Norme internationale

ISO 27799

Informatique de santé — Contrôles de sécurité de l'information dans le domaine de la santé basés sur l'ISO/IEC 27002

Health informatics — Information security controls in health based on ISO/IEC 27002

Troisième édition
2025-12

Numéro de référence
ISO 27799:2025(fr)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 215, *Informatique de santé*, en collaboration avec le comité technique CEN/TC 251, *Informatique de santé*, du Comité européen de normalisation (CEN), *Informatique de santé,* conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette troisième édition annule et remplace les normes ISO 27799:2016 et ISO/TS 14441:2013, qui ont fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— l'alignement sur la nouvelle structure de la norme ISO/IEC 27002:2022 et les autres modifications apportées à cette norme par rapport à la version précédente;

— la révision et l'ajout de contrôles spécifiques à la santé;

— la suppression d'éléments qui ne figuraient à l'origine que dans la deuxième édition du présent document, mais qui ont été inclus par la suite dans la norme ISO/CEI 27002:2022;

— ajout d'Annexes informatives fournissant des recommandations relatives à la cybersécurité dans les organismes de santé et, sur la base de ISO/TS 14441:2013, 5.3, mise à jour des exemples d'exigences en matière de sécurité et de protection de la vie privée pour les systèmes d'information de santé.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

0.1 Généralités

Le présent document contient un ensemble de contrôles de la sécurité de l'information pour les organismes de santé. Il prend en considération tous les contrôles de la norme ISO/IEC 27002:2022 et, dans certains cas, complète les contrôles ou fournit des recommandations pour leur application dans le domaine de la santé. Il existe également quelques contrôles supplémentaires spécifiques à la santé qui ne sont dérivés d'aucun des contrôles de la norme ISO/IEC 27002:2022.

0.2 Contexte et historique

Les facteurs qui ont une incidence sur la sécurité de l'information dans les soins de santé sont notamment les suivants:

a) Utilisation d'un équipement dont le fonctionnement repose sur les technologies numériques et qui est déployé exclusivement ou majoritairement dans le domaine de la santé. Les dispositifs médicaux intégrant des logiciels de santé en sont le meilleur exemple.

b) La nécessité de trouver un équilibre entre la sécurité et l'efficacité cliniques et la sécurité de l'information.

c) Préserver la vie privée des personnes soignées tout en assurant l'accès aux informations personnelles pertinentes en matière de santé à des fins de diagnostic et de traitement.

d) La nature distribuée des informations personnelles sur la santé, à la fois au sein des organisations et entre elles (éventuellement dans des juridictions différentes), entraîne la nécessité de niveaux élevés d'interopérabilité entre divers systèmes, applications et dispositifs.

e) Les usagers sont très divers: médecins, infirmières, autres cliniciens, stagiaires, étudiants, aides-soignants, techniciens, personnel administratif et bénévoles, ainsi que les personnes soignées et leurs mandataires.

f) Les multiples interdépendances et flux d'informations entre et au sