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

*Health informatics — Information security management in health
using ISO/IEC 27002*

Sample Document

get full document from standards.iteh.ai



Numéro de référence
ISO 27799:2016(F)

© ISO 2016

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2016, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos	vii
Introduction	viii
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Structure de la présente Norme internationale	3
5 Politiques de sécurité de l'information	4
5.1 Orientations de la direction en matière de sécurité de l'information	4
5.1.1 Politiques de sécurité de l'information	4
5.1.2 Revue des politiques de sécurité de l'information	6
6 Organisation de la sécurité de l'information	6
6.1 Organisation interne	6
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information	6
6.1.2 Séparation des tâches	7
6.1.3 Relations avec les autorités	8
6.1.4 Relations avec des groupes de travail spécialisés	8
6.1.5 La sécurité de l'information dans la gestion de projet	8
6.2 Appareils mobiles et télétravail	9
6.2.1 Politique en matière d'appareils mobiles	9
6.2.2 Télétravail	9
7 La sécurité des ressources humaines	10
7.1 Avant l'embauche	10
7.1.1 Sélection des candidats	10
7.1.2 Termes et conditions d'embauche	11
7.2 Pendant la durée du contrat	11
7.2.1 Responsabilités de la direction	11
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	12
7.2.3 Processus disciplinaire	12
7.3 Rupture, terme ou modification du contrat de travail	13
7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail	13
8 Gestion des actifs	13
8.1 Responsabilités relatives aux actifs	13
8.1.1 Inventaire des actifs	13
8.1.2 Propriété des actifs	14
8.1.3 Utilisation correcte des actifs	14
8.1.4 Restitution des actifs	15
8.2 Classification de l'information	15
8.2.1 Classification des informations	15
8.2.2 Marquage des informations	16
8.2.3 Manipulation des actifs	17
8.3 Manipulation des supports	17
8.3.1 Gestion des supports amovibles	17
8.3.2 Mise au rebut des supports	18
8.3.3 Transfert physique des supports	18
9 Contrôle d'accès	18
9.1 Exigences métier en matière de contrôle d'accès	18
9.1.1 Politique de contrôle d'accès	18
9.1.2 Accès aux réseaux et aux services en réseau	19
9.2 Gestion de l'accès utilisateur	20
9.2.1 Enregistrement et désinscription des utilisateurs	20

9.2.2	Maîtrise de la gestion des accès utilisateur	21
9.2.3	Gestion des privilèges d'accès	21
9.2.4	Gestion des informations secrètes d'authentification des utilisateurs	22
9.2.5	Revue des droits d'accès utilisateur	22
9.2.6	Suppression ou adaptation des droits d'accès	22
9.3	Responsabilités des utilisateurs	23
9.3.1	Utilisation d'informations secrètes d'authentification	23
9.4	Contrôle de l'accès au système et aux applications	23
9.4.1	Restriction d'accès à l'information	24
9.4.2	Sécuriser les procédures de connexion	24
9.4.3	Système de gestion des mots de passe	24
9.4.4	Utilisation de programmes utilitaires à privilèges	25
9.4.5	Contrôle d'accès au code source des programmes	25
10	Cryptographie	25
10.1	Mesures cryptographiques	25
10.1.1	Politique d'utilisation des mesures cryptographiques	25
10.1.2	Gestion des clés	26
11	Sécurité physique et environnementale	26
11.1	Zones sécurisées	26
11.1.1	Périmètre de sécurité physique	26
11.1.2	Contrôles physiques des accès	27
11.1.3	Sécurisation des bureaux, des salles et des équipements	27
11.1.4	Protection contre les menaces extérieures et environnementales	27
11.1.5	Travail dans les zones sécurisées	27
11.1.6	Zones de livraison et de chargement	28
11.2	Matériels	28
11.2.1	Emplacement et protection du matériel	28
11.2.2	Services généraux	29
11.2.3	Sécurité du câblage	29
11.2.4	Maintenance du matériel	29
11.2.5	Sortie des actifs	29
11.2.6	Sécurité du matériel et des actifs hors des locaux	30
11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel	30
11.2.8	Matériel utilisateur laissé sans surveillance	31
11.2.9	Politique du bureau propre et de l'écran vide	31
12	Sécurité liée à l'exploitation	31
12.1	Procédures et responsabilités liées à l'exploitation	31
12.1.1	Procédures d'exploitation documentées	31
12.1.2	Gestion des changements	32
12.1.3	Dimensionnement	32
12.1.4	Séparation des environnements de développement, de test et d'exploitation	32
12.2	Protection contre les logiciels malveillants	33
12.2.1	Mesures contre les logiciels malveillants	33
12.3	Sauvegarde	33
12.3.1	Sauvegarde des informations	33
12.4	Journalisation et surveillance	34
12.4.1	Journalisation des événements	34
12.4.2	Protection de l'information journalisée	35
12.4.3	Journaux administrateur et opérateur	36
12.4.4	Synchronisation des horloges	37
12.5	Maîtrise des logiciels en exploitation	37
12.5.1	Installation de logiciels sur des systèmes en exploitation	37
12.6	Gestion des vulnérabilités techniques	37
12.6.1	Gestion des vulnérabilités techniques	37
12.6.2	Restrictions liées à l'installation de logiciels	38
12.7	Considérations sur l'audit du système d'information	38
12.7.1	Mesures relatives à l'audit des systèmes d'information	38

