NORME INTERNATIONALE

ISO 27789

Deuxième édition
2021-10

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

Health informatics — Audit trails for electronic health records

Numéro de référence
ISO 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 www.iso.org/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 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.