PROJET
FINAL

NORME
INTERNATIONALE

**ISO/FDIS
27789**

ISO/TC **215**

Secrétariat: ANSI

Début de vote:
2021-05-19

Vote clos le:
2021-07-14

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

Health informatics — Audit trails for electronic health records

TRAITEMENT PARALLÈLE ISO/CEN

Numéro de référence
ISO/FDIS 27789:2021(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 215, *Informatique de santé*, en collaboration avec le comité technique CEN/TC 251, *Informatique de santé*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO 27789:2013), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— harmonisation du format des enregistrements d'audit avec le format DICOM;

— révision du contenu de l'Annexe A;

— révision du graphique de l'Annexe B;

— mise à jour de la Bibliographie.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

0.1 Généralités

Parmi tous les types d'informations personnelles, les informations personnelles de santé sont considérées comme étant les plus confidentielles et la protection de leur confidentialité est essentielle pour préserver la vie privée des sujets de soins. Afin de protéger la qualité des informations en matière de santé, il est également important que leur cycle de vie complet soit entièrement auditable. Il convient de créer, de traiter et de gérer les dossiers de santé de façon à garantir l'intégrité et la confidentialité de leur contenu et à permettre aux sujets de soins de contrôler de manière tout à fait légitime la façon dont les dossiers sont créés, utilisés et conservés.

La confiance dans les dossiers de santé informatisés nécessite des éléments de sécurité physiques et techniques ainsi que des éléments d'intégrité des données. Parmi les exigences de sécurité les plus importantes pour protéger les informations personnelles de santé et l'intégrité des dossiers figurent celles qui concernent l'audit et le contrôle d'accès. Elles permettent de respecter les obligations envers les sujets de soins confiant leurs informations aux systèmes de dossiers de santé informatisés (DSI). Elles contribuent également à protéger l'intégrité des dossiers, car elles incitent fortement les utilisateurs à se conformer aux politiques organisationnelles appliquées à l'utilisation de ces systèmes.

Un audit et un contrôle d'accès efficaces peuvent favoriser la détection des utilisations abusives des systèmes de DSI ou des données de DSI et peuvent aider les organisations et les sujets de soins à obtenir réparation face à des utilisateurs ayant abusé de leurs privilèges d'accès. Afin que l'audit soit efficace, il est nécessaire que les pistes d'audit contiennent suffisamment d'informations pour permettre le traitement de situations très diverses (voir Annexe A).

Les journaux d'audit constituent un complément aux contrôles d'accès. Les journaux d'audit fournissent un moyen d'évaluer la conformité aux politiques organisationnelles en matière d'accès et peuvent contribuer à améliorer et à affiner la politique en elle-même. Mais, comme une telle politique a besoin d'anticiper l'apparition de cas imprévus ou d'urgence, l'analyse des journaux d'audit devient, dans ces cas-là, le meilleur moyen d'assurer le contrôle des accès.

Le domaine d'application du présent document est strictement limité à la consignation des événements. Les modifications apportées aux valeurs des champs d'un DSI sont supposées être enregistrées dans le système de base de données des DSI, et non, dans le journal d'audit. Le système de DSI est supposé contenir les valeurs de chaque champ, avant et après leur mise à jour, ce qui répond aux architectures de base de données actuelles. Le journal d'audit en soi n'est supposé contenir aucune information personnelle de santé autre que les identifiants et les liens pointant vers le dossier.

Le dossier de santé informatisé propre à un certain individu peut appartenir à plusieurs systèmes d'informations différents, situés à l'intérieur ou au-delà des frontières organisationnelles, voire même juridictionnelles. Afin de garder la trace de toutes les actions impliquant les dossiers relatifs à un sujet de soins particulier, il est indispensable de disposer d'un cadre commun. Le présent document fournit un tel cadre. Pour prendre en charge des pistes d'audit couvrant des domaines distincts, il est essentiel que ce cadre inclue des références aux politiques qui spécifient les exigences propres à chaque domaine, telles que les règles de contrôle d'accès et les durées de conservation. Les politiques régissant les domaines peuvent être référencées implicitement par l'identification de la source du journal d'audit.