13	Sécurité des communications	38
13.1	Management de la sécurité des réseaux	38
13.1.1	Contrôle des réseaux	38
13.1.2	Sécurité des services de réseau	39
13.1.3	Cloisonnement des réseaux	39
13.2	Transfert de l'information	39
13.2.1	Politiques et procédures de transfert de l'information	39
13.2.2	Accords en matière de transfert d'information	40
13.2.3	Messagerie électronique	40
13.2.4	Engagements de confidentialité ou de non-divulgence	41
14	Acquisition, développement et maintenance des systèmes d'information	41
14.1	Exigences de sécurité applicables aux systèmes d'information	41
14.1.1	Analyse et spécification des exigences de sécurité de l'information	41
14.1.2	Sécurisation des services d'application sur les réseaux publics	43
14.1.3	Protection des transactions liées aux services d'application	43
14.2	Sécurité des processus de développement et d'assistance technique	44
14.2.1	Politique de développement sécurisé	44
14.2.2	Procédures de contrôle des changements apportés au système	44
14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	44
14.2.4	Restrictions relatives aux changements apportés aux progiciels	45
14.2.5	Principes d'ingénierie de la sécurité des systèmes	45
14.2.6	Environnement de développement sécurisé	45
14.2.7	Développement externalisé	45
14.2.8	Phase de test de la sécurité du système	46
14.2.9	Test de conformité du système	46
14.3	Données de test	46
14.3.1	Protection des données de test	46
15	Relations avec les fournisseurs	47
15.1	Sécurité de l'information dans les relations avec les fournisseurs	47
15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	47
15.1.2	La sécurité dans les accords conclus avec les fournisseurs	47
15.1.3	Chaîne d'approvisionnement informatique	48
15.2	Gestion de la prestation du service	48
15.2.1	Surveillance et revue des services des fournisseurs	48
15.2.2	Gestion des changements apportés dans les services des fournisseurs	48
16	Gestion des incidents liés à la sécurité de l'information	49
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations	49
16.1.1	Responsabilités et procédures	49
16.1.2	Signalement des événements liés à la sécurité de l'information	49
16.1.3	Signalement des failles liées à la sécurité de l'information	50
16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision	50
16.1.5	Réponse aux incidents liés à la sécurité de l'information	51
16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information	51
16.1.7	Recueil de preuves	51
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	52
17.1	Continuité de la sécurité de l'information	52
17.1.1	Organisation de la continuité de la sécurité de l'information	52
17.1.2	Mise en œuvre de la continuité de la sécurité de l'information	53
17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information	53
17.2	Redondances	53
17.2.1	Disponibilité des moyens de traitement de l'information	53
18	Conformité	54
18.1	Conformité aux obligations légales et réglementaires	54
18.1.1	Identification de la législation et des exigences contractuelles applicables	54

