NORME INTERNATIONALE

ISO 27799

Première édition
2008-07-01

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

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

Numéro de référence
ISO 27799:2008(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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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.

L'ISO 27799 a été élaborée par le comité technique ISO/TC 215, *Informatique de santé*.

Introduction

La présente Norme internationale fournit des recommandations 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 en mettant en œuvre l'ISO/CEI 27002[1)]. Plus précisément, la présente Norme internationale traite des besoins de gestion de la sécurité de l'information spécifiques au domaine 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 tous les individus, les entreprises, les institutions et les gouvernements, il existe, dans le secteur de la santé, des exigences particulières à satisfaire pour garantir la confidentialité, l'intégrité, l'auditabilité et la disponibilité des informations personnelles de santé. Beaucoup considèrent que ces informations sont 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. L'intégrité des informations de santé doit être protégée afin de garantir la sécurité du patient. 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 est aussi critique pour fournir des soins médicaux de manière efficace. Les systèmes d'informations de santé doivent répondre à des demandes particulières afin de rester opérationnels en cas de catastrophes naturelles, de pannes de système ou d'attaques par refus de service. Protéger la confidentialité, l'intégrité et la disponibilité des informations de santé requiert donc une expertise spécifique du secteur de la santé.

L'utilisation croissante des technologies sans fil et de l'Internet dans la délivrance de soins rend plus urgent de gérer efficacement la sécurité des technologies de l'information dans le domaine de la santé. Ces technologies complexes, si elles ne sont pas appliquées correctement, augmenteront les risques de perte de la confidentialité, de l'intégrité et de la disponibilité des informations de santé. Quels que soient leur taille, leur situation ou les types de prestations, tous les organismes de santé ont besoin de mettre en œuvre des contrôles stricts pour protéger les informations de santé qui leur sont confiées. Pourtant, beaucoup de professionnels exercent de manière isolée ou dans des petites cliniques qui ne disposent pas des ressources informatiques nécessaires pour gérer la sécurité des informations. Les organismes de santé doivent donc définir des recommandations claires, concises et spécifiques au domaine de la santé sur la sélection et l'application de tels contrôles. Ces recommandations doivent s'adapter à toutes les prestations de service du domaine de la santé et ce, quel que soit leur taille, leur situation et leur modèle. En bref, l'accroissement des échanges électroniques d'informations personnelles de santé entre professionnels de la santé justifie l'utilité de l'adoption d'une référence commune en matière de gestion de la sécurité des informations de soins.

L'ISO/CEI 27002 est déjà largement déployée pour la gestion de la sécurité des informations de santé par l'intermédiaire des directives nationales ou régionales dans les pays suivants: Australie, Canada, France, Pays-Bas, Nouvelle-Zélande, Afrique du Sud et Royaume-Uni. L'intérêt se développe également dans d'autres pays. La présente Norme internationale rassemble l'expérience acquise au cours de ces expérimentations nationales dans la gestion de la sécurité des informations personnelles de santé et se présente comme un document complémentaire de la norme générique ISO/CEI 27002. Elle n'a pas pour objectif de supplanter l'ISO/CEI 27002 ni l'ISO/CEI 27001, mais plutôt de compléter ces normes plus générales.

La présente Norme internationale transpose l'ISO/CEI 27002 au domaine de la santé en prenant soin de considérer l'application appropriée des contrôles 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 contrôle de l'ISO/CEI 27002 est essentielle si les informations personnelles de santé devaient être protégées de manière adéquate. La présente Norme internationale contraint ainsi à mettre en œuvre certaines mesures de sécurité spécifiées dans l'ISO/CEI 27002, ce qui a conduit à inclure dans l'Article 7 plusieurs mentions normatives instituant comme obligatoire l'application de certaines mesures de sécurité. Par exemple 7.2.1 établit que

1) Ces recommandations s'appuient sur la version révisée de l'ISO/CEI 27002:2005.

*Les organisations traitant des informations de santé, y compris des informations personnelles de santé, **doivent** posséder une politique formelle de sécurité de l'information approuvée par la direction, publiée, puis communiquée à l'ensemble des employés ainsi qu'aux tiers concernés.*

Dans le domaine de la santé, un organisme (par exemple un hôpital) peut être certifié conformément à l'ISO/CEI 27001 sans être certifié, ni même reconnu, de la présente Norme internationale. Alors que les organismes de santé s'efforcent d'améliorer la sécurité des informations personnelles de santé, la conformité à la présente Norme internationale, en tant que norme plus rigoureuse dans le domaine de la santé, se répandra pour le plus grand nombre.

