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 2019



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2019

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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 ..... **iv**
Introduction ..... **vi**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Abréviations **2**
5 Conformité **3**
6 Sensibilité des éléments du dossier et rôles fonctionnels **3**
6.1 Sensibilité de RECORD_COMPONENT 3
6.2 Rôles fonctionnels 4
6.3 Mise en correspondance du rôle fonctionnel avec la sensibilité de COMPOSITION 4
7 Représentation des informations de politique d'accès dans un EHR_EXTRACT **5**
7.1 Vue d'ensemble 5
7.2 Représentation UML de l'archétype de la politique d'accès COMPOSITION 7
7.2.1 Politique d'accès 7
7.2.2 Cible 8
7.2.3 Critère de demande 9
7.2.4 Contrainte de sensibilité 10
7.2.5 Informations d'attestation 11
7.3 Archétype de la COMPOSITION de politique d'accès 12
8 Représentation des informations du rapport d'expertise **12**
8.1 Généralités 12
8.1.1 Extrait de rapport d'expertise de DSI 13
8.1.2 Contrainte de rapport d'expertise 13
8.1.3 Entrée de rapport d'expertise de DSI 14
8.1.4 Description de l'extrait de DSI 15
8.1.5 Extrait démographique 16
Annexe A (informative) **Exemple illustratif de contrôle d'accès** **17**
Annexe B (informative) **Relations entre l'ISO 13606-4 et des approches alternatives** **21**
Bibliographie **23**

© ISO 2019 – Tous droits réservés

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.

 © ISO 2019 – Tous droits réservés

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.

© ISO 2019 – Tous droits réservés

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.

 © ISO 2019 – Tous droits réservés

— la difficulté (pour le patient ou pour toute autre personne) à classer de manière normalisée la sensibilité éventuelle d'un élément de dossier;

— la difficulté à déterminer l'importance éventuelle d'une entrée unique dans un dossier de santé pour les soins futurs du patient et pour les classes d'utilisateurs;

— la nature logiquement indélébile du DSI et le besoin de gérer de manière rigoureuse les révisions des autorisations d'accès, de la même manière que les révisions des entrées du DSI elles-mêmes;

— le besoin de déterminer très rapidement un accès approprié, en temps réel et potentiellement dans un environnement informatique réparti;

— le niveau élevé de demandes exprimées par une minorité croissante de patients de voir leur consentement à la divulgation enregistré et respecté;

— le faible niveau de demandes relatives à ces exigences de la part de la majorité des patients, qui a historiquement limité l'engagement prioritaire à s'attaquer à cet aspect de la communication des DSI.

Afin de prendre en charge des DSI interopérables et des communications sans interruption des données du DSI entre les prestataires de soins de santé, il convient que la négociation exigée pour déterminer s'il convient qu'un demandeur quelconque de données de DSI reçoive les données puisse être automatisée. Si ce n'était pas possible, les délais et la charge de travail nécessaires à la gestion des décisions humaines pour toutes les communications de dossiers ou presque rendraient inutiles tout effort de permettre l'interopérabilité des données.

Les grands principes de l'approche du développement des normes dans le domaine du contrôle d'accès des communications de DSI consistent à faire correspondre les caractéristiques et les paramètres d'une demande et les politiques de l'émetteur du DSI, ainsi que tout contrôle d'accès ou déclaration de consentement dans le DSI spécifié, pour tenir à jour les preuves appropriées de la divulgation et permettre un traitement automatisé. Dans la pratique, des efforts sont en cours pour développer des normes internationales de définition de systèmes de contrôle d'accès et de gestion des privilèges qui soient capables de négociation entre ordinateurs. Ce type de travail est cependant fondé sur les services de santé qui se mettent d'accord sur un cadre mutuellement cohérent de définition des privilèges qu'ils souhaitent attribuer au personnel ainsi que sur le spectre de sensibilité qu'ils permettent aux patients de définir dans leurs DSI. Cela exige de la cohérence dans la manière d'exprimer les informations pertinentes, afin que cette sensibilité soit évolutive au moment de la définition (lors de l'ajout de nouvelles entrées au DSI), au moment de l'exécution (lorsqu'un DSI complet est récupéré ou interrogé) et qu'elle soit durable sur toute la durée de vie du patient. Il est important également de reconnaître que, dans un avenir prévisible, des différences continueront d'exister entre les pays sur des approches spécifiques de sécurisation des communications de DSI, dont des législations différentes, et qu'une approche fortement prescriptive de la normalisation n'est pas possible à l'heure actuelle.

Le présent document ne spécifie donc pas les règles d'accès elles-mêmes. Il ne spécifie pas à qui il convient de donner l'accès, à quoi et par quels mécanismes de sécurité; il convient que celles-ci soient déterminées par les communautés d'utilisateurs, les lignes directrices et la législation nationales. Elle définit un cadre de base qui peut être utilisé comme spécification minimale de la politique d'accès au DSI et une représentation générique plus riche pour la communication d'informations de politique plus détaillées. Ce cadre complète l'architecture générale définie dans l'ISO 13606-1 et définit les structures d'information spécifiques qui doivent être communiquées en tant que parties d'un EHR_EXTRACT, défini dans l'ISO 13606-1. Certains types d'accords nécessaires à la sécurité des communications de DSI sont inévitablement en dehors du domaine d'application du présent document et sont traités de manière plus complète dans l'ISO 22600 (Gestion de privilèges et contrôle d'accès).

Il convient de noter qu'il existe un certain nombre de dépendances explicites et implicites sur l'utilisation d'autres normes conjointement au présent document, pour la cohésion générale d'un déploiement de sécurité de l'information interopérable. Outre l'accord relatif à la série complète de normes appropriées, un régime d'assurance adapté semble nécessaire (lequel ne fait pas partie du domaine d'application du présent document).