18.1.2	Droits de propriété intellectuelle	54
18.1.3	Protection des enregistrements	54
18.1.4	Protection de la vie privée et protection des données à caractère personnel	55
18.1.5	Réglementation relative aux mesures cryptographiques	56
18.2	Revue de la sécurité de l'information	56
18.2.1	Revue indépendante de la sécurité de l'information	56
18.2.2	Conformité avec les politiques et les normes de sécurité	56
18.2.3	Examen de la conformité technique	57
Annexe A (informative) Menaces pesant sur la sécurité des informations de santé		58
Annexe B (informative) Plan d'action pratique pour la mise en œuvre de l'ISO/IEC 27002 dans le domaine de la santé		63
Annexe C (informative) Liste de vérification de la conformité à l'ISO 27799		78
Bibliographie		99

Sample Document

get full document from standards.iteh.ai

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 sur la liste ISO des déclarations de brevets reçues (voir www.iso.org/brevets).

Les éventuelles appellations commerciales utilisées dans le présent document sont données pour information à l'intention des utilisateurs et ne constituent pas une approbation ou une recommandation.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, aussi bien que pour des informations 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*

Cette deuxième édition annule et remplace la première édition (ISO 27799:2008), qui a fait l'objet d'une révision technique.

Introduction

La présente Norme internationale fournit des préconisations aux organismes de santé et aux autres dépositaires d'informations personnelles de santé sur la meilleure façon de protéger la confidentialité, l'intégrité et la disponibilité de ces informations. Elle s'appuie sur les lignes directrices générales fournies par l'ISO/IEC 27002:2013 et les étend en traitant des besoins en matière de management de la sécurité de l'information propres au secteur de la santé et à son environnement de mise en œuvre particulier. Même si la protection et la sécurité des informations personnelles sont importantes pour l'ensemble des individus, des entreprises, des institutions et des gouvernements, il existe, dans le secteur de la santé, des exigences particulières à respecter pour assurer la confidentialité, l'intégrité, l'auditabilité et la disponibilité des informations personnelles de santé. Beaucoup considèrent que ces informations comptent parmi les informations personnelles les plus confidentielles. La protection de cette confidentialité est essentielle chaque fois que le respect de la vie privée des sujets de soins doit être assuré. Il est nécessaire de protéger l'intégrité des informations de santé afin d'assurer la sécurité des patients. L'un des principes clés de cette protection est de pouvoir garantir que le cycle de vie complet de l'information est auditable de bout en bout. La disponibilité des informations de santé a également un caractère critique pour la prestation efficace de soins de santé. Il est nécessaire que les systèmes d'information de santé répondent à des demandes particulières afin de rester opérationnels en cas de catastrophes naturelles, de défaillances du système ou d'attaques par déni de service. Protéger la confidentialité, l'intégrité et la disponibilité des informations de santé nécessite donc une expertise spécifique du secteur de la santé.

Quels que soient leur taille, leur situation ou les types de prestations qu'ils fournissent, tous les organismes de santé ont besoin de mettre en œuvre des mesures strictes pour protéger les informations de santé qui leur sont confiées. Pourtant, beaucoup de professionnels de la santé exercent de manière isolée ou dans de petites cliniques qui ne disposent pas des ressources informatiques nécessaires pour assurer le management de la sécurité de l'information. Les organismes de santé ont donc besoin de définir des préconisations claires, concises et particulières au secteur de la santé pour la sélection et la mise en œuvre de telles mesures. Il est nécessaire que la présente Norme internationale s'adapte à toutes les tailles, toutes les situations et tous les types de prestations fournis en soins de santé. Enfin, l'accroissement des échanges électroniques d'informations personnelles de santé entre professionnels de la santé (y compris l'utilisation de services Internet et sans fil) justifie l'utilité de l'adoption d'une référence commune en matière de management de la sécurité de l'information dans le domaine de la santé.

L'ISO/IEC 27002 est déjà largement déployée pour le management de la sécurité de l'informatique de santé par l'intermédiaire de directives nationales ou régionales en Afrique du Sud, en Australie, au Canada, en France, en Nouvelle-Zélande, aux Pays-Bas, au Royaume-Uni et dans d'autres pays. L'ISO 27799 s'appuie sur l'expérience acquise au cours de ces expérimentations nationales dans le management de la sécurité des informations personnelles de santé et se présente comme un document complémentaire de la norme ISO/IEC 27002. Elle n'a pas pour objectif de supplanter la série de normes ISO/IEC 27000-, mais plutôt de compléter ces normes plus générales.

