PROJET DE NORME INTERNATIONALE

ISO/DIS 25237

ISO/TC **215**	Secrétariat: **ANSI**
Début de vote: **2015-09-03**	Vote clos le: **2015-12-03**

Informatique de santé — Pseudonymization

Health informatics — Pseudonymisation

ICS: 35.240.80

TRAITEMENT PARRALLÈLE ISO/CEN

Le présent projet a été élaboré dans le cadre de l'Organisation internationale de normalisation (ISO) et soumis selon le mode de collaboration **sous la direction de l'ISO**, tel que défini dans l'Accord de Vienne.

Le projet est par conséquent soumis en parallèle aux comités membres de l'ISO et aux comités membres du CEN pour enquête de cinq mois.

En cas d'acceptation de ce projet, un projet final, établi sur la base des observations reçues, sera soumis en parallèle à un vote d'approbation de deux mois au sein de l'ISO et à un vote formel au sein du CEN.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

Numéro de référence
ISO/DIS 25237:2015(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 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 appelée 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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant : Avant-propos — Informations supplémentaires.

Le comité chargé de l'élaboration du présent document est l'ISO/TC 215, *Informatique de santé*. L'ISO/TS 25237 a été élaborée par le comité technique ISO/TC 215, *Informatique de santé*.

Introduction

La pseudonymisation est reconnue comme une méthode importante de protection des informations de santé à caractère personnel. Les services associés peuvent être utilisés aussi bien au plan national que pour la communication transfrontière.

Les domaines d'application concernent, sans s'y limiter, les secteurs suivants :

— l'utilisation indirecte des données cliniques (par exemple, la recherche) ;

— les essais cliniques et la surveillance post-marketing ;

— les soins pseudonymes ;

— les systèmes d'identification des patients ;

— la surveillance et l'évaluation de la santé publique ;

— les dossiers confidentiels sur la sécurité des patients (par exemple, les effets indésirables d'un médicament) ;

— les rapports comparatifs fondés sur des indicateurs de qualité ;

— le contrôle par les pairs ;

— les groupes de consommateurs ;

— l'assistance technique.

La présente Spécification technique fournit un modèle conceptuel des aspects en jeu, des exigences en matière de pratiques fiables ainsi que des spécifications pour la planification et la mise en œuvre des services de pseudonymisation.

La spécification d'un workflow général et d'une politique en matière d'opérations fiables servira de guide général pour la mise en œuvre ainsi qu'à des fins d'assurance qualité, et aidera l'utilisateur des services de pseudonymisation à déterminer la confiance qu'il peut accorder aux prestations assurées. Ce guide permettra aux organismes d'éducation d'exécuter eux-mêmes des services de pseudonymisation, avec des compétences suffisantes pour atteindre le degré voulu de qualité et de réduction des risques.

Informatique de santé — Pseudonymisation

1 Domaine d'application

La présente Spécification technique établit un certain nombre de principes et d'exigences visant à garantir la protection de la vie privée, grâce à des services de pseudonymisation ayant pour objet de protéger les informations de santé à caractère personnel. La présente Spécification technique est applicable aux organismes qui souhaitent s'engager dans des processus de pseudonymisation pour eux-mêmes et aux organismes qui se déclarent dignes de confiance pour engager des opérations dans des services de pseudonymisation.

La présente Spécification technique :

— définit un concept de base pour la pseudonymisation ;

— donne une vue d'ensemble des différents cas d'utilisation où l'opération de pseudonymisation peut être réversible ou irréversible ;

— définit une méthodologie de base pour les services de pseudonymisation, y compris au niveau des aspects organisationnels et techniques ;

— fournit un guide pour l'évaluation des risques en cas de ré-identification ;

— spécifie un cadre politique et des exigences minimales en matière de pratiques fiables pour un service de pseudonymisation ;

— spécifie un cadre politique et des exigences minimales pour la ré-identification contrôlée.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

IHE Healthcare De-Identification Handbook: 2014

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
contrôle d'accès
ensemble des moyens garantissant que seules les entités autorisées peuvent accéder aux ressources d'un système informatique, et seulement d'une manière autorisée

[ISO/IEC 2382-8:1998, définition 08.04.01]

3.2
anonymisation
processus par lequel des données à caractère personnel sont altérées irréversiblement, de telle façon que la personne concernée ne puisse plus être identifiée, directement ou indirectement, par le responsable du traitement des données, seul ou en collaboration avec une autre partie

NOTE Ce concept est absolu et peut, dans la pratique, être difficile à mettre en œuvre.

NOTE Adapté de l'ISO/IEC 29100:2011, Technologies de l'information — Techniques de sécurité — Cadre privé.