© ISO 2019 – Tous droits réservés

0.3 Scénarios de communication

0.3.1 Flux de données

Les interfaces et les modèles de message exigés pour prendre en charge la communication de DSI constituent le sujet de l'ISO 13606-5. La description présentée ici est une vue d'ensemble du processus de communication permettant de montrer les interactions pour lesquelles des fonctions de sécurité sont nécessaires. La Figure 1 représente les flux de données principaux et les scénarios que le présent document doit envisager. Pour chaque flux de données principal, il existe une réponse d'accusé de réception et facultativement un rejet peut être retourné à la place des données demandées.

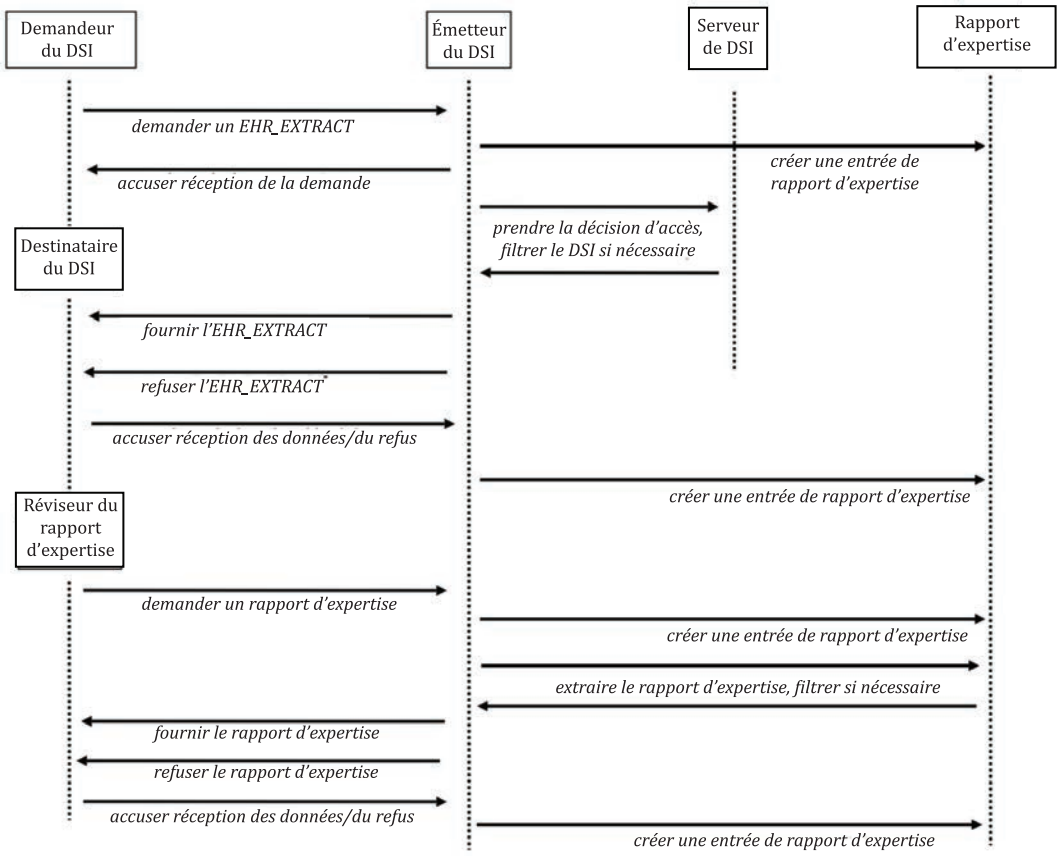


Figure 1 — Principaux flux de données et processus relatifs à la sécurité couverts par le présent document

Le demandeur du DSI, le destinataire du DSI et le réviseur du rapport d'expertise peuvent être des professionnels de santé, le patient, un représentant légal ou toute autre partie ayant les autorisations suffisantes pour accéder aux informations de soins de santé. L'EHR_EXTRACT comme le rapport d'expertise, s'ils sont fournis, peuvent devoir être filtrés pour limiter la divulgation afin de respecter les privilèges du destinataire. Cet aspect du contrôle d'accès sera discuté plus loin dans l'introduction (toutes les parties représentées ici, et pas uniquement l'émetteur du DSI, doivent tenir à jour un rapport d'expertise. Cependant, pour une meilleure lisibilité, les autres processus de rapport d'expertise ne sont pas représentés ni décrits ici.).

Les paragraphes qui suivent décrivent chaque flux de données de la Figure 1.

0.3.2 Demander des données de DSI

Cette interaction n'est pas toujours exigée (par exemple, les données de DSI peuvent être poussées de l'émetteur vers le destinataire comme dans le cas d'une lettre de sortie). L'interface de demande doit inclure un profil du demandeur suffisant pour permettre à l'émetteur du DSI de pouvoir prendre une décision d'accès, pour remplir un rapport d'expertise et fournir les données appropriées au destinataire

 © ISO 2019 – Tous droits réservés

prévu. Dans certains cas, le demandeur du DSI peut ne pas être la même partie que le destinataire du DSI, par exemple, un agent logiciel peut déclencher une notification contenant des données de DSI à envoyer à un professionnel de santé. Dans ce cas, ce sont les justificatifs du destinataire du DSI qui déterminent principalement la décision d'accès à prendre.

Une demande de DSI peut devoir inclure ou faire référence à des accords d'accès et des mandats de soins, par exemple par la fourniture d'une forme quelconque de consentement explicite de la part du patient ou d'un mandat de soins.

La négociation entre le demandeur et l'émetteur des données de DSI sera de plus en plus automatisée et il convient que les informations incluses dans cette interaction suffisent à permettre une négociation totalement informatisée.

Les exigences relatives à cette interaction sont reflétées par le modèle d'interface REQUEST_EHR_EXTRACT défini dans l'ISO 13606-5.