L'ISO 27799 transpose l'ISO/IEC 27002 au domaine de la santé en prenant soin de considérer l'application appropriée des mesures de sécurité dans l'objectif de la protection des informations personnelles de santé. Dans certains cas, ces considérations ont conduit les auteurs à conclure que l'application de certains objectifs de sécurité de l'ISO/IEC 27002 est essentielle pour protéger les informations personnelles de santé de manière adéquate. L'ISO 27799 contraint ainsi à mettre en œuvre certaines mesures de sécurité spécifiées dans l'ISO/IEC 27002.

Tous les objectifs de sécurité décrits dans l'ISO/IEC 27002 sont applicables à l'informatique de santé, mais certaines mesures nécessitent des explications supplémentaires sur la façon de les optimiser afin de protéger la confidentialité, l'intégrité et la disponibilité des informations de santé. Il existe également des exigences supplémentaires spécifiques du secteur de la santé. La présente Norme internationale fournit des préconisations supplémentaires dans un format que les personnes responsables de la sécurité des informations de santé peuvent aisément comprendre et adopter.

Dans le domaine de la santé, un organisme (par exemple un hôpital) peut être certifié conformément à l'ISO/IEC 27001 sans devoir être certifié, ni même reconnu, selon l'ISO 27799. On espère toutefois qu'à

mesure que les organismes de santé s'efforcent d'améliorer la sécurité des informations personnelles de santé, la conformité à l'ISO 27799 se généralisera en tant que norme plus rigoureuse dans le domaine de la santé.

Objectifs

Les principaux objectifs de la sécurité de l'information résident dans la protection de la confidentialité, de la disponibilité et de l'intégrité (y compris l'authenticité, l'imputabilité et l'auditabilité) des informations. Dans le domaine de la santé, le respect de la vie privée des sujets de soins dépend de la protection de la confidentialité des informations personnelles de santé. Afin de protéger cette confidentialité, il est également nécessaire de prendre des mesures pour préserver l'intégrité des données, ne serait-ce que parce qu'il est possible de corrompre l'intégrité des données de contrôle d'accès, des systèmes de traçabilité et d'autres données système par le biais de techniques permettant la violation de la confidentialité et ce, de manière parfois totalement invisible. De plus, la sécurité des patients dépend de la protection de l'intégrité des informations personnelles de santé. L'absence de protection peut également entraîner des maladies, des blessures, voire la mort. De même, une disponibilité élevée des informations est une qualité très importante pour les systèmes de santé puisque le temps est souvent un facteur primordial dans l'administration des traitements. En effet, des catastrophes susceptibles de provoquer des interruptions de service dans des systèmes informatiques ne relevant pas du domaine de la santé peuvent coïncider avec le moment où l'obtention des informations contenues dans les systèmes de santé est d'une importance capitale. De même, les attaques par déni de service contre les systèmes en réseau sont de plus en plus fréquentes.

Les mesures abordées dans la présente Norme internationale ont été identifiées comme appropriées aux soins de santé, afin de protéger la confidentialité, l'intégrité et la disponibilité des informations personnelles de santé et de garantir l'auditabilité et l'imputabilité de l'accès à ces informations. Ces mesures contribuent à éviter les erreurs médicales susceptibles de se produire lorsque l'intégrité des informations de santé n'a pas pu être préservée. Elles contribuent également à garantir la continuité des services médicaux proposés.

Des considérations supplémentaires déterminent les objectifs relatifs à la sécurité des informations de santé. Elles comprennent les aspects suivants:

- a) l'observation des obligations légales, telles qu'exprimées dans les lois et les réglementations relatives à la protection des données, applicables à la protection du respect de la vie privée d'un sujet de soins¹⁾;
- b) le maintien dudit respect de la vie privée et des meilleures pratiques de sécurité dans le domaine de l'informatique de santé;
- c) le maintien de l'imputabilité de chacun et de l'organisme au sein de l'ensemble des organismes et des professionnels de la santé;
- d) le soutien à la mise en œuvre du management systématique des risques au sein des organismes de santé;
- e) la réponse aux besoins en matière de sécurité identifiés lors de situations de soins de santé communes;
- f) la diminution des coûts d'exploitation en facilitant l'utilisation croissante de la technologie dans un environnement sûr, sécurisé et bien géré qui soutient, sans les entraver, les activités de soins de santé en cours;
- g) le maintien de la confiance du public dans les organismes de santé ainsi que dans les systèmes d'information sur lesquels reposent ces organismes;

