchant à la santé
(ISO/DIS 27789:2010)*

Health informatics — Audit trails for electronic health records (ISO/DIS 27789:2010)

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

Inhalt

	Seite
Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Symbole und Abkürzungen	11
5 Anforderungen an und Verwendung von Auditdaten	11
5.1 Ethische und formale Anforderungen	11
5.1.1 Allgemeines	11
5.1.2 Zugriffsleitlinie	11
5.1.3 Eindeutige Identifikation der Benutzer von Informationssystemen	12
5.1.4 Benutzerrollen	12
5.1.5 Sichere Auditeinträge	12
5.2 Verwendung von Auditdaten	12
5.2.1 Lenkung und Überwachung	12
5.2.2 Wahrnehmung von Rechten durch die behandelten Personen	13
5.2.3 Ethischer oder rechtlicher Aktionsnachweis von Gesundheitsdienstleistern	13
6 Auslösende Ereignisse	13
6.1 Allgemeines	13
6.2 Einzelheiten zu den Ereignistypen und deren Inhalten	14
6.2.1 Zugriffereignisse auf persönliche Gesundheitsinformationen	14
6.2.2 Abfrageereignisse zu den persönlichen Gesundheitsinformationen	14
7 Einzelheiten zum Auditeintrag	15
7.1 Allgemeines Eintragsformat	15
7.2 Identifizierung von auslösenden Ereignissen	16
7.2.1 Ereignis-ID (Event ID)	16
7.2.2 Ereignisaktionscode (Event Action Code)	17
7.2.3 Ereignisdatum und -uhrzeit (Event Date und Event Time)	18
7.2.4 Ereignistypcode (Event Type Code)	18
7.3 Benutzeridentifizierung	19
7.3.1 Benutzer-ID (User ID)	19
7.3.2 Alternative Benutzer-ID (Alternative User ID)	19
7.3.3 Benutzername (User Name)	19
7.3.4 Benutzer ist Anfragender (User Is Requestor)	19
7.3.5 Rollen-ID-Code (Role ID Code)	20
7.4 Identifizierung des Zugriffspunkts	21
7.4.1 Code für den Typ des Netzwerkzugriffspunkts (Network Access Point Type Code)	21
7.4.2 Netzwerkzugriffspunkt-ID (Network Access Point ID)	22
7.5 Identifizierung der Auditquelle	22
7.5.1 Überblick	22
7.5.2 Standort-ID des Auditunternehmens (Audit Enterprise Site ID)	23
7.5.3 Auditquellen-ID (Audit Source ID)	23
7.5.4 Code für den Auditquellentyp (Audit Source Type Code)	23
7.6 Identifizierung des Teilnehmerobjekts	24
7.6.1 Überblick	24
7.6.2 Code für den Teilnehmerobjekttyp (Participant Object Type Code)	25
7.6.3 Code für die Rolle des Teilnehmerobjekttyps (Participant Object Type Code Role)	25
7.6.4 Datenlebenszyklus des Teilnehmerobjekts (Participant Object Data Life Cycle)	26