0.3.3 Générer une entrée de journal d'accès au DSI

Il s'agit d'une pratique prise pour hypothèse de tout système de DSI, mais elle n'est pas spécifiée en tant qu'interface normative en raison des nombreuses approches et capacités des systèmes actuels. L'interopérabilité des systèmes d'expertise internes de tout système de DSI n'est pas exigée, sauf pour la prise en charge du modèle défini à l'Article 8 du présent document et de l'interface correspondante définie dans l'ISO 13606-5.

0.3.4 Accuser réception de la demande de DSI

Aucune considération de sécurité spécifique aux soins de santé.

0.3.5 Prendre la décision d'accès, filtrer les données de DSI

Lors du traitement de la demande de DSI, les politiques relatives à l'émetteur du DSI et les politiques d'accès du DSI lui-même doivent toutes être prises en compte pour déterminer quelles données sont extraites du DSI cible. Le présent document ne peut pas dicter l'ensemble complet de politiques pouvant influencer l'émetteur du DSI, potentiellement dérivées de législations nationales, régionales, spécifiques à l'organisation, professionnelles et autres.

Une décision de filtrer les données de DSI sur la base de leur sensibilité et des privilèges du demandeur et du destinataire du DSI doit être conforme aux politiques concernées et peut devoir trouver l'équilibre entre les risques cliniques du refus d'accès à l'information et les risques médicolégaux relatifs à la divulgation de l'information.

Le présent document définit toutefois un cadre général de représentation interopérable des politiques d'accès qui peut concerner tout DSI particulier créé par le patient ou par ses représentants. Celles-ci peuvent ne pas être stockées dans le système de DSI physique de cette manière; elles peuvent par exemple être intégrées dans un serveur de politique relié au serveur de DSI.

Cette décision d'accès est discutée plus en détails à l'Article 7.

0.3.6 Refuser la fourniture de l'EHR_EXTRACT

Si la décision d'accès est un refus, un ensemble grossier de raisons doit être défini afin de développer un ensemble de raisons adaptées de la part de l'émetteur du DSI. Cependant, il est important que le refus et l'éventuelle raison donnée n'indiquent pas au destinataire que les données de DSI demandées n'existent pas. La simple divulgation de leur existence peut être dommageable pour un patient.

Aucune considération de sécurité spécifique aux soins de santé. Le modèle d'interface est défini dans l'ISO 13606-5.

0.3.7 Fournir l'EHR_EXTRACT

Il convient de noter que le destinataire du DSI peut ne pas être le même que le demandeur du DSI et que la fourniture d'un DSI peut ne pas avoir été déclenchée par une demande. Elle peut avoir été initiée par

© ISO 2019 – Tous droits réservés

l'émetteur dans le cadre d'un protocole de soins partagé ou pour ajouter de nouvelles données à un DSI existant.

Il est exigé que l'EHR_EXTRACT soit conforme au modèle de référence défini dans l'ISO 13606-1 et au modèle d'interface défini dans l'ISO 13606-5.

L'EHR_EXTRACT doit inclure ou faire référence à toute politique d'accès pertinente, représentée conformément au présent document, pour orienter toute propagation à venir des données de DSI communiquées. Les politiques ne peuvent être référencées que si le destinataire du DSI est connu comme ayant un accès direct aux mêmes informations par d'autres moyens.

0.3.8 Accuser réception de l'EHR_EXTRACT

Aucune considération de sécurité spécifique aux soins de santé.

0.3.9 Générer une entrée de journal d'accès au DSI

Comme décrit en 0.3.3.

0.3.10 Demander à voir le journal d'accès au DSI

Permettre à un patient de découvrir qui a eu accès à tout ou partie de son DSI dans un environnement de partage des informations est aujourd'hui considéré comme une pratique souhaitable. Le domaine d'application de cette interface, tel que défini dans le présent document, consiste à demander à voir le rapport d'expertise qui informe le destinataire de qui a accédé à quelles parties de son DSI dans un système de DSI donné et quand. Cette interface n'est pas destinée à prendre en charge les situations dans lesquelles un contrôle complet d'un rapport d'expertise est exigé à des fins légales ou pour d'autres investigations. Cette interface est expliquée à l'Article 6.

Le modèle d'interface est défini dans l'ISO 13606-5.

0.3.11 Générer une entrée de journal d'accès au DSI

Comme décrit en 0.3.3.

0.3.12 Fournir le journal d'accès au DSI

Il s'agit d'une pratique souhaitable qui exige une représentation interopérable de cette entrée (ou de cet ensemble d'entrées). Cette interface est expliquée à l'Article 6.

Bien qu'une investigation légale exige qu'un rapport d'expertise soit fourni sous forme complète et non modifiée, la présentation d'un rapport d'expertise à un patient ou à un professionnel de santé peut exiger de filtrer certaines entrées (par exemple celles qui font référence à des données du DSI auxquelles le patient n'a pas accès).

Le modèle d'interface est défini dans l'ISO 13606-5.

0.3.13 Refuser le journal d'accès au DSI

Si la demande n'est pas satisfaite, il est nécessaire de définir un ensemble grossier de raisons. Cependant, il est important que le refus et l'éventuelle raison donnée n'indiquent pas au destinataire que les données de DSI demandées n'existent pas. La simple divulgation de leur existence peut être dommageable pour un patient.

Aucune considération de sécurité spécifique aux soins de santé. Le modèle d'interface est défini dans l'ISO 13606-5.

0.3.14 Accuser réception du journal d'accès au DSI

Aucune considération de sécurité spécifique aux soins de santé.

0.3.15 Générer une entrée de journal d'accès au DSI

 © ISO 2019 – Tous droits réservés

Comme décrit en 0.3.3.