1) Outre les obligations légales, une importante source d'informations sur les obligations éthiques relatives aux informations de santé, le code d'éthique de l'OMS, est disponible. Ces obligations éthiques peuvent dans certains cas avoir des répercussions sur la politique de sécurité des informations de santé.

- h) le respect des normes professionnelles et de la déontologie, telles que les organismes professionnels liés à la santé les ont établies (dans la mesure où la sécurité de l'information préserve la confidentialité et l'intégrité des informations de santé);
- i) l'exploitation des systèmes électroniques d'information de santé au sein d'un environnement correctement sécurisé contre les menaces;
- j) le soutien à l'interopérabilité entre les systèmes de santé, étant donné que les informations de santé circulent de plus en plus entre les organismes et au-delà des frontières juridictionnelles (particulièrement quand une telle interopérabilité renforce la bonne gestion des informations de santé dans le but de garantir la continuité de leur confidentialité, de leur intégrité et de leur disponibilité).

Lien avec la gouvernance de l'information²⁾, la gouvernance d'entreprise et la gouvernance clinique

Alors que les organismes de santé peuvent adopter des positions différentes à propos de la gouvernance clinique et de la gouvernance d'entreprise, l'importance de l'intégration et du suivi de la gouvernance de l'information devrait transcender le débat en tant qu'élément essentiel aux deux premières. Tandis que les organismes de santé deviennent de plus en plus dépendants des systèmes d'information pour l'administration de soins (en exploitant, par exemple, les technologies d'aide à la prise de décision ou en s'appuyant davantage sur des soins de santé fondés sur des preuves plutôt que sur l'expérience), il semble de plus en plus évident que les pertes d'intégrité, de disponibilité et de confidentialité ont des conséquences cliniques importantes. Les problèmes issus de ces conséquences seront considérés comme des manquements aux obligations éthiques et légales inhérentes à l'obligation de diligence.

Tous les pays et toutes les juridictions disposent sans aucun doute d'études de cas dans lesquelles ces failles ont conduit à des erreurs de diagnostic, à des décès ou à des rétablissements retardés. Il est donc nécessaire que les fondements de la gouvernance clinique accordent autant d'importance au management efficace du risque relatif à la sécurité de l'information qu'aux programmes d'administration de soins, stratégies de gestion des infections et autres problèmes de gestion purement cliniques. La présente Norme internationale aidera les responsables de la gouvernance clinique à comprendre la contribution apportée par des stratégies de sécurité de l'information efficaces.

Informations de santé à protéger

Il existe plusieurs types d'informations dont la confidentialité, l'intégrité et la disponibilité³⁾ ont besoin d'être protégées:

- a) les informations personnelles de santé;
- b) les données pseudonymisées issues des informations personnelles de santé, par le biais d'une certaine méthodologie d'identification des pseudonymes;
- c) les données statistiques et de recherche, notamment les données anonymisées issues des informations personnelles de santé, par suppression des données à caractère personnel;
- d) les connaissances cliniques/médicales sans rapport avec un sujet de soins particulier, notamment les données d'aide à la décision clinique (par exemple les données sur les réactions indésirables consécutives à la prise d'un médicament);
- e) les données sur les professionnels de la santé, sur le personnel et sur les bénévoles;
- f) les informations liées à la surveillance de la santé publique;
- g) les données des systèmes de traçabilité produites par les systèmes d'information de santé qui contiennent des informations personnelles de santé ou des données pseudonymisées issues d'informations personnelles de santé, ou qui contiennent des données relatives aux actes des utilisateurs vis-à-vis de ces informations personnelles de santé; et

2) Dans certains pays, la «gouvernance de l'information» est appelée «assurance de l'information».