	Seite
7.6.5	Typcode der Teilnehmerobjekt-ID (Participant Object ID Type Code)..... 27
7.6.6	Sensibilität des Teilnehmerobjekts (Participant Object Sensitivity)..... 28
7.6.7	Teilnehmerobjekt-ID 29
7.6.8	Teilnehmerobjektname (Participant Object Name) 29
7.6.9	Teilnehmerobjektanfrage (Participant Object Query) 29
7.6.10	Teilnehmerobjektdetails (Participant Object Detail) 29
8	Auditeinträge für einzelne Ereignisse 30
8.1	Zugriffereignisse 30
8.2	Abfrageereignisse 31
9	Sichere Verwaltung von Auditdaten 33
9.1	Überlegungen zur Sicherheit 33
9.2	Sichern der Verfügbarkeit des Auditsystems 34
9.3	Anforderungen an die Aufbewahrung 34
9.4	Sicherung der Vertraulichkeit und Integrität von Audit-Trails 34
9.5	Zugriff auf Auditdaten 35
Anhang A	(informativ) Auditszenarien 36
A.1	Überblick 36
A.2	Fall des verärgerten Prominenten 36
A.3	Fall des durchgesetzten Rechts auf Privatsphäre (retrospektiv, nicht aktiv) 38
A.4	Fall eines Servers mit beeinträchtigter Sicherheit 39
A.5	Fall eines mit Privilegien ausgestatteten Benutzers, der diese Privilegien missbraucht 39
A.6	Fall der fehlgeleiteten Untersuchungsergebnisse 40
A.7	Fall der erratischen Transaktionen 41
A.8	Fall der verschwundenen Auditeinträge – Ziel ist Audit-Repository 42
A.9	Fall eines Hackers, der gefälschte Auditeinträge erzeugt 42
A.10	Fall eines Hackers, der Auditeinträge ausspioniert und diese auf böswillige Weise verwendet 42
A.11	Fall einer ungewöhnlichen (autorisierten/nicht autorisierten) Konfigurationsänderung 42
A.12	Fall eines Benutzers, der einen Brute-Force-Angriff auf ein Passwort unternimmt 43
Anhang B	(informativ) Auditprotokolldienste 44
B.1	Dienste im Diagramm 44
B.2	Auditloggerdienst (Audit Logger Service) 45
B.3	Auditeinträgerzeugerdienst (Audit Record Generator Service) 46
B.4	Auditereigniskatalogdienst (Audit Event Catalog Service) 46
B.5	Auditüberwachungsdienst (Audit Monitor Service) 47
B.6	Warnmeldungs- oder Benachrichtigungsdienst (Alert oder Notification Service) 50
B.7	Auditberichtsdienst (Audit Report Service) 51
B.8	Auditauswertungsdienst (Audit Analysis Service) 53
Literaturhinweise	 54

Vorwort

Dieses Dokument (prEN ISO 27789:2010) 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.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 27789:2010 wurde vom CEN als prEN ISO 27789:2010 ohne irgendeine Abänderung genehmigt.

Einleitung

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 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. 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.

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.

Wer ist Zielgruppe dieser Norm?

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.

Vergleich mit verwandten Normen zu Audit-Trails für elektronische Gesundheitsakten

Diese Norm stimmt mit den Anforderungen von ISO 27799:2008, *Health informatics — 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* [1], 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 3881 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.

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

Die Einträge der elektronische Gesundheitsakten behandelter Personen können in vielen unterschiedlichen Informationssystemen innerhalb einer Organisation oder auch organisations- oder zuständigkeitsbereichs-übergreifend liegen. Um die Übersicht über alle Aktionen zu behalten, die Einträge zu einer bestimmten behandelten Person betreffen, ist ein gemeinsamer Rahmen erforderlich.

Audit-Trails für elektronische Gesundheitsakten, die auf unterschiedliche Systeme verteilt sind, benötigen einen gemeinsamen Rahmen, um die Auditierbarkeit des vollständigen Satzes der persönlichen Gesundheitsinformationen aufrechtzuerhalten. Dieses Dokument legt diesen gemeinsamen Rahmen für die auslösenden Ereignisse eines Audits und für Auditdaten fest.

Nach ISO 27799 müssen Informationssysteme, die persönliche Gesundheitsinformationen enthalten, jedes Mal, wenn ein Benutzer über das System auf diese Informationen zugreift, sie erzeugt, aktualisiert oder archiviert, einen sicheren Auditeintrag erstellen. Bei diesem Auditeintrag handelt es sich mindestens um eine eindeutige Identifizierung des Benutzers und 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 bzw. der die Funktion ausgeführt wurde.

Der Anwendungsbereich dieser Norm beschränkt sich auf an elektronischen Gesundheitsakten ausgeführte Aktionen. Diese Aktionen werden durch die Zugriffsleitlinien für die Domäne bestimmt, in der die elektronische Gesundheitsakte liegt. Audit-Trails für elektronische Gesundheitsakten können bei der Feststellung der Einhaltung der Zugriffsleitlinien helfen.