0.4 Exigences et approche technique

0.4.1 Exigences générales relatives à la sécurité des soins de santé

Les exigences les plus largement acceptées pour une approche générale de sécurité dans les domaines traitant de données sensibles et personnelles sont publiées dans l'ISO/IEC 27002. Celle-ci spécifie les types de mesures qu'il convient de prendre pour protéger les biens tels que les données de DSI et les manières de communiquer ces données en sécurité dans le cadre d'un environnement informatique réparti. Un guide spécifique à la santé pour la présente norme générale a été publié dans l'ISO 27799 (Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002). Celui-ci facilite la formulation de politiques de sécurité communes en soins de santé, et il est censé promouvoir l'adoption de composants et de services de sécurité interopérables. L'ISO 22600 (Informatique de santé — Gestion de privilèges et contrôle d'accès) définit une approche architecturale complète de définition et de gestion formelles et cohérentes de ces politiques. 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.

Les exigences de sécurité précises qui doivent être satisfaites pour autoriser une instance de communication de DSI particulière dépendent d'un certain nombre de politiques nationales et locales sur les sites d'envoi et de réception et au niveau de tous les liens intermédiaires sur la chaîne de communication. Beaucoup de ces politiques s'appliquent aux communications de soins de santé en général et varient selon les pays et les contextes médicaux d'une manière qu'il convient que le présent document ne définisse pas et qu'il ne peut pas définir. L'approche prise lors de la rédaction du présent document a donc consisté à prendre pour hypothèse que les politiques, composants et services de sécurité généraux contribuent à une phase de négociation (la *décision d'accès*) avant de sanctionner la communication d'un extrait de DSI et protègent les flux de données effectifs du DSI.

Le présent document prend par conséquent pour hypothèse qu'une politique ou un ensemble de politiques de sécurité générale conforme à l'ISO 27799 est en place sur tous les sites participant à une communication de DSI et que ces politiques sont conformes aux législation nationales ou internationales sur la protection des données. Des politiques supplémentaires peuvent être exigées pour la conformité aux règlementations spécifiques nationales, locales, professionnelles ou de l'organisation, applicables à la communication ou à l'utilisation de données de DSI. La définition de ces politiques ne fait pas partie du domaine d'application du présent document.

0.4.2 Relations avec d'autres normes de sécurité

L'accès légitime aux données du DSI est déterminé par une large gamme de politiques, dont certaines peuvent exister sous forme de documents, certaines sont codées dans des applications et certaines dans des composants de systèmes d'autorisation formels. Il est connu que les fournisseurs et les organisations diffèrent dans leur manière de mettre en œuvre les politiques et les services de contrôle d'accès et leur degré d'informatisation actuel.

L'ISO 22600 (toutes les parties) définit un modèle logique générique pour la représentation des privilèges des acteurs principaux (entités), des politiques de contrôle d'accès relatives à des objets cibles potentiels et du processus de négociation exigé pour parvenir à une décision d'accès. La Figure 2 représente les concepts du contrôle d'accès basé sur les rôles défini dans l'ISO 22600 (toutes les parties).

© ISO 2019 – Tous droits réservés

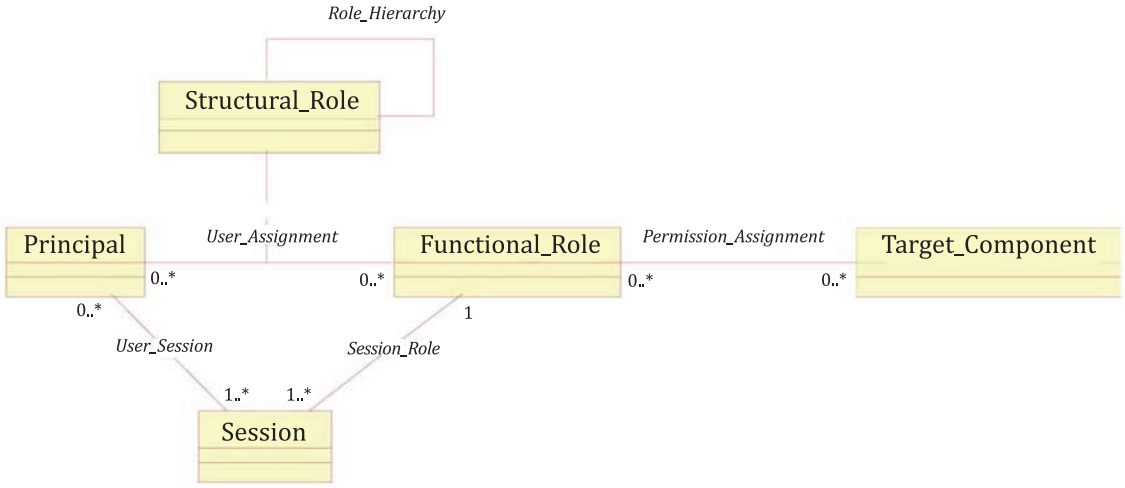


Figure 2 — Principaux concepts et types de politiques définis dans le contrôle d'accès basé sur les rôles [ISO 22600 (toutes les parties)]

Avec la définition des contraintes sur les rôles, les processus, les objets cibles et les privilèges associés par les politiques, la Figure 2 devient la Figure 3, conformément à l'ISO 22600 (toutes les parties).

