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.

— 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).

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.

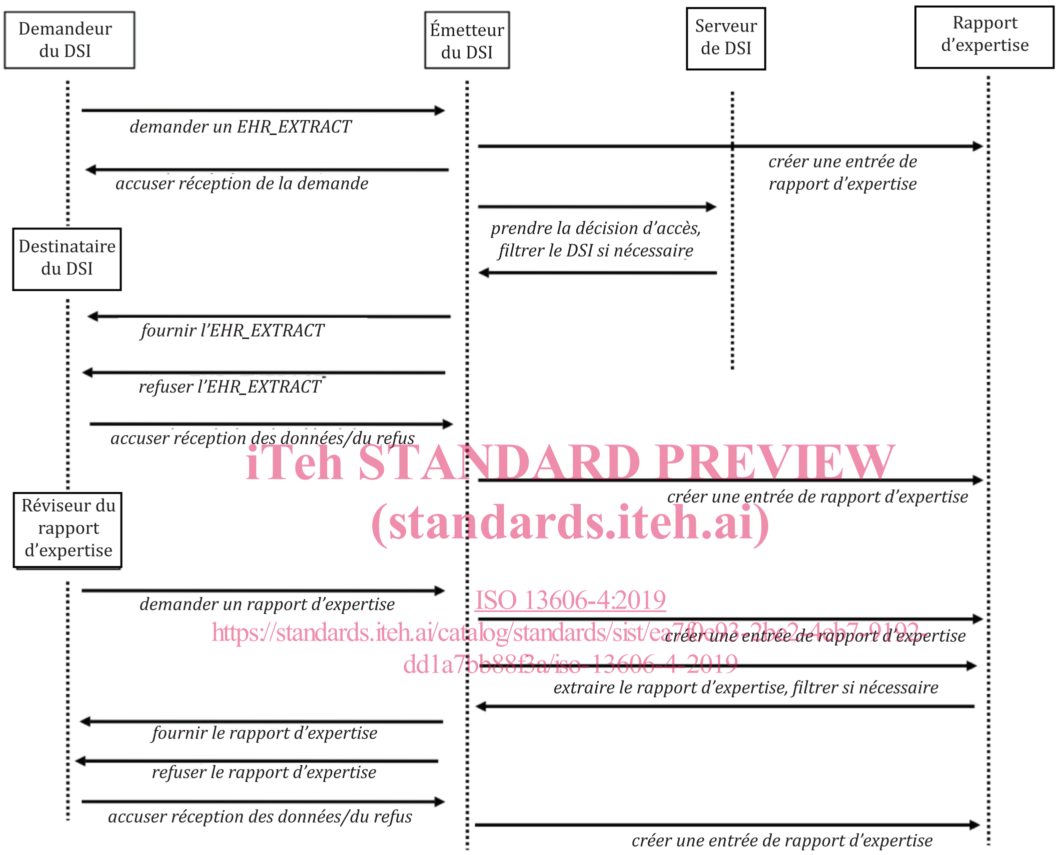

Figure 1 — Principaux flux de données et processus relatifs à la sécurité couverts par le présent document

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

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

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

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).

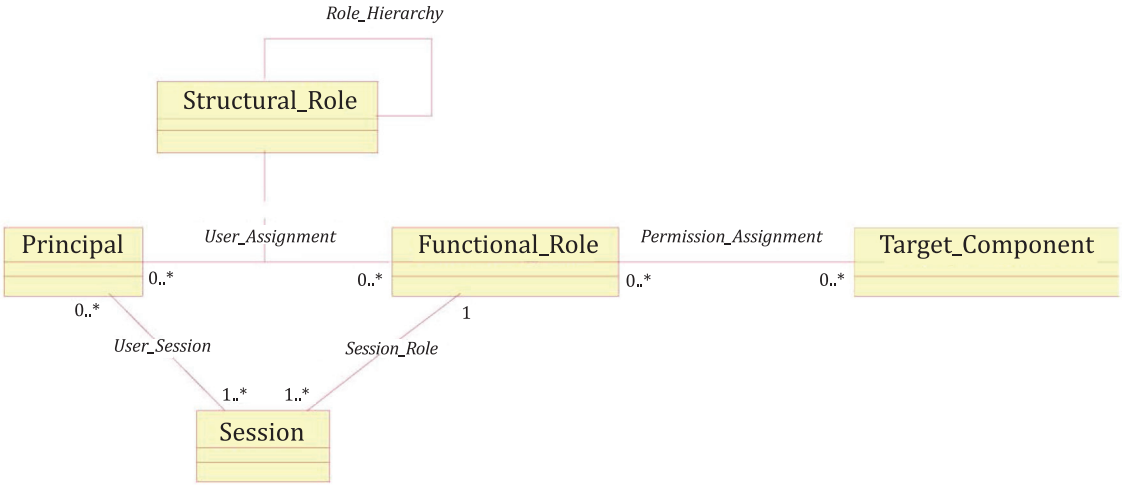

Figure 2 — Principaux concepts et types de politiques définis dans le contrôle d'accès basé sur les rôles [ISO 22600 (toutes les parties)]

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).

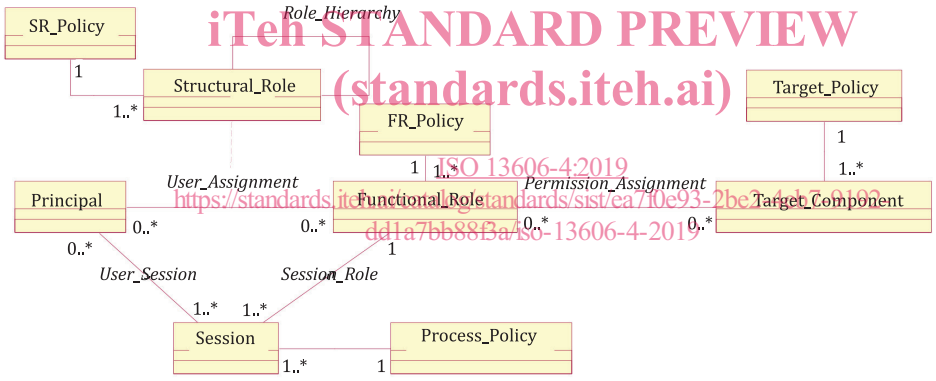

Figure 3 — Schéma RBAC selon la politique

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

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.