PROJET
FINAL

NORME INTERNATIONALE

ISO/FDIS 27799

ISO/TC **215**

Secrétariat: ANSI

Début de vote:
2016-03-17

Vote clos le:
2016-05-17

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

Veuillez consulter les notes administratives en page iii

Numéro de référence
ISO/FDIS 27799:2016(F)

TRAITEMENT PARALLÈLE ISO/CEN

Le présent projet final 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 final a été établi sur la base des observations reçues lors de l'enquête parallèle sur le projet.

Le projet final est par conséquent soumis aux comités membres de l'ISO et aux comités membres du CEN en parallèle à un vote d'approbation de deux mois au sein de l'ISO et à un vote formel au sein du CEN.

Les votes positifs ne doivent pas être accompagnés d'observations.

Les votes négatifs doivent être accompagnés des arguments techniques pertinents.

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

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 soins[1)];

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'information[2)], 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 disponibilité[3)] 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 conséquentes 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.