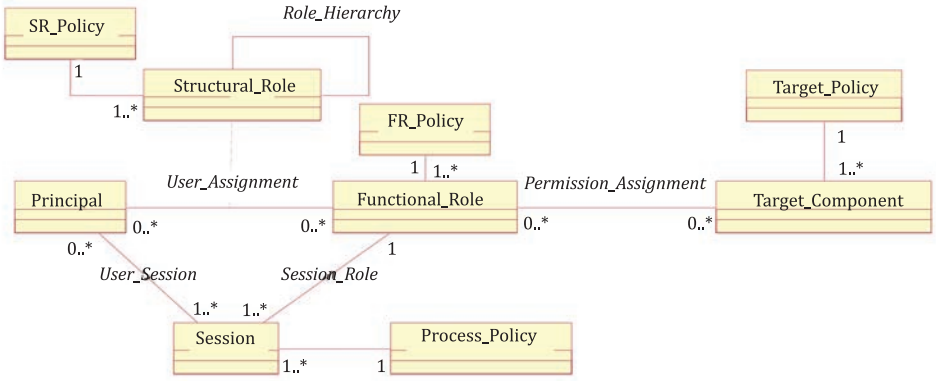


Figure 3 — Schéma RBAC selon la politique

Comme illustré sur la Figure 3, les acteurs principaux (personnes, agents, etc.) sont mis en correspondance avec un ou plusieurs rôles fonctionnels qui sont influencés par les rôles structurels qu'ils sont autorisés à tenir. Par exemple, une personne médicalement qualifiée et un spécialiste en pédiatrie peuvent tenir un ou plusieurs rôles structurels (comme pédiatre consultant dans un hôpital, responsable du dépistage chez les enfants pour la région). Ces rôles structurels peuvent permettre à la personne de tenir à certains moments le rôle fonctionnel de clinicien personnel envers un patient. Le rôle fonctionnel peut être permanent ou limité à une seule session d'utilisateur. Les rôles fonctionnels sont mis en correspondance avec des permissions d'exécuter des opérations particulières (comme la saisie de nouvelles entrées dans le DSI) et avec des objets particuliers (par exemple les données du DSI que le détenteur du rôle est autorisé à voir).

Aux fins du présent document, la classe Target_Component représentée sur la Figure 3 représente les données du DSI détenues par l'émetteur du DSI. L'association Permission_Assignment définit les politiques qui autorisent ou refusent l'accès à tout ou partie du DSI, qui doivent également être communiquées au destinataire du DSI pour adoption et propagation ultérieures. Bien que le présent document prenne pour hypothèse l'adoption de la norme, il est reconnu que les structures et la terminologie fonctionnelles nationales peuvent différer et que des variantes sont possibles. Le présent document spécifie toutefois uniquement le modèle de politique en tant que cadre de communication

 © ISO 2019 – Tous droits réservés

interopérable des politiques d'accès réelles. Il ne définit pas lui-même le contenu des politiques d'accès qui doivent être déterminées au niveau juridictionnel ou plus local.

En tant que complément de la présente norme, l'ISO 21298 définit les ensembles de rôles structurels et de rôles fonctionnels qui peuvent être utilisés à l'international pour prendre en charge la négociation et la mise en relation des politiques (par exemple pendant la phase de négociation d'une décision d'accès). Le présent document prend également pour hypothèse l'adoption de cette norme et s'aligne sur elle.

La relation entre le modèle de politique défini dans le présent document et le système de classification de confidentialité et de sécurité des soins de santé HL7 est expliquée à l'Annexe B.

L'ISO 27789 définit une représentation complète des informations de rapport d'expertise et d'historique d'expertise relatives à tous les évènements qui peuvent se produire dans les systèmes de dossier de santé informatisé de santé. Cela inclut la communication des données du DSI entre les référentiels et les systèmes. Le présent document prend pour hypothèse la conformité à cette norme et définit un profil (sous-ensemble) du modèle de rapport d'expertise de l'ISO 27789 spécifiquement destiné à la communication avec les patients et les autres parties autorisées des informations indiquant qui a accès au DSI d'un patient spécifique, quand et pourquoi.

Un grand nombre d'exigences médicolégales et éthiques spécifiques au DSI sont exprimées dans l'ISO 18308, bien que la conformité avec celles-ci soit principalement satisfaite par l'intermédiaire des classes et attributs spécifiques du modèle de référence de DSI (publié dans l'ISO 13606-1). La norme ISO 13606 dans son entier permet la conformité à l'ISO 18308 et le présent document permet spécifiquement la conformité à ses exigences éthiques et légales et à ses principes d'information juste.

0.5 Modèle de politique d'accès au DSI

0.5.1 Approche générale

Dans le modèle de référence de l'ISO 13606-1, chaque COMPOSITION dans l'EHR_EXTRACT inclut un attribut access_policy_id facultatif pour permettre de faire référence à ces politiques à tout niveau de détail dans la hiérarchie d'imbrication du DSI. Chaque COMPOSITION peut par conséquent référencer tout nombre de politiques d'accès ou de déclarations de consentement qui définissent les privilèges nécessaires prévus ainsi que les profils des acteurs principaux (utilisateurs, agents, logiciels, dispositifs, délégués, etc.) pour y accéder. Le modèle d'information de l'Article 7, destiné à la représentation et à la communication des informations de politique d'accès, a été délibérément gardé très général pour permettre la diversité des critères de politiques stipulées dans différents pays et différents réseaux régionaux de soins de santé. Des vocabulaires normalisés sont définis sous forme de listes de termes par défaut pour certaines des principales propriétés du modèle. Bien qu'il soit recommandé de les adopter dès lors qu'elles sont adaptées, il est reconnu que les juridictions peuvent posséder des exigences, des législations ou des investissements existants qui signifient qu'elles ne peuvent pas adopter ces listes de termes internationales normalisées. Le présent document autorise par conséquent les juridictions à déclarer la conformité au moyen de listes de termes alternatives.