3.3
données anonymisées
données de sortie produites par un processus d'anonymisation

NOTE Adapté de l'ISO/IEC 29100:2011, Technologies de l'information — Techniques de sécurité — Cadre privé.

3.4
identifiant anonyme
identifiant d'une personne ne permettant pas d'identifier la personne physique

3.5
authentification
établissement de la validité de l'identité déclarée

3.6
attaquant
personne cherchant à exploiter les vulnérabilités potentielles d'un système biométrique
[ISO/IEC 19792:2009(en)]

3.7
cryptogramme, texte chiffré
données résultant d'un chiffrement et dont le contenu sémantique n'est pas disponible sans recours à des techniques cryptographiques

[ISO/IEC 2382-8:1998, définition 08.03.08]

3.8
confidentialité
propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés

[ISO 7498-2:1989, définition 3.3.16]

3.9
clé de chiffrement de contenu
clé cryptographique utilisée pour chiffrer le contenu d'une communication

3.10
responsable du traitement
personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel

3.11
cryptographie
discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée

[ISO 7498-2:1989, définition 3.3.20]

3.12
algorithme cryptographique
⟨chiffre⟩ méthode permettant de transformer des données dans le but d'en masquer la quantité d'information, d'empêcher que la modification de celle-ci ne soit pas détectée et/ou d'en prévenir une utilisation non autorisée

3.13
gestion de clés
gestion de clés cryptographiques
production, stockage, distribution, suppression, archivage et application de clés conformément à la **politique de sécurité** (3.43)

[ISO 7498-2:1989, définition 3.3.33]

3.14
intégrité des données
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[ISO 7498-2:1989, définition 3.3.21]

3.15
liage de données
appariement et combinaison de données issues de plusieurs bases de données

3.16
protection des données
organisation technique et sociale permettant de négocier, gérer et garantir le caractère privé et la sécurité des informations

3.17
personne concernée
personne à laquelle se rapportent les données

3.18
déchiffrement
reconstitution, à partir d'un cryptogramme, des données originales correspondantes

[ISO/IEC 2382-8:1998, définition 08.03.04]

NOTE Un cryptogramme peut être chiffré une deuxième fois ; dans ce cas, un déchiffrement unique ne restitue pas le texte en clair original.

3.19
désidentification
terme général qui désigne tout processus réduisant l'association entre un ensemble de données d'identification et la personne concernée

3.20
données d'identification directe
données qui identifient directement un individu

NOTE Les identifiants directs sont les données qui peuvent être utilisées pour identifier une personne sans informations supplémentaires ou par recoupement avec d'autres informations du domaine public.

3.21
divulgation
le fait de révéler des données ou d'y donner accès

NOTE Le fait que le destinataire regarde réellement les données, les transforme en connaissances ou les conserve, est sans importance vis-à-vis de la réalisation de la communication.

3.22
chiffrement
transformation cryptographique de données produisant un **cryptogramme** (3.6)

[ISO 7498-2:1989, définition 3.3.27]

NOTE Voir **cryptographie** (3.10).

3.23
identifiant du sujet de soins
identifiant de soins de santé
identifiant d'une personne, destiné à être principalement utilisé par un système de soins de santé

3.24
personne identifiable
personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale

[Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données]

3.25
identification
processus consistant à utiliser des attributs déclarés ou observés d'une entité pour distinguer cette entité parmi d'autres dans un ensemble d'identités

NOTE L'identification d'une entité dans un contexte déterminé permet à une autre entité de différencier les entités avec lesquelles elle interagit.

3.26
identifiant
information utilisée pour déclarer une identité, avant corroboration potentielle par un authentifiant correspondant (tel qu'utilisé dans le présent document)

[ENV 13608-1]

3.27
données d'identification indirecte
données qui ne peuvent identifier une personne que lorsqu'elles sont utilisées conjointement avec d'autres données d'identification indirecte

NOTE Les identifiants indirects peuvent réduire à un individu la population à laquelle la personne appartient, s'ils sont utilisés en combinaison.

EXEMPLES Code postal, sexe, âge, date de naissance.