Tous les objectifs de contrôle de la sécurité décrits dans l'ISO/CEI 27002 sont applicables à l'informatique de santé mais certaines mesures requièrent 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 spécifiques supplémentaires dans le secteur de la santé. La présente Norme internationale apporte des recommandations supplémentaires dans un format que les personnes responsables de la sécurité des informations de santé peuvent aisément comprendre et adopter.

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 réitérer ce qui a déjà été écrit dans l'ISO/CEI 27002 ou dans l'ISO/CEI 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 système organisé. Un effort commun a été accompli pour se concentrer sur les exigences de sécurité nécessaires dans l'unique but de délivrer des informations électroniques de santé sur lesquels les services de soins peuvent s'appuyer.

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 indications sur ce sujet. Sont aussi concernés leur conseiller en sécurité, les consultants, les auditeurs, les fournisseurs et les prestataires de services tiers.

Avantages de l'utilisation de la présente Norme internationale

L'ISO/CEI 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. La présente Norme internationale prend en compte la mise en œuvre de l'ISO/CEI 27002 dans le domaine de la santé et prête une attention particulière aux défis propres à ce domaine. En respectant cette Norme internationale, les organismes de santé s'engagent à garantir que la confidentialité et l'intégrité des données en leur possession sont maintenues, que les systèmes d'informatique de santé primordiaux restent disponibles et que l'imputabilité des informations de santé est respectée.

L'adoption de ces recommandations par les organismes de santé à la fois au sein et au-delà de leur juridiction facilitera la coopération et permettra l'adoption en toute sécurité de nouvelles technologies coopératives en matière de soins médicaux. Le partage d'informations sécurisées et dans le respect de la vie privée peut considérablement améliorer les résultats des soins médicaux.

En suivant ces recommandations, 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 sur leurs résultats allant jusqu'a 2 %.

Enfin, une approche cohérente de la sécurité de l'information, accessible à tous les individus liés au secteur médical, améliorera le moral des employés ainsi que la confiance du public dans les systèmes détenteurs de ces informations personnelles.

Comment utiliser la présente Norme internationale ?

Les lecteurs qui ne connaissent pas encore l'ISO/CEI 27002 sont encouragés à lire les paragraphes introductifs de la présente Norme internationale avant de continuer leur lecture. Les personnes chargées de la mise en œuvre de la présente Norme internationale doivent lire attentivement l'ISO/CEI 27002, étant donné que le texte ci-dessous fait fréquemment référence aux paragraphes correspondants de celle-ci. Le présent document ne peut être pleinement compris sans consulter l'intégralité du texte de l'ISO/CEI 27002.

Les lecteurs qui ne connaissent pas la sécurité des informations de santé ainsi que ses objectifs, ses défis et tout ce qui l'entoure trouveront un véritable intérêt dans la lecture de la brève introduction de l'Article 5.

Les lecteurs à la recherche de recommandations relatives à la mise en œuvre de l'ISO/CEI 27002 dans un environnement relatif à la santé trouveront un plan d'action pratique dans l'Article 6. Aucune exigence impérative n'est présente dans cet article. Au contraire, des conseils et des indications d'ordre général sont donnés sur la meilleure façon de procéder à la mise en œuvre de l'ISO/CEI 27002 dans le domaine de la santé. L'article est organisé selon un cycle d'activités (planifier-déployer-contrôler-agir) décrit dans l'ISO/CEI 27001. Le respect de ce cycle aboutira à une mise en œuvre fiable d'un système de gestion de la sécurité de l'information.

Les lecteurs à la recherche de conseils particuliers sur les 11 articles relatifs aux mesures de sécurité et sur les 39 catégories de contrôle principales décrits dans l'ISO/CEI 27002 les trouveront dans l'Article 7. Cet article accompagne le lecteur à travers chacun des 11 articles relatifs aux mesures de sécurité de l'ISO/CEI 27002. Les exigences minimales sont indiquées lorsque besoin est et, dans certains cas, des directives normatives sur l'application correcte de certaines mesures de sécurité de l'ISO/CEI 27002 sont données en vue de la protection des informations de santé.

La présente Norme internationale se conclut par trois annexes informatives. L'Annexe A décrit les menaces générales qui planent sur les informations de santé. L'Annexe B décrit brièvement les tâches et les documents relatifs au système de gestion de la sécurité des informations. L'Annexe C présente les avantages des outils d'aide à la mise en place de cette sécurité. Enfin, une bibliographie fournit une liste des normes relatives à la sécurité des informations de santé.