Les environnements de santé et de soins comprennent des réseaux de plus en plus complexes d'agences et d'acteurs de milieux de soins de santé classiques, d'aide sociale, de prestataires et d'agences informels et bénévoles (comme les organismes caritatifs d'aide sociale), comprenant également les patients eux-mêmes, les familles et quelquefois leurs réseaux sociaux. Tous ces acteurs peuvent par moments établir des accords pour permettre le partage de données de santé personnelles. Étant donnée la nature dynamique de cette «équipe de soins virtuelle», il peut se révéler peu pratique de négocier ces accords de partage de données de manière classique à base de documents échangés entre les personnes. Il est donc probable que ces agences établissent des accords-cadres qui spécifient à l'avance les normes auxquelles chacune se conforme, toutes les correspondances entre leurs domaines de privilèges respectifs et la manière dont les données doivent être gérées dans chacun de ces domaines de privilèges. Comme indiqué ci-dessus, ce modèle de politique permet à la place aux juridictions de déclarer les listes de termes alternatives qu'elles utilisent. Cela permet une certaine flexibilité dans l'adoption du présent document, qui reconnaît que des environnements complexes de partage de données peuvent devoir établir de nouveaux vocabulaires potentiellement plus riches pour décrire la gamme plus large d'acteurs et de rôles dans cet environnement.

© ISO 2019 – Tous droits réservés

Un certain nombre de systèmes existants et hérités peuvent ne pas pouvoir intégrer des spécifications de politiques riches en définitions et de nombreuses régions de soins de santé peuvent ne pas être en mesure de définir ces politiques pendant quelques années. Par conséquent, en tant que complément au modèle de politique général de l'Article 7, le présent document définit deux vocabulaires qui peuvent fournir une base minimale pour une prise de décision relative à la politique d'accès et garantir une interopérabilité de politique d'accès de base, bien qu'à un niveau relativement grossier.

Ces deux vocabulaires sont les suivants:

a) une classification de la sensibilité des données du DSI (au niveau de COMPOSITION);

b) une classification de haut niveau des demandeurs et des destinataires de DSI, par le biais d'un ensemble de rôles fonctionnels.

0.5.2 Définition du «besoin de connaître» dans le traitement des données de DSI

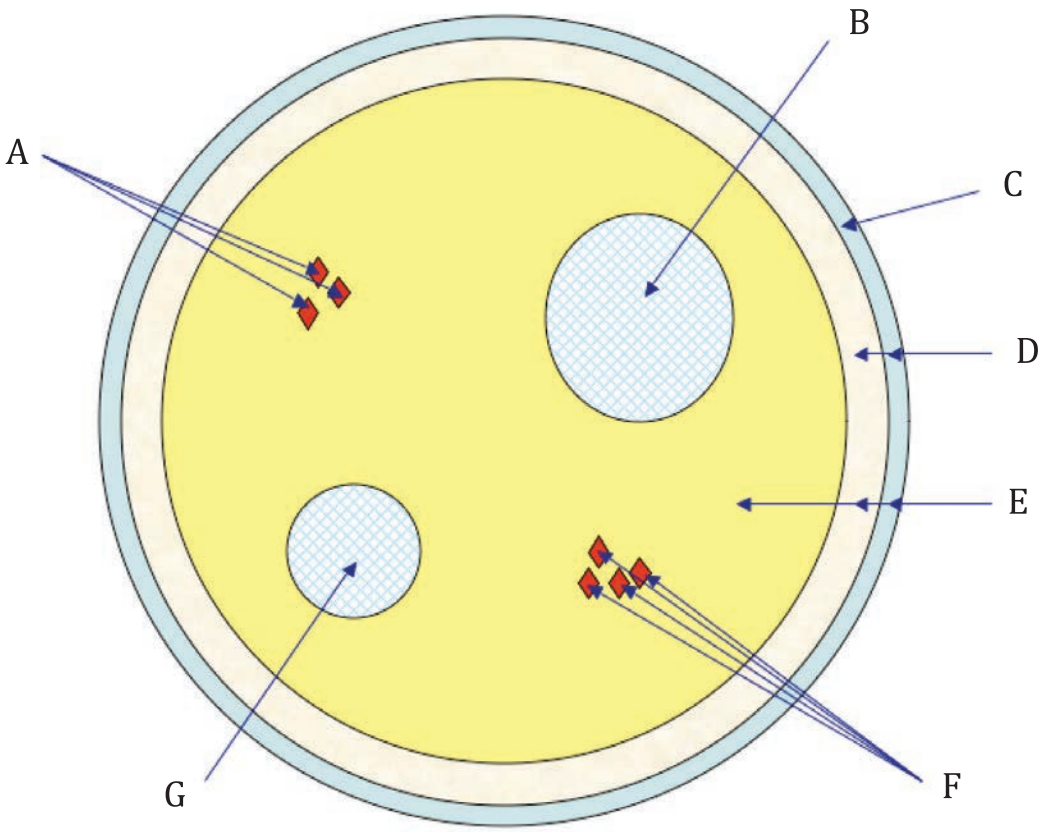
Dans de nombreux environnements de soins de santé (dans et entre des équipes de soins de santé qui collaborent dans la mise à disposition directe de soins aux patients), la norme est de partager les informations du dossier de santé de manière ouverte. La grande majorité des patients souhaite que cela se passe ainsi et de nombreux patients sont en fait surpris du fait que leur dossier de santé soit peu partagé aujourd'hui lorsqu'il conviendrait de le partager plus pour la sécurité et la continuité des soins.

Quelques systèmes actuels de soins de santé (sous format papier ou électronique) définissent des cloisonnements de contrôle d'accès internes complexes des dossiers de santé qu'ils contiennent. Même s'il est considéré comme utile de définir de nombreuses politiques d'accès finement définies, dans la pratique les systèmes de soins de santé, les services de santé nationaux et les millions de patients pourraient avoir besoin de beaucoup de temps pour spécifier des politiques de contrôle d'accès adaptées à toutes leurs données de DSI et pour mettre en œuvre des composants logiciels aptes à exécuter de nombreux calculs complexes de mise en relation des politiques en temps réel. La maintenance de ces politiques à mesure que les exigences de soins médicaux relatives à chaque patient évoluent représente elle aussi un processus complexe.

