NORME INTERNATIONALE

ISO 13606-4

Première édition
2019-06

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Health informatics — Electronic health record communication — Part 4: Security

Numéro de référence
ISO 13606-4:2019(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
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*.

Cette première édition de l'ISO 13606-4 annule et remplace la première édition de l'ISO/TS 13606-4:2009, qui a fait l'objet d'une révision technique.

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

— rôles fonctionnels;

  — certains termes relatifs aux rôles fonctionnels ont été mis à jour pour s'aligner sur CONTSYS;

  — les règles d'utilisation de ce vocabulaire stipulent maintenant que les juridictions peuvent nommer des alternatives ou des spécialisations de ces termes si nécessaire;

— modèle de politique d'accès;

  Le modèle de politique d'accès permet maintenant d'utiliser les termes alternatifs des juridictions le cas échéant.

— modèle de rapport d'expertise.

  Le modèle de rapport d'expertise est maintenant aligné sur la norme ISO 27789 pour les historiques d'expertise de DSI. Il contient plus d'informations qu'il n'y en a dans l'ISO 27789: il s'agit d'un type de spécialisation traitant spécifiquement de la communication des informations du DSI et des informations du rapport d'expertise. Il inclut donc des informations sur l'extrait de DSI ou l'extrait de rapport d'expertise communiqué, ce qui ne fait pas partie du domaine d'application de l'ISO 27789.

Une liste de toutes les parties de la série ISO 13606 se trouve sur le site web de l'ISO.

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

Le présent document fait partie d'une série de normes en cinq parties, publiées conjointement par le CEN et l'ISO dans le cadre de l'Accord de Vienne. Dans le présent document, la dépendance à l'une des autres parties de la série est explicitement indiquée là où elle s'applique.

0.2 Sujets abordés dans la présente partie de l'ISO 13606

La communication des dossiers de santé informatisés (DSI) complets ou de parties de ceux-ci, dans les limites d'une organisation et entre organisations, quelquefois même au-delà des frontières nationales, pose des problèmes du point de vue de la sécurité. Il convient de créer, traiter et gérer les dossiers de santé de manière à assurer la confidentialité de leur contenu et à permettre aux patients de contrôler la manière dont ils sont utilisés. Dans le monde entier, ces principes s'inscrivent progressivement dans les législations nationales de protection des données. Ces instruments déclarent que le sujet des soins a le droit de jouer un rôle central dans les décisions prises sur le contenu et la distribution de son dossier de santé informatisé, ainsi que le droit d'être informé de son contenu. Il convient que la communication des informations des dossiers de santé à des tiers se fasse uniquement avec l'accord du patient (qui peut être toute indication spécifique et informée donnée librement de son souhait, par laquelle le sujet des informations signifie son accord avec le traitement de ses données personnelles). L'ISO 22600-3 donne de plus amples détails. Pour la communication des DSI au-delà des frontières nationales, l'ISO 22857 donne des recommandations qui peuvent être utilisées pour définir des spécifications appropriées de politique de sécurité.

Dans l'idéal, il convient que chaque entrée affinée dans le dossier d'un patient soit accessible uniquement par les personnes qui ont l'autorisation de voir ces informations, spécifiées ou approuvées par le patient et reflétant la nature dynamique de l'ensemble des personnes disposant d'un devoir de soins légitime envers le patient tout au long de sa vie. La liste de contrôle d'accès inclut également dans l'idéal les personnes qui ont l'autorisation d'accéder aux données pour des raisons autres que le devoir de soins (comme la gestion d'un service de soins, l'épidémiologie et la santé publique, la recherche consentie) mais exclut toute information qu'elles n'ont pas besoin de connaître ou que le patient considère comme trop personnelles pour les leur divulguer. Par ailleurs, il convient que l'étiquetage par les patients ou leurs représentants d'informations comme étant personnelles ou privées ne gêne pas les personnes ayant un besoin légitime de voir les informations en cas d'urgence ni n'ait pour conséquence que des authentiques prestataires de soins de santé disposent d'un point de vue incomplet qui les induirait en erreur dans la gestion du patient. Le point de vue des patients sur la sensibilité inhérente[1)] des données de leur dossier de santé peut évoluer dans le temps, à mesure que leurs angoisses à propos de leur santé ou que les attitudes sociétales envers leurs problèmes de santé changent. Les patients peuvent souhaiter que leur famille, leurs amis, les soignants et les membres de leur communauté bénéficient de niveaux d'accès différents. Les familles peuvent souhaiter offrir un moyen leur permettant d'accéder à des parties du dossier les uns des autres (pas nécessairement dans la même mesure) afin de surveiller les progrès des états de santé hérités au sein d'une famille.

Un tel ensemble d'exigences est sans doute plus complet que celui qui est exigé des contrôleurs de données dans la plupart des autres domaines industriels. Dans la pratique, il est rendu extrêmement complexe en raison des éléments suivants:

— le grand nombre d'entrées dans le dossier de santé au cours des soins de santé administrés de nos jours au patient;

— le grand nombre de personnels de soins de santé, changeant souvent de postes, pouvant potentiellement entrer en contact avec un patient à tout moment;

— le grand nombre d'organisations avec lesquelles un patient peut entrer en contact au cours de sa vie;

1) Le terme sensibilité est largement utilisé dans le domaine de la sécurité pour une large gamme de protections et de contrôles mais dans le présent document, ce terme se réfère uniquement aux contrôles d'accès.