3.28
information
connaissance concernant un objet qui, dans un contexte déterminé, a une signification particulière
[ISO/IEC 2382-1:1993]

NOUVEAU TERME
donnée
représentation réinterprétable d'une information sous une forme conventionnelle convenant à la communication, à l'interprétation ou au traitement

NOTE Les données peuvent être traitées par des moyens humains ou automatiques.
[ISO/IEC 2382-1:1993]

3.29
irréversibilité
pour toute transformation d'identifiable en pseudonyme, situation dans laquelle il est informatiquement irréalisable de remonter à l'identifiant d'origine en partant du pseudonyme

3.30
clé
série de symboles commandant les opérations de **chiffrement** (3.21) et de **déchiffrement** (3.17)

[ISO 7498-2:1989, définition 3.3.32]

3.31
liage d'objets d'information
processus permettant d'établir une association logique entre différents objets d'information

3.32
personne physique
être humain par opposition à personne morale, laquelle peut être un organisme privé ou public

3.33
identification de personne
processus établissant une association entre un objet d'information et une personne physique

3.34
identifiant personnel
information permettant d'identifier une même et unique personne dans un contexte donné

3.35
données à caractère personnel
toute information concernant une personne physique identifiée ou identifiable (« personne concernée »)

[Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données]

3.36
principale utilisation des données à caractère personnel
utilisation des données à caractère personnel pour dispenser des soins de santé

3.37
respect de la vie privée
garantie de l'absence d'intrusion dans la vie privée ou les affaires d'un individu dans la mesure où cette intrusion résulte de la collecte et de l'utilisation illégales et non fondées de données relatives à cet individu

[ISO/IEC 2382-8:1998, définition 08.01.23]

3.38
traitement de données à caractère personnel
toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction

[Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données]

3.39
sous-traitement
personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

[Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données]

3.40
pseudonymisation
type particulier de désidentification qui à la fois, supprime la corrélation avec lapersonne concernée et ajoute une association entre un ensemble donné de caractéristiques concernant la personne concernée et un ou plusieurs pseudonymes

3.41
pseudonyme
identifiant personnel différent de l'identifiant personnel normalement utilisé et employé avec des données pseudonymisées pour assurer la cohérence de l'ensemble de données, reliant ainsi toutes les informations relatives à une personne concernée, sans communiquer la véritable identité de la personne

NOTE 1 Le pseudonyme peut être dérivé de l'identifiant personnel normalement utilisé, de manière réversible ou irréversible, ou n'avoir aucun rapport avec ce dernier.

NOTE 2 Le terme de pseudonyme se limite généralement à désigner un identifiant qui ne permet pas la dérivation directe de l'identifiant personnel normal. De telles informations pseudonymes sont donc fonctionnellement anonymes. Une tierce partie de confiance peut être en mesure d'obtenir l'identifiant personnel normal à partir du pseudonyme.

3.42
destinataire
personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication de données

3.43
utilisation indirecte~~, secondaire,~~ des données à caractère personnel
On entend par utilisation indirecte, une utilisation qui diverge de l'usage initialement prévu pour les données collectées.

3.44
politique de sécurité
plan ou programme d'action adopté pour assurer la sécurité informatique

[ISO/IEC 2382-8:1998, définition 08.01.06]

3.45
tierce partie de confiance
autorité de sécurité, ou son mandataire, à qui d'autres entités accordent leur confiance pour des activités en rapport avec la sécurité

[ISO/IEC 18014-1:2008]

4 Symboles (et abréviations)

HIPAA Loi américaine sur la transférabilité des régimes d'assurance-maladie et l'imputabilité des données sensibles [Health Insurance Portability and Accountability Act]

SIH Système d'information hospitalier

VIH Virus de l'immunodéficience humaine

IP Protocole Internet [Internet Protocol]

VoV Victime de violence

5 Exigences concernant la protection du caractère privé des identités dans le domaine de la santé

5.1.1 Objectifs de la protection de la vie privée

L'objectif de la protection de la vie privée, en tant qu'objectif de sécurité visant à garantir la confidentialité, est d'empêcher la communication non autorisée ou non souhaitée d'informations sur une personne, lesquelles peuvent en outre influer sur des facteurs de risque juridiques, organisationnels et financiers. La protection de la vie privée est un sous-domaine du droit générique au respect de la vie privée qui, par définition, englobe d'autres entités sensibles au respect du caractère privé des données, telles que les organisations. Étant donné que l'aspect « respect de la vie privée » est le mieux réglementé et le plus répandu, ce modèle conceptuel met l'accent sur le respect du caractère privé des données. Des solutions de protection conçues pour le respect de la vie privée peuvent également être transposées pour la protection des données sensibles d'autres entités. Cela peut être utile dans les pays où le caractère privé des données des entités ou des organisations est réglementé par la loi.

La protection des données à caractère personnel a deux objectifs dont l'un consiste à protéger les données à caractère personnel en interaction avec des applications en ligne (par exemple, navigation Web) et l'autre, à protéger les données à caractère personnel collectées dans des bases de données. La présente Spécification technique se limitera à ce dernier objectif.