Tandis qu'une suite de politiques d'accès peut être définie en théorie (par les patients ou par d'autres) pour offrir un cadre à plusieurs niveaux d'accès dans tout DSI donné, dans la pratique la plupart des milieux médicaux opèrent sur la base de privilèges par défaut accordés dans le dossier de santé à tout professionnel de soins de santé ou médical ayant un intérêt légitime pour le patient. (La définition des personnes ayant un intérêt légitime varie selon les organisations et ne fait pas partie du domaine d'application du présent document.) Cependant, il est également bien accepté que les patients et les professionnels puissent avoir besoin par moments de restreindre l'accès à certaines données du DSI plus personnelles et sensibles. Il est courant également dans la plupart des services de santé d'isoler certains milieux médicaux comme contenant des parties exclusives d'un DSI (par exemple les cliniques de santé sexuelle).

Ce type d'isolement de milieux médicaux ou le marquage des données du DSI comme particulièrement sensibles est tout à fait distinct de toute subdivision du DSI qui peut être définie pour aider à la navigation et au flux de travail dans les spécialités médicales, par exemple en définissant des parties relatives au cancer ou au diabète dans le DSI. La Figure 4 propose une représentation de la manière dont un DSI peut être subdivisé logiquement du point de vue du besoin de connaître, la classification de la confidentialité (sensibilité) étant représentée au moyen de classes d'utilisateurs et pour des contextes de soins particuliers.

 © ISO 2019 – Tous droits réservés



Légende

A entrées privées partagées avec le MG
B entrées restreintes à l'équipe de santé sexuelle
C entrées accessibles au personnel administratif
D entrées accessibles au personnel de soutien médical
E entrées accessibles aux équipes de soins directs
F entrées privées partagées avec plusieurs parties nommées
G entrées restreintes aux services de santé en prison

Figure 4 — Représentation des domaines d'accès dans un exemple de DSI

Dans cette représentation, il est pris pour hypothèse que le patient dispose d'un accès complet à son DSI. La majorité du DSI de ce patient est accessible à toute partie fournissant des soins médicaux directs. Cependant, le DSI contient plusieurs entrées privées; certaines sont restreintes au médecin généraliste (de famille) du patient et certaines à une liste distincte de parties nommées. Le DSI contient également certaines entrées créées par et restreintes à une clinique de santé sexuelle et d'autres restreintes au service de santé d'une prison. Les deux ne sont accessibles qu'aux parties disposant des privilèges supplémentaires relatifs au sous-domaine (le patient peut toutefois nommer d'autres parties pouvant accéder à ces sous-ensembles du DSI s'il le souhaite). L'un des aspects des privilèges est l'attribution par une organisation de rôles à un clinicien pouvant être tenus en cas d'urgence et qui confèrent des privilèges qui excèdent ceux de son rôle normal. Ces cas d'urgence peuvent par exemple donner accès à un plus grand nombre de dossiers de patients que le nombre habituel aux soins du clinicien (cette utilisation du statut d'urgence doit être spécifiquement signalée et régulièrement revue).

Certaines parties du DSI sont délibérément accessibles également au personnel de soutien médical qui peut devoir revoir certaines conclusions médicales afin d'exécuter des tâches telles que la planification ou la réalisation d'investigations. Une très petite partie de cet exemple de DSI a également été rendue

© ISO 2019 – Tous droits réservés

accessible au personnel administratif. Les commis aux rendez-vous, secrétaires et porteurs ont tous besoin de connaître certains faits à propos d'un patient afin de jouer leur rôle dans la fourniture générale de soins efficaces, comme par exemple savoir qu'un patient a des besoins spéciaux d'assistance judiciaire ou qu'il aura besoin de 24 % d'oxygène et d'un fauteuil roulant afin d'être transporté au service de radiologie.

Cet exemple n'illustre pas la façon dont les patients peuvent être exclus de l'accès à certaines parties du DSI mais ces dispositions peuvent être stipulées au moyen du cadre général de politique de l'Article 7, si la législation sur la protection des données le permet. Des données de DSI fournies à titre confidentiel par un parent du patient peuvent être un exemple de ce cas.

Bien qu'un ensemble de politiques richement définies puisse être développé pour des types spécifiques de patients, des contextes spécifiques ou simplement parce qu'un patient peut être plus concerné par son DSI qu'un autre, l'adoption de solutions de DSI réparties doit être gérée en se basant sur le fait qu'un ensemble de défauts sensible et un cadre simple parviendront à satisfaire la majorité des cas dans un avenir proche. La raison en est qu'un ensemble de politiques trop développé peut ne pas pouvoir être interprété et directement intégré dans le système de DSI d'un destinataire de DSI, même si les informations de ces politiques peuvent être communiquées de manière normalisée.

Outre la représentation générique des informations de politique d'accès au DSI, le présent document définit également, par conséquent, une spécification pour une base minimale de communication de la sensibilité de données de DSI dans un EHR_EXTRACT, en spécifiant la sensibilité des COMPOSITION à l'intérieur de celui-ci conformément à la classification définie en 6.1. Cette classification correspond aux divers sous-domaines de données de DSI représentés sur la Figure 4.

Dans la pratique, tout système de DSI donné peut disposer d'autres mécanismes pour indiquer la sensibilité des données de DSI ou un concept équivalent. Le présent document n'exige pas que les systèmes de DSI stockent les données en fonction des niveaux de sensibilité définis en 6.1 mais qu'ils puissent établir des correspondances avec cette classification lors de la génération d'un EHR_EXTRACT.