3) Le degré de disponibilité dépend des utilisations dont ces données feront l'objet.

- h) les données de sécurité pour les systèmes d'information de santé, y compris les données de contrôle d'accès et autres données de configuration du système liées à la sécurité pour les systèmes d'information de santé.

La mesure dans laquelle il est nécessaire de protéger la confidentialité, l'intégrité et la disponibilité dépend de la nature des informations, de leur utilisation et du niveau de risque auquel elles sont exposées. Par exemple, des données statistiques [point c) ci-dessus] ne sont pas toujours confidentielles, mais la protection de leur intégrité peut relever de la plus haute importance. De même, les données des systèmes de traçabilité [point g) ci-dessus] peuvent ne pas exiger une grande disponibilité (un archivage régulier par heure et non par seconde peut suffire pour certaines applications), mais leur contenu peut être hautement confidentiel. Une appréciation du risque peut déterminer de façon appropriée le degré d'effort nécessaire à la protection de la confidentialité, de l'intégrité et de la disponibilité (voir [B.4.4](#)). Il est nécessaire d'intégrer les résultats d'une appréciation régulière du risque aux ressources et priorités de l'organisme mettant en œuvre cette norme.

Les menaces et les vulnérabilités en matière de sécurité des informations de santé

Les types ainsi que les descriptions des menaces et des vulnérabilités qui affectent la sécurité de l'information varient amplement. Aucune n'est vraiment propre au domaine de la santé, cependant, la singularité dans ce domaine réside dans la multitude de facteurs à considérer lors de l'évaluation de ces menaces et de ces vulnérabilités.

De par leur nature, les organismes de santé opèrent dans un environnement qui peut difficilement être fermé aux visiteurs et au grand public. Au sein des grands organismes de santé, le nombre de personnes se déplaçant dans les zones opérationnelles est conséquent. Ces facteurs augmentent la vulnérabilité des systèmes face aux menaces physiques. La probabilité que de telles menaces se réalisent peut augmenter quand des sujets de soins ou des proches émotifs ou atteints d'une maladie mentale sont présents.

L'importance primordiale d'une identification correcte des sujets de soins ainsi que d'une association efficace à leur dossier de santé amène les organismes de santé à réunir des informations d'identification détaillées. Les registres régionaux ou juridictionnels des patients (c'est-à-dire les registres des sujets de soins) sont parfois les référentiels les plus exhaustifs et actuels d'informations d'identification disponibles dans une juridiction. Ces informations d'identification représentent une valeur potentielle considérable pour ceux qui voudraient commettre un vol d'identité; il convient donc de les protéger rigoureusement.

De nombreux organismes de santé sont perpétuellement en manque de moyens et leur personnel est parfois obligé de travailler sous une forte pression et avec des systèmes maintenus en service longtemps après la date à laquelle ils auraient dû être changés. Ces facteurs peuvent augmenter le risque que certains types de menaces se réalisent et peut accroître les vulnérabilités. D'un autre côté, les professionnels, membres du personnel technique, administratif, les auxiliaires et les bénévoles évoluant dans le domaine de la santé considèrent pour la plupart leur travail comme une véritable vocation. Leur dévouement et la diversité de leurs expériences peut souvent diminuer efficacement l'exposition aux vulnérabilités. Beaucoup de ces professionnels de la santé justifient d'un haut niveau de formation qui différencie les soins de santé de nombreux autres secteurs industriels sur le plan de l'incidence des menaces internes.

Il convient donc de considérer l'environnement de la santé, avec ses menaces et ses vulnérabilités propres, avec une attention toute particulière. L'[Annexe A](#) contient une liste d'informations sur les types de menaces qui doivent être prises en compte par les organismes de santé lors de l'appréciation des risques relatifs à la confidentialité, l'intégrité et la disponibilité des informations de santé et à l'intégrité et la disponibilité des systèmes d'information associés.

À quel public la présente Norme internationale est-elle destinée ?

La présente Norme internationale est destinée aux responsables de la supervision de la sécurité des informations de santé, ainsi qu'aux organismes de santé et autres dépositaires d'informations de santé qui cherchent des préconisations sur ce sujet. Sont aussi concernés leurs conseillers en sécurité, consultants, auditeurs, fournisseurs et prestataires de services tiers.