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

1 Domaine d'application

1.1 Généralités

La présente Norme internationale fournit des lignes directrices permettant d'interpréter et de mettre en œuvre l'ISO/CEI 27002[2)] dans le domaine de l'informatique de santé et constitue un complément à cette dernière.

La présente Norme internationale spécifie une série de contrôles détaillés en vue de la gestion de la sécurité des informations de santé et apporte des indications de bonne pratique en matière de 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 en termes de sécurité propre aux dispositifs de leur organisme et de garantir la confidentialité, l'intégrité et la disponibilité des informations personnelles de santé.

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

La présente Norme internationale conjointement à l'ISO/CEI 27002 définissent les exigences en termes de sécurité de l'information dans le domaine des soins médicaux, 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 en matière de mise en œuvre des différentes technologies est une caractéristique importante. La technologie en matière de sécurité ne cesse 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 soient soumises à des révisions régulières, leur validité peut se compter en années. De manière également importante, l'absence de conseils technologiques laisse aux fournisseurs et aux prestataires de services l'entière liberté de suggérer des technologies nouvelles ou en développement capables de répondre aux exigences décrites dans la présente Norme internationale.

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

1.2 Exclusions du domaine d'application

Les domaines suivants de la sécurité de l'information n'entrent pas dans le cadre de la présente Norme internationale:

a) les méthodologies et les essais statistiques en vue d'un anonymisation efficace des informations personnelles de santé;

b) les méthodologies en vue de la pseudonymisation des informations personnelles de santé (voir la référence bibliographique [10] pour un exemple de Spécification technique qui traite spécifiquement de ce sujet);

---

2) Ces recommandations s'appuient sur la version révisée de l'ISO/CEI 27002:2005.

c) la qualité des services fournis par le réseau et les méthodes pour évaluer la disponibilité des réseaux utilisés pour l'informatique de santé;

d) la qualité des données (opposée à l'intégrité des données).

2 Références normatives

Les documents de référence suivants sont indispensables pour 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/CEI 27002:2005, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information*

3 Termes et définitions

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

3.1 Termes médicaux

3.1.1
informatique de santé
discipline scientifique relative aux tâches cognitives du traitement de l'information et de la communication liées à la pratique, l'enseignement et la recherche de la médecine, comprenant également la science et la technologie de l'information qui accompagnent ces tâches

[ISO/TR 18307:2001, définition 3.73]

3.1.2
système d'information de santé
dépôt d'informations relatives à la santé d'un sujet de soins sous une forme pouvant être informatisée, conservée, transmise de manière sûre et accessible par une multitude d'utilisateurs autorisés

NOTE Adapté de l'ISO/TR 20514:2005, définition 2.25.

3.1.3
soins de santé
tout type de services fournis par des professionnels ou des paraprofessionnels ayant une conséquence sur l'état de santé d'un individu

[Parlement européen, 1998, d'après la définition de l'OMS]

3.1.4
organisme de santé
terme générique utilisé pour définir les différents types d'organismes prestataires de soins de santé

[ISO/TR 18307:2001, définition 3.74]

3.1.5
professionnel de santé
personne habilitée par un organisme reconnu à effectuer certaines tâches liées à la santé

NOTE Adapté de l'ISO/TS 17090-1:2002, définition 3.18.

3.1.6
prestataire de soins de santé
toute personne ou tout organisme impliqué ou associé à la prestation de soins de santé, ou se chargeant du bien-être d'un patient

3.1.7
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

[ISO 22587:2004, définition 3.7]

3.1.8
patient
sujet recevant des soins

Voir 3.1.10.

3.1.9
information personnelle de santé
information relative à la santé physique ou mentale d'un individu identifiable ou à la prestation de services de santé, incluant les informations suivantes:

a) informations à propos de l'inscription d'un individu souhaitant bénéficier de services de santé;

b) informations relatives à la solvabilité d'un individu ou à sa légitimité à recevoir à des soins de santé;

c) numéro, symbole ou signe particulier attribué à un individu dans le seul but de pouvoir l'identifier à des fins médicales;

d) toute information consignée à propos d'un individu lors de la prestation de services de santé;

e) informations issues d'un essai ou d'un examen effectué sur une partie du corps ou sur une substance corporelle;

f) identification d'une personne (par exemple un professionnel de la santé) en tant que prestataire de soins de santé à un individu.

NOTE Une information personnelle de santé ne rentre pas dans le cadre d'informations isolées ou accompagnées d'autres informations disponibles, et qui ont été rendues anonymes, c'est-à-dire que l'identité de l'individu sur lequel porte ces informations ne peut pas être formellement identifié à partir de cette seule information.