0.2 Avantages de l'utilisation du présent document

La normalisation des pistes d'audit concernant l'accès aux dossiers de santé informatisés a deux objectifs:

— assurer que l'information contenue dans le journal d'audit est suffisante pour reconstruire clairement la chronologie détaillée des événements ayant conduit au contenu d'un dossier de santé informatisé;

— assurer que la piste d'audit des actions relatives au dossier d'un sujet de soins puisse être suivie de façon fiable, même si elle couvre différents domaines organisationnels.

Le présent document est destiné aux responsables de la supervision de la sécurité ou de la confidentialité des informations de santé, aux organismes de santé et aux autres dépositaires d'informations de santé qui sont à la recherche de recommandations concernant les pistes d'audit, ainsi qu'à leurs conseillers en matière de sécurité, consultants, auditeurs, fournisseurs et prestataires de service externes.

0.3 Normes relatives aux pistes d'audit des dossiers de santé informatisés

Le présent document est élaboré sur la base du travail débuté dans le document RFC 3881 concernant l'accès aux DSI et s'y conforme. Le présent document repose également sur le contenu de l'ISO/TS 21089:2018 et s'y conforme.

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

1 Domaine d'application

Le présent document définit un cadre commun pour les pistes d'audit des dossiers de santé informatisés (DSI), en termes d'événements déclencheurs d'audit et de données d'audit, afin de conserver l'ensemble complet des informations personnelles de santé auditables, quels que soient les systèmes et les domaines d'information.

Le présent document s'applique aux systèmes de traitement des informations personnelles de santé qui créent un enregistrement d'audit sécurisé chaque fois qu'un utilisateur crée des informations personnelles de santé, qu'il les lit, qu'il les met à jour ou qu'il les archive par le biais du système.

NOTE Au minimum, ces enregistrements d'audit identifient de manière unique l'utilisateur, identifient de manière unique le sujet de soins, identifient la fonction exécutée par l'utilisateur (création d'un dossier, lecture d'un dossier, mise à jour d'un dossier, etc.) et enregistrent la date et l'heure auxquelles la fonction a été exécutée.

Le présent document ne couvre que les actions effectuées sur le dossier de santé informatisé, qui sont régies par une politique d'accès propre au domaine dans lequel s'inscrit le dossier de santé informatisé. Il ne traite d'aucune information personnelle de santé issue de dossiers de santé informatisés, à l'exception des identifiants, les enregistrements d'audit ne contenant que des liens pointant vers des segments du DSI, tels que définis par la politique d'accès applicable.

Le présent document ne couvre pas non plus la spécification et l'utilisation des journaux d'audit à des fins de gestion et de sécurité du système, par exemple, la détection des problèmes de performance, des failles au niveau des applications, ou le support de reconstruction des données, qui sont traités par les normes de sécurité informatique générales, telles que l'ISO/IEC 15408 (toutes les parties)[[9]].

L'Annexe A donne des exemples de scénarios d'audit. L'Annexe B donne un aperçu des services de journal d'audit.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 27799:2016, *Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002*

ISO 8601-1, *Date et heure — Représentations pour l'échange d'information — Partie 1: Règles de base*

ISO/TS 21089:2018, *Informatique de santé — Flux d'informations "trusted end-to-end"*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/TS 21089:2018 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier

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

3.2
politique d'accès
définition des obligations concernant l'autorisation d'accès à une ressource

3.3
responsabilité
obligation d'un individu ou d'une organisation de rendre compte de ses activités, de l'exécution d'un livrable ou d'une tâche, d'assumer la responsabilité de ces activités, livrables ou tâches, et d'en divulguer les résultats de façon transparente

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

3.4
agent
entité, telle qu'un logiciel ou un dispositif, qui entreprend des actions programmées