Les auteurs de la présente Norme internationale n'ont pas pour intention d'écrire une introduction sur la sécurité informatique, ils ne veulent pas non plus répéter ce qui a déjà été écrit dans l'ISO/IEC 27002 ou dans l'ISO/IEC 27001. De nombreuses exigences de sécurité sont communes à tous les systèmes informatisés, que ce soit dans la finance, la fabrication, le contrôle industriel ou dans n'importe quel domaine d'activité organisé. Un effort commun a été accompli pour se concentrer sur les exigences de sécurité nécessaires dans l'unique but de fournir des informations électroniques de santé qui peuvent être utilisées dans l'administration de soins.

Avantages de l'utilisation de la présente Norme internationale

L'ISO/IEC 27002 est une Norme internationale vaste et complexe et les conseils qui y sont donnés ne sont pas spécialement adaptés au domaine de la santé. L'ISO 27799 permet la mise en œuvre uniforme de l'ISO/IEC 27002 dans des environnements de santé et prête une attention particulière aux défis propres à ce secteur. En suivant cette norme, les organismes de santé contribuent à garantir que la confidentialité et l'intégrité des données en leur possession sont protégées, que les systèmes d'information de santé primordiaux restent disponibles et que l'imputabilité des informations de santé est préservée.

L'adoption de la présente Norme internationale par les organismes de santé à la fois au sein et entre les juridictions facilitera la coopération et permettra l'adoption en toute sécurité de nouvelles technologies coopératives pour la prestation de soins de santé. Le partage d'informations sécurisées et dans le respect de la vie privée peut considérablement améliorer les résultats des soins de santé.

En mettant en œuvre la présente Norme internationale, les organismes de santé peuvent s'attendre à une diminution des incidents de sécurité, tant en nombre qu'en gravité. Les ressources peuvent ainsi être redistribuées vers des activités productives. La sécurité informatique permet ainsi aux ressources de santé d'être distribuées de manière rentable et productive. En effet, une étude réalisée par le très reconnu Forum sur la sécurité de l'information en partenariat avec des analystes de marché a démontré que, grâce à une sécurité correctement développée, des organismes ont enregistré une hausse de leurs résultats allant jusqu'à 2 %.

Enfin, une approche cohérente de la sécurité informatique, accessible à tous les individus impliqués dans les soins de santé, améliorera le moral du personnel ainsi que la confiance du public dans les systèmes détenteurs de d'informations personnelles de santé.

Comment utiliser la présente Norme internationale ?

Les lecteurs qui ne connaissent pas encore l'ISO/IEC 27002 sont encouragés à lire les paragraphes introductifs de cette norme avant de poursuivre leur lecture. Il est nécessaire que les personnes chargées de la mise en œuvre de l'ISO 27799 lisent d'abord attentivement l'ISO/IEC 27002 étant donné que le texte ci-après fait fréquemment référence aux articles et paragraphes correspondants de celle-ci. La présente Norme internationale ne peut être pleinement comprise sans consulter le texte intégral de l'ISO/IEC 27002.

Les lecteurs à la recherche de préconisations concernant la mise en œuvre de l'ISO/IEC 27002 dans un environnement de santé trouveront un plan d'action pratique à l'[Annexe B](#). Cet article ne contient aucune exigence impérative. Au contraire, des conseils et des préconisations d'ordre général sont donnés sur la meilleure façon de procéder à la mise en œuvre de l'ISO/IEC 27002 dans le domaine de la santé. L'article est organisé selon un cycle d'activités (planifier-réaliser-contrôler-agir) décrit dans l'ISO/IEC 27001. Le respect de ce cycle aboutira à une mise en œuvre fiable d'un système de management de la sécurité de l'information.

Les lecteurs à la recherche de conseils particuliers sur les articles relatifs aux mesures de sécurité et sur les catégories de mesures décrits dans l'ISO/IEC 27002 les trouveront dans les articles de la présente Norme internationale avec le même numéro d'article et le même titre que dans l'ISO/IEC 27002. Cet article accompagne le lecteur à travers chacun des onze articles relatifs aux mesures de sécurité de l'ISO/IEC 27002. Le cas échéant, les exigences minimales sont indiquées et, dans certains cas, des lignes directrices normatives sur l'application correcte de certaines mesures de sécurité de l'ISO/IEC 27002 sont données en vue de la protection des informations de santé.