0.5.3 Rôles fonctionnels d'accès aux données de DSI

Afin de prendre une décision d'accès, le profil et le but d'un destinataire de DSI proposé doivent être mis en correspondance avec les politiques s'appliquant au DSI détenu par l'émetteur de DSI, dont la sensibilité des RECORD_COMPONENT spécifiques qui ont été demandés.

Le profil du demandeur et/ou du destinataire doit donc être spécifié de manière interopérable. Comme discuté ci-dessus, les exigences, la législation, les attributs et les vocabulaires utilisés à cette fin varient dans chaque pays et ne peuvent pas encore être normalisés.

Cependant, afin de permettre un niveau d'interopérabilité de base, la conformité minimale au présent document exige, soit que toute demande d'un EHR_EXTRACT inclue, dans le cadre de la spécification de la demande, le rôle fonctionnel du destinataire de DSI prévu, comme défini en 6.2 et correspondant à ceux définis dans l'ISO 21298, soit que soit utilisé une liste de termes alternative spécifiée par une juridiction.

La corrélation entre le rôle fonctionnel et la sensibilité du DSI, en vue d'accorder ou de refuser une demande d'accès, ou de filtrer l'EHR_EXTRACT est définie en 6.3.

Cette correspondance offre un moyen basique (grossier) de limiter le domaine d'application de l'accès au DSI conformément au type de partie qui fait la demande d'accès. Une plus grande sophistication peut toujours être ajoutée dans les situations dans lesquelles une spécification interopérable du profil du demandeur a été définie au niveau local ou national. Une illustration de la façon dont cette mise en correspondance basique peut être combinée avec un petit nombre de spécifications supplémentaires afin de spécifier un ensemble relativement riche de contraintes d'accès est donnée à l'Annexe A.

0.6 Interopérabilité du rapport d'expertise

Il est largement reconnu que les détails des interactions avec un système de DSI doivent être conservés à des fins d'expertise. Cependant, la manière dont ces types de rapports d'expertise sont mis en œuvre est assez spécifique à chaque système de DSI, qui est en partie déterminée par l'approche de persistance

 © ISO 2019 – Tous droits réservés

(comme le stockage de la base de données) adoptée et peut également être orientée en partie par la législation locale ou nationale.

Les exigences relatives aux historiques d'expertise de DSI sont spécifiées dans l'ISO 27789:2013 Informatique de santé — Historique d'expertise des dossiers de santé informatisés. Cette norme spécifie un cadre commun pour les historiques d'expertise pour les DSI, en termes d'évènements déclencheurs et de données d'expertise, permettant de conserver l'ensemble complet d'informations de santé personnelles qui peuvent être expertisées dans les systèmes et les domaines d'information.

Cependant, la preuve est faite de jour en jour que la possibilité pour les patients de revoir les informations sur l'accès à leurs données de DSI, non seulement est un droit légitime mais encourage effectivement un comportement moral parmi les professionnels de santé qui accèdent alors uniquement aux dossiers qu'ils ont réellement besoin de voir. Bien que les systèmes de DSI individuels puissent offrir un certain degré d'accès au rapport d'expertise, cet accès est aujourd'hui généralement fourni aux administrateurs de bases de données au moyen d'outils et d'interfaces qui ne sont pas adaptés à la possibilité pour les patients de consulter l'historique d'accès à leur propre DSI. Dans un scénario de DSI réparti (partagé), le DSI et les journaux d'accès au DSI sont inévitablement répartis également.

Une spécification interopérable est donc exigée pour un ensemble basique de données pouvant être fournies en réponse à une demande (de la part d'un patient ou de son représentant) de la liste des accès au DSI (contenue dans un système de DSI). Elle est donc définie à la fois comme modèle d'information de revue de rapport d'expertise dans le présent document et comme modèle d'interface demande-réponse dans l'ISO 13606-5. Puisque les futurs systèmes de DSI et systèmes de consignation de rapports d'expertise seront de plus en plus conformes à l'ISO 27789 et peuvent donc posséder des modèles de données internes et/ou des interfaces qui reflètent sa structure, le modèle de rapport d'expertise de l'Article 8 du présent document inclut les informations de mise en correspondance avec l'ISO 27789. Toutes les propriétés du modèle de rapport d'expertise du présent document n'ont pas de correspondance avec l'ISO 27789, car certains détails décrivant le type de données de DSI accédées devront être tirés du système de DSI lui-même.

Cette demande de rapport d'expertise n'est pas destinée à constituer le moyen par lequel un rapport d'expertise est examiné dans le cadre d'une investigation formelle des accès à un système de DSI ni le moyen pour des communications interopérables entre les systèmes d'historique d'expertise.

© ISO 2019 – Tous droits réservés

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

1 Domaine d'application

Le présent document décrit une méthodologie permettant de spécifier les privilèges nécessaires pour accéder aux données de DSI. Cette méthodologie forme une partie de l'architecture générale de communication de DSI définie dans l'ISO 13606-1.

Le présent document cherche à traiter uniquement les exigences relatives aux communications de DSI et à représenter et communiquer les informations spécifiques au DSI qui permettent de prendre une décision d'accès. Elle fait également référence aux exigences de sécurité générale qui s'appliquent aux communications de DSI et signale des solutions techniques et des normes qui spécifient les détails de services répondant à ces besoins de sécurité.

NOTE Les exigences de sécurité pour les systèmes de DSI non associées à la communication de DSI ne relèvent pas du domaine d'application du présent document.

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 13606-1, *Informatique de santé — Communication du dossier de santé informatisé — Partie 1: Modèle de référence*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 13606-1, 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 http://www.electropedia.org/.

3.1
autorité
entité responsable de l'émission des certificats

Note 1 à l'article: La présente spécification distingue deux types d'autorité: l'autorité de certification qui émet des certificats à clé publique et l'autorité de certificats d'attribut qui émet des certificats d'attribut.

© ISO 2019 – Tous droits réservés