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

3.5
alerte
ce qui est envoyé lorsque le service de surveillance remarque une série d'événements correspondant à un modèle

3.6
audit
revue et examen indépendants de dossiers et d'activités, menés dans le but d'évaluer l'adéquation des contrôles du système pour garantir la conformité aux politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires à introduire dans les contrôles, politiques ou procédures

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

3.7
archive d'audit
archive créée à partir de la collecte d'un ou de plusieurs journaux d'audit

3.8
données d'audit
données obtenues à partir d'un ou de plusieurs enregistrements d'audit

3.9
journal d'audit
séquence chronologique d'enregistrements d'audit, chacun contenant des données sur un événement spécifique

3.10
enregistrement d'audit
enregistrement d'un événement unique particulier ayant eu lieu au cours du cycle de vie du dossier de santé informatisé

3.11
système d'audit
système de traitement de l'information permettant de tenir à jour un ou plusieurs journaux d'audit

3.12
piste d'audit
enregistrement chronologique des activités d'un système, suffisant pour permettre la reconstruction, la vérification et l'examen de la séquence des environnements et des activités qui encadrent, ou conduisent à, une opération, une procédure ou un événement dans une transaction, de ses débuts jusqu'à ses résultats finaux

[SOURCE: GCST]

3.13
authentification
moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée

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

3.14
autorisation
attribution de droits, comprenant la permission d'accès sur la base de droits d'accès

[SOURCE: ISO/IEC 2382:2015, 2126256, modifiée — Les Notes à l'article ont été supprimées.]

3.15
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

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

3.16
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés

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

3.17
temps universel coordonné
UTC
échelle de temps qui constitue la base d'une diffusion radioélectrique coordonnée des fréquences étalon et des signaux horaires

Note 1 à l'article: Le temps universel coordonné a la même marche que le temps atomique international, mais en diffère d'un nombre entier de secondes.

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

3.18
intégrité des données
propriété assurant que l'exactitude et la cohérence des données sont préservées quels que soient les changements effectués

[SOURCE: ISO 2382:2015, 2126247, modifiée — Les Notes à l'article ont été supprimées.]

3.19
dossier de santé informatisé
DSI
dépôt (d'ensembles organisés) d'informations relatives à la santé d'un sujet de soins, sous une forme pouvant être informatisée

[SOURCE: ISO/TR 20514:2005, 2.11, modifiée — Le texte entre parenthèses a été ajouté.]

3.20
segment de dossier de santé informatisé
segment de DSI
partie d'un dossier de santé informatisé constituant une ressource distincte pour la politique d'accès

3.21
identification
processus de reconnaissance des attributs qui identifient l'objet

[SOURCE: ISO 16678:2014, 2.1.7]

3.22
identifiant
mot ou groupe de mots servant à identifier ou nommer un élément de données et en préciser parfois certaines propriétés

[SOURCE: ISO 2382:2015, 2121623]

3.23
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

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

3.24
intégrité
propriété d'exactitude et de complétude

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

3.25
identifiant d'objet
OID
identifiant unique à l'échelle planétaire d'un objet d'information

Note 1 à l'article: Les identifiants d'objet utilisés dans le présent document correspondent à des systèmes de code. Ces systèmes de code peuvent être définis dans une norme ou peuvent être définis localement par une implémentation. L'identifiant d'objet est spécifié en utilisant la notation de syntaxe abstraite numéro 1 (ASN.1) définie dans l'ISO/IEC 8824-1 et dans l'ISO/IEC 8824-2.

3.26
politique
ensemble de règles relatives à un objectif particulier

Note 1 à l'article: Une règle peut s'exprimer sous forme d'obligation, d'autorisation, de permission ou d'interdiction.

[SOURCE: ISO 19101-2:2018, modifiée — La Note 1 à l'article a été ajoutée.]