Une fois l'ISO/IEC 27002 mise en place, le management continu est considéré comme essentiel s'il est nécessaire de maintenir les bénéfices de la Norme internationale. [L'Article 18](#) traite de l'évaluation de la conformité et des exigences pour le management continu de la sécurité de l'information. [L'Annexe C](#) comporte une matrice d'auto-évaluation eu égard à la conformité.

La présente Norme internationale se conclut par quatre annexes informatives.

[L'Annexe A](#) décrit les menaces générales qui planent sur les informations de santé. [L'Annexe B](#) décrit brièvement un plan d'action pratique pour la mise en œuvre de Norme internationales complémentaires relatives à la sécurité de l'information. [L'Annexe C](#) fournit une liste de vérification de la conformité à l'ISO 27799. [L'Article 2](#) fournit une liste des normes citées en tant que références normatives; la bibliographie fournit une liste d'autres normes associées relatives à la sécurité des informations de santé.

Sample Document

get full document from standards.iteh.ai

Sample Document

get full document from standards.iteh.ai

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

1 Domaine d'application

La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) à risques pour la sécurité de l'information de l'organisme.

La présente Norme internationale spécifie des lignes directrices permettant d'interpréter et de mettre en œuvre l'ISO/IEC 27002 dans le domaine de l'informatique de santé et constitue un complément à cette dernière⁴⁾.

La présente Norme internationale fournit des préconisations de mise en œuvre des mesures décrites dans l'ISO/IEC 27002 et les complète, le cas échéant, de façon à ce qu'elles puissent être utilisées efficacement dans le management de la sécurité des informations de santé. La mise en œuvre de la présente Norme internationale permettra aux organismes de santé et aux autres dépositaires d'informations de santé de garantir le niveau minimal requis de sécurité approprié aux conditions de leur organisme et de protéger la confidentialité, l'intégrité et la disponibilité des informations personnelles de santé dans leurs activités de soins.

La présente Norme internationale s'applique à tous les aspects des informations de santé, quelle que soit la forme (mots, chiffres, enregistrements sonores, dessins, vidéos et images médicales), le support utilisé pour les stocker (imprimés, documents manuscrits ou stockage électronique) ou les moyens mis en œuvre pour leur transmission (en main propre, par fax, par réseau informatique ou par courrier), de sorte que l'information soit toujours correctement protégée.

La présente Norme internationale et l'ISO/IEC 27002 définissent les exigences en termes de sécurité de l'information dans les soins de santé, mais elles ne définissent pas la façon de satisfaire à ces exigences. En d'autres termes, dans toute la mesure du possible, la technologie est absente de la présente Norme internationale. La neutralité sur les technologies de mise en œuvre est une caractéristique importante. La technologie en matière de sécurité continue de se développer rapidement. Le rythme de cette évolution se mesure actuellement en mois et non plus en années. En revanche, bien que les Normes internationales soient soumises à des révisions régulières, il est prévu qu'elles restent valides pendant plusieurs années. De manière également importante, la neutralité sur les technologies laisse aux fournisseurs et aux prestataires de services l'entière liberté de suggérer des technologies nouvelles ou en développement qui peuvent répondre aux exigences décrites dans la présente Norme internationale.

Comme mentionné dans l'introduction, la connaissance de l'ISO/IEC 27002 est indispensable à la compréhension de la présente Norme internationale.

Les domaines suivants de la sécurité de l'information ne relèvent pas du domaine d'application de la présente Norme internationale:

- a) les méthodologies et les essais statistiques en vue d'une anonymisation efficace des informations personnelles de santé;
- b) les méthodologies en vue de la pseudonymisation des informations personnelles de santé (voir la bibliographie pour une brève description d'une Spécification technique qui traite spécifiquement de ce sujet);
- c) la qualité des services fournis par le réseau et les méthodes pour évaluer la disponibilité des réseaux utilisés pour l'informatique de santé;

4) La présente Norme internationale est cohérente avec la version révisée de l'ISO/IEC 27002.