Die durch diese Norm festgelegten Audit-Trails 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 [6], behandelt.

Die vorliegende Norm enthält Beispiele für Dienste für eine sichere 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 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 auf die Ressourcen eines Datenverarbeitungssystems nur von autorisierten Entitäten über autorisierte Kanäle zugegriffen werden kann

[ISO/IEC 2382-8:1998]

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]

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

Auditierbarkeit

Eigenschaft, die sicherstellt, dass eine von einem beliebigen Sicherheitssubjekt an einem beliebigen Sicherheitsobjekt vorgenommene beliebige Aktion überprüft werden kann, um die tatsächlichen operationalen Verantwortlichkeiten zu ermitteln

[ENV 13608-1:2000]

3.12

Authentisierung

Prozess der zuverlässigen Identifizierung von Sicherheitssubjekten durch sichere Zuweisung eines Bezeichners und dessen Authentifikators

[ISO 7498-2:1998]

3.13

Autorisierung

Gewährung von Rechten

3.14

Autorität

Entität, die für die Ausgabe von Zertifikaten verantwortlich ist

3.15

Verfügbarkeit

Eigenschaft, auf Anforderung durch eine autorisierte Entität zugänglich und nutzbar zu sein

[ISO 7498-2:1998]

3.16

Vertraulichkeit

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

[ISO 7498-2:1998]

3.17

Datenintegrität

Eigenschaft, dass Daten nicht auf unberechtigte Weise verändert oder zerstört wurden

[ISO 7498-2:1998]

3.18

eGA

elektronische Gesundheitsakte

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

3.19

eGA-Anbieter

Entität, die im rechtmäßigen Besitz von eGA-Daten ist und sich in einer Position befindet, diese Daten einer anderen entsprechenden Entität zu übermitteln

3.20

eGA-Empfänger

Entität, der von einem eGA-Anbieter eGA-Daten übermittelt werden

3.21

eGA-Anforderer

Entität, die die Anforderung einer eGA-Übermittlung zwischen einem eGA-Anbieter und einem eGA-Empfänger einleitet

3.22

eGA-Segment

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

3.23

Identifizierung

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

[ISO/IEC 2382-8:1998]

3.24

Bezeichner

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

[ENV 13608-1:2000]

3.25

Integrität

Eigenschaft der Absicherung der Richtigkeit und Vollständigkeit von Werten

[ISO/IEC 27000:2009]

3.26

Schlüssel

Folge von Symbolen, die die Chiffrier- und Dechiffrieroperationen steuern

[ISO 7498-2:1998]

3.27

Leitlinie

Policy

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

[ISO/TS 22600-1:2005]

3.28

Privileg

Berechtigung

Fähigkeit, die einer Entität von einer Autorität zugewiesen wird

3.29

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]

3.30

Rolle

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

3.31

Sensibilität

Informationen zugewiesenes Maß der Wichtigkeit, das den Schutzbedarf dieser Informationen angibt

3.32

Sicherheit

Kombination aus Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit

[ENV 13608-1:2000]

3.33

Sicherheitsleitlinie

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

3.34

Sicherheitsdienst

Dienst, der von einer Schicht miteinander kommunizierender offener Systeme erbracht wird und die angemessene Sicherheit der Systeme oder des Datentransfers sicherstellt

[ISO 7498-2:1998]

3.35

behandelte Person zu Behandelnder

Person, die terminlich eingeplant ist, eine Gesundheitsdienstleistung zu erhalten, diese gerade erhält oder bereits erhalten hat

[ISO/TS 18308:2004]

3.36

Ziel

Ressource, auf die zugegriffen wird

3.37

Benutzer

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

4 Symbole und Abkürzungen

eGAelektronische Gesundheitsakte

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.