3.27
privilège
capacité assignée à une entité par une autorité

3.28
gestion des documents d'activité
champ de l'organisation et de la gestion en charge d'un contrôle de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents d'activité, y compris des processus de capture et de préservation de la preuve et de l'information liées aux activités et aux opérations sous la forme de documents d'activité

[SOURCE: ISO 15489-1:2016, 3.15, modifiée]

3.29
rôle
ensemble de compétences et/ou de performances, associé à une tâche

3.30
politique de sécurité
plan ou programme d'action adopté pour assurer la sécurité informatique

[SOURCE: ISO/IEC 2382:2015, 2126246, modifiée — Les Notes à l'article ont été supprimées.]

3.31
sensibilité
mesure du risque ou du risque perçu qu'un sujet subisse un préjudice associé à ces données ou que celles-ci soient utilisées de manière abusive ou soient mal utilisées

3.32
sujet de soins
personne ou groupe défini de personnes qui reçoit, qui est habilité à recevoir ou qui a reçu des services de soins

[SOURCE: ISO/TS 17975:2015, modifiée — La Note à l'article a été ajoutée.]

Note 1 à l'article: Par exemple, un patient, un client ou un membre d'un régime de santé.

3.33
utilisateur
personne ou autre entité autorisée par un fournisseur à utiliser tout ou partie des services proposés par le fournisseur

Note 1 à l'article: Ce terme désigne également un être humain qui utilise un système pour adresser des demandes à des objets afin qu'ils exécutent des fonctions sur le système en son nom.

[SOURCE: COACH; OMG]

4 Abréviations

HL7® Health Level Seven (organisme de normalisation des échanges informatiques dans le domaine de la santé)

5 Exigences et usages des données d'audit

5.1 Exigences éthiques et formelles

5.1.1 Généralités

Les prestataires de soins de santé ont certaines responsabilités professionnelles et éthiques à assumer, comme entre autres, la protection de la vie privée des sujets de soins ainsi que la documentation des conclusions et des activités de soins. Restreindre l'accès aux dossiers de santé et garantir leur utilisation appropriée sont deux exigences essentielles dans le domaine des soins de santé et, dans de nombreuses juridictions, ces exigences sont fixées par la loi.

Les pistes d'audit sécurisées concernant les accès aux dossiers de santé informatisés peuvent appuyer la conformité avec l'éthique professionnelle, les politiques organisationnelles et la législation, mais elles ne sont pas suffisantes en elles-mêmes pour évaluer la complétude d'un dossier de santé informatisé.

5.1.2 Politique d'accès

L'accès à la piste d'audit doit être régi par une politique d'accès. Il convient que cette politique soit définie par l'organisation responsable de la tenue du journal d'audit.

La politique d'accès doit être conforme à l'ISO 27799:2016, 9.1.1.

NOTE 1 La politique d'accès est censée définir la structure d'un segment de DSI.

NOTE 2 Dans l'enregistrement d'audit, la politique d'accès est identifiée par la source du journal d'audit.

Des recommandations sur la spécification et l'implémentation des politiques d'accès peuvent être consultées dans l'ISO 22600 (toutes les parties).[[6]] Un champ «Ensemble de politiques d'autorisation de l'objet participant» est défini en 7.6.6 afin de prendre en charge les références aux politiques réelles dans l'enregistrement d'audit.

5.1.3 Identification sans équivoque des utilisateurs du système informatique

Les pistes d'audit doivent fournir suffisamment de données pour identifier sans équivoque tous les utilisateurs autorisés du système d'informations de santé. Les utilisateurs du système d'informations peuvent aussi bien être des personnes que d'autres entités.

Les pistes d'audit doivent fournir suffisamment de données pour déterminer quels utilisateurs et systèmes externes autorisés ont accédé à ou ont reçu des données de dossier de santé de la part du système.

5.1.4 Rôles des utilisateurs

La piste d'audit doit présenter le rôle de l'utilisateur ayant appliqué l'action enregistrée aux informations personnelles de santé.