3.1.10
sujet de soins
une ou plusieurs personnes devant recevoir, recevant ou ayant reçu une prestation de santé

[ISO/TS 18308:2004, définition 3.40]

3.2 Termes relatifs à la sécurité de l'information

3.2.1
bien
tout élément représentant de la valeur pour l'organisme

[ISO/CEI 13335-1:2004, définition 2.2]

NOTE Dans le contexte de la sécurité de l'information, les biens comprennent

a) l'information de santé,

b) les services informatiques,

c) le matériel informatique,

d) les logiciels,

e) les systèmes de communication,

f) les média,

g) les systèmes informatiques, et

h) les appareils médicaux enregistrant ou consignant des données.

3.2.2
imputabilité
propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité

[ISO 7498-2:1989, définition 3.3.3]

3.2.3
assurance
résultat d'un ensemble de processus de conformité grâce auquel un organisme peut se fier à l'état de sa gestion en matière de sécurité de l'information

3.2.4
disponibilité
propriété d'être accessible et utilisable sur demande par une entité autorisée

[ISO 7498-2:1989, définition 3.3.11]

3.2.5
évaluation de conformité
processus par le biais desquels un organisme vient confirmer le fonctionnement et l'efficacité de ses contrôles de sécurité de l'information

NOTE La conformité juridique se rapporte uniquement aux contrôles de sécurité mis en place pour fournir les exigences de la législation concernée, à l'image de la directive de l'union européenne relative à la protection des données personnelles.

3.2.6
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]

3.2.7
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]

3.2.8
contrôle de l'information
processus par lesquels un organisme obtient l'assurance que les risques relatifs à l'information, assurance elle-même étroitement liée aux capacités fonctionnelles et à l'intégrité de l'organisme, sont correctement identifiés et gérés

3.2.9
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

NOTE D'autres propriétés, telles que la comptabilité des utilisateurs mais aussi l'authenticité, la non-répudiation et la fiabilité sont souvent cités comme des aspects relatifs à la sécurité de l'information. Cependant, il est possible de les considérer comme des dérivés des trois propriétés principales énoncées dans la définition.

3.2.10
risque
combinaison de la probabilité d'un événement et de ses conséquences

[ISO Guide 73:2002, définition 3.1.1]

3.2.11
appréciation du risque
ensemble du processus d'analyse du risque et d'évaluation du risque

[ISO Guide 73:2002, définition 3.3.1]

3.2.12
management du risque
activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque

NOTE Le management du risque inclut généralement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

[ISO Guide 73:2002, définition 3.1.7]

3.2.13
traitement du risque
processus de sélection et de mise en œuvre des mesures visant à modifier (en général à diminuer) le risque

NOTE Adapté de l'ISO Guide 73:2002, définition 3.4.1.

3.2.14
intégrité du système
propriété établissant qu'un système accomplit la fonction prévue de manière constante sans risque d'être la cible d'une manipulation non autorisée, qu'elle soit accidentelle ou volontaire

3.2.15
menace
cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme

[ISO/CEI 13335-1:2004, définition 2.25]

3.2.16
vulnérabilité
point faible d'un bien ou d'un groupe de biens pouvant être utilisé pour une menace

[ISO/CEI 13335-1:2004, définition 2.26]

4 Termes abrégés

ISMF Forum sur la gestion de la sécurité de l'information (Information Security Management Forum)

ISMS Système de gestion de la sécurité de l'information (Information Security Management System)

IT Technologie informatique (Information Technology)

SLA Contrat de service (Service Level Agreement)

SOA Déclaration d'applicabilité (Statement of Applicability)

5 Sécurité de l'information de santé

5.1 Objectifs de la sécurité de l'information de santé

Les principaux objectifs de la sécurité de l'information résident dans la protection de la confidentialité, de la disponibilité et de l'intégrité (dont l'authenticité, l'imputabilité et l'auditabilité) des informations. Dans le domaine des soins médicaux, 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, des mesures doivent également être prises pour conserver l'intégrité des données. Si ce n'est que parce qu'il est possible de corrompre l'intégrité des données de contrôle d'accès, des traces d'audit, et d'autres systèmes de données par le biais de techniques permettant la violation de documents confidentiels, 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 entraîner des maladies, des blessures ou même la mort. De même, une disponibilité élevée en matière d'information est une qualité très importante pour les systèmes de santé puisque le temps est un facteur primordial dans l'administration des traitements. En effet, des incidents pourraient provoquer des ruptures dans des systèmes informatiques ne relevant pas du domaine de la santé au moment où l'obtention de l'information est une question de vie ou de mort. De même, les attaques par refus de service contre les systèmes réseau sont de plus en plus fréquentes.