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

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

ISO 27799, 7.8.1.2 gibt folgende Anforderungen an die Leitlinie zur Zugriffskontrolle an:

- Organisationen, die persönliche Gesundheitsinformationen verarbeiten, müssen eine Leitlinie zur Zugriffskontrolle haben, die den Zugang/Zugriff zu diesen Daten regelt.
- Die Leitlinie der Organisation zur Zugriffskontrolle sollte auf der Basis von vordefinierten Rollen mit zugehörigen Befugnissen, die konsistent mit, aber nicht begrenzt auf die Erfordernisse dieser Rolle sind, eingeführt werden.
- Die Leitlinie zur Zugriffskontrolle, so, wie sie als Komponente des Informationssicherheits-Rahmenwerks in ISO 27799, 7.2.1, beschrieben ist, muss berufliche, ethische, rechtliche und auf die behandelte Person bezogene Anforderungen widerspiegeln und sollte die Aufgaben, die von den Heilberuflern ausgeführt werden, und den Arbeitsablauf dieser Aufgaben berücksichtigen.

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.

ISO 27799, 7.8.2.2, legt für die Umsetzung des Privilegienmanagements Folgendes fest:

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.

Funktionelle und strukturelle Rollen sind in ISO/TS 21298 [9] dokumentiert. Zusätzliche Anleitungen zum Privilegienmanagement im Gesundheitswesen sind in ISO/TS 22600, Teil 1 bis Teil 3 [8], angegeben.

5.1.5 Sichere Auditeinträge

ISO 27799 (7.7.10.2) fordert jedes Mal, wenn auf persönliche Gesundheitsinformationen zugegriffen wird bzw. diese erzeugt, aktualisiert oder archiviert werden, die Erstellung sicherer Auditeinträge. 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 ausreichend 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.

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 Behandelten zugegriffen haben;
- Feststellen, wer für den Inhalt des Eintrags verantwortlich ist (Zurechenbarkeit);
- 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 und des Zeitpunkts des Zugriffs.

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, 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:

- 1) Zugriffereignisse auf persönliche Gesundheitsinformationen;
- 2) Abfrageereignisse zu persönlichen Gesundheitsinformationen.

Beispiele für Ereignisse, die außerhalb des Anwendungsbereichs liegen:

- 1) Start- und Stoppereignisse des Anwendungsprogramms;
- 2) Authentisierungsereignisse, die die Benutzerauthentisierung einschließen;
- 3) Eingabe- und Ausgabeereignisse in die/aus der externen Umgebung;
- 4) Zugriffereignisse auf andere Informationen als persönliche Gesundheitsinformationen;
- 5) Sicherheitswarnereignisse im Zusammenhang mit den Anwendungsprogrammen;
- 6) Zugriffereignisse auf das in den Anwendungsprogrammen aufbewahrte Auditprotokoll;
- 7) vom Betriebssystem, der Middleware usw. generierte Ereignisse;
- 8) durch Verwendung von Systemprogrammen generierte Zugriffereignisse;
- 9) Verbindungs-/Trennungereignisse zwischen Geräten und Netzwerk;
- 10) Start-/Stoppereignisse der Schutzsysteme, zum Beispiel Virenschutzsysteme;
- 11) 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.

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“.

Ereignis	Inhalt
Abfrageereignisse zu der persönlichen Gesundheitsinformation	Wann Wer Welche Abfragebedingung

7 Einzelheiten zum Auditeintrag

7.1 Allgemeines Eintragsformat

Dieser Abschnitt beschreibt das allgemeine Format der Auditeinträge. Zum Eintragsinhalt der einzelnen Ereignisse siehe Abschnitt 8. Das Eintragsformat ist in Übereinstimmung mit RFC 3881 [1] definiert.

Die Tabelle ist wie folgt zu interpretieren:

Multiplizität:

- (1): nur 1 existiert;
- (0..1): 0 oder 1 existiert;
- (1..2): 1 oder 2 existiert (existieren);
- (0..N): 0 bis N existiert (existieren).

Optionalität:

- M: obligatorisch;
- MC: bedingt obligatorisch;
- U: optional;
- M/U: obligatorisch oder optional in Bezug auf Ereignisse.