Il convient que les systèmes d'informations traitant des informations personnelles de santé soient pourvus d'un contrôle d'accès en fonction du rôle, qui soit en mesure de mettre en correspondance chaque utilisateur avec un ou plusieurs rôles et chaque rôle avec une ou plusieurs fonctions du système, comme recommandé dans l'ISO 27799:2016, 9.2.3.

Les rôles fonctionnels et structurels sont documentés dans l'ISO 21298.[[4]] Des recommandations supplémentaires sur la gestion des privilèges dans le domaine de la santé sont données dans l'ISO 22600 (toutes les parties)[[6]].

5.1.5 Enregistrements d'audit sécurisés

Des enregistrements d'audit sécurisés conformes à l'ISO 27799:2016, 12.4.1 doivent être créés à chaque fois que des informations personnelles de santé sont lues, créées, mises à jour ou archivées. Les enregistrements d'audit doivent être conservés par le biais d'une gestion sécurisée des enregistrements.

5.2 Usages des données d'audit

5.2.1 Gouvernance et supervision

Les pistes d'audit doivent fournir des données permettant aux autorités responsables d'évaluer la conformité à la politique organisationnelle et son efficacité.

Cela implique:

— la détection des accès non autorisés aux dossiers de santé;

— l'évaluation des accès d'urgence; et

— la détection des abus de privilèges;

et le support de:

— la documentation des accès entre les domaines; et

— l'évaluation des politiques d'accès.

NOTE Une évaluation complète de la conformité à la politique organisationnelle peut nécessiter des données complémentaires qui ne sont pas contenues dans l'enregistrement d'audit, telles que des informations relatives à l'utilisateur, des tableaux ou des enregistrements de permission concernant une entrée physique dans des salles sécurisées. Voir Annexe B en ce qui concerne les services de journal d'audit.

Les pistes d'audit doivent fournir suffisamment de données pour déterminer tous les accès aux dossiers de sujets de soins, ayant eu lieu au cours d'une période déterminée et effectués par un utilisateur donné.

Les pistes d'audit doivent fournir suffisamment de données pour déterminer tous les accès aux dossiers de sujets de soins ayant eu lieu au cours d'une période déterminée et considérés comme représentant un risque élevé de violation de la vie privée.

5.2.2 Sujets de soins exerçant leurs droits

Les pistes d'audit doivent fournir suffisamment de données pour permettre aux sujets de soins:

— d'évaluer le ou les utilisateurs qui ont eu accès à leur dossier de santé et à quel moment;

— d'évaluer la responsabilité concernant le contenu du dossier;

— de déterminer si les directives traitant du consentement du sujet de soins, eu égard à l'accès aux données le concernant ou la divulgation de celles-ci, sont respectées; et

— de déterminer les accès d'urgence au dossier de santé du sujet de soins (le cas échéant) octroyés par un utilisateur, y compris l'identification de l'utilisateur, l'heure d'accès et l'endroit à partir duquel a eu lieu l'accès.

5.2.3 Exigences de preuve et de conservation

Les pistes d'audit doivent conserver des données (que les prestataires de soins de santé peuvent utiliser comme preuves documentées) afin d'identifier les actions qui ont été entreprises (création, recherche, lecture, correction, mise à jour, extraction, exportation, archivage, etc.) en lien avec ces informations, quand et par qui.

Les enregistrements d'audit doivent être conservés conformément à la politique de conservation décrite en 9.3.

Les documents suivants fournissent des recommandations et des informations supplémentaires:

— ISO/TS 21089;

— ISO/HL7 10781[[20]].

6 Événements déclencheurs

6.1 Généralités

Les événements d'audit (événements déclencheurs) qui sont à l'origine de la génération d'enregistrements d'audit par le système d'audit sont définis en fonction de l'échelle, de l'objectif et du contenu des politiques de confidentialité et de sécurité de chaque système d'informations de santé. Le domaine d'application du présent document étant limité aux informations personnelles de santé, seuls les événements déclencheurs relatifs à l'accès et à la recherche de telles informations sont spécifiés dans cet article.