Les contrôles abordés dans l'Article 7 sont propres au domaine de la santé afin de protéger la confidentialité, l'intégrité et la disponibilité des informations personnelles de santé ainsi que pour garantir l'auditabilité et l'imputabilité de l'accès à ces informations. Ces contrôles contribuent à éviter les erreurs médicales qui peuvent survenir lorsque l'intégrité des informations de santé n'a pas su être préservée. Elles contribuent également à garantir une certaine cohérence dans les soins médicaux prodigués.

Des considérations supplémentaires déterminent les objectifs de la sécurité des informations médicales. Elles comprennent

a) l'observation des obligations législatives, telles qu'exprimées dans les droits et les réglementations de données de protection applicables à la protection du respect de la vie privée du patient[3];

b) préserver ledit respect de la vie privée et des meilleures pratiques de sécurité dans le domaine de l'informatique de santé;

c) préserver l'imputabilité de chacun et de l'organisme au sein de l'ensemble des organismes et des professionnels de la santé;

d) aider à la mise en œuvre de la gestion systématique des risques au sein des organismes de santé;

e) répondre aux besoins en matière de sécurité identifiés lors de situations médicales communes;

f) diminuer les 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 médicales en cours;

g) garder la confiance du public dans les organismes de santé ainsi que dans les systèmes sur lesquels reposent ces organismes;

h) préserver les normes professionnelles et la déontologie, telles que les organismes professionnels relatifs à la santé les ont établies (à partir du moment où la sécurité de l'information préserve la confidentialité et l'intégrité des informations de santé);

i) mettre en place des systèmes électroniques d'informations de santé au sein d'un environnement correctement sécurisé contre les menaces;

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

j) faciliter l'interopérabilité parmi les systèmes de santé étant donné que les informations de santé circulent de plus en plus entre les organismes et à travers les 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).

5.2 Sécurité de l'information au sein du contrôle de l'information[4)]

Ces dernières années, la gouvernance d'entreprise est devenue un problème majeur pour les organismes en tout genre, en réponse aux mouvements réglementaires incarnés par des initiatives telles la loi Sarbanes Oxley et la loi Health Insurance Portability and Accountability aux États-Unis, l'accord européen de Bâle II, le rapport Turnbull au Royaume-Uni ou encore par la loi KontraG en Allemagne. De même, la dépendance croissante des organismes vis-à-vis des informations et des technologies connexes donne énormément d'importance au contrôle de l'information dans le cadre des processus de gestion des risques fonctionnels.

De nombreux domaines de la gestion de l'information, telles l'accréditation et la protection de données, peuvent être considérés comme appartenant au domaine du contrôle de l'information. Il est extrêmement important que le domaine du contrôle de l'information se joigne à l'effort de déploiement actuel en termes de sécurité de l'information afin que soit toujours portée l'attention requise à la confidentialité, à l'intégrité et à la disponibilité. La sécurité de l'information apparaît clairement comme un aspect essentiel de l'élargissement des aspects de la gouvernance des informations.

5.3 Contrôle de l'information au sein de la gouvernance clinique et d'entreprise

Alors que les organismes de santé peuvent différer à propos de la gouvernance clinique et de la gouvernance d'entreprise, l'importance de l'intégration et du suivi du contrôle de l'information devrait les mettre d'accord. Tandis que les organismes de santé deviennent de plus en plus dépendants des systèmes d'informations relatifs à 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 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 engendrent 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 possèdent sans aucun doute des études de cas dans lesquelles ces failles ont conduit à des erreurs de diagnostic, à des décès ou à des rétablissements retardés. Les fondements de la gouvernance clinique doivent donc accorder autant d'importance à la gestion efficace du management 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 à contenu médical.

5.4 Informations de santé devant être protégées

Il existe plusieurs types d'informations dont la confidentialité, l'intégrité et la disponibilité[5)] doivent être protégées:

a) les informations personnelles de santé;

b) les données de pseudonymisation issues des informations personnelles de santé par le biais d'une certaine méthodologie d'identification des pseudonymes;

c) les données statistiques et de recherche, dont les données d'anonymisation issues des informations personnelles de santé par suppression des données d'identification personnelle;

d) les connaissances cliniques/médicales sans rapport avec un sujet de soins particulier, dont les données d'aide à la décision médicale (par exemple les données sur les réactions indésirables conséquentes à la prise d'un médicament);

4) Dans certains pays, l'expression «assurance des informations» est synonyme de «contrôle de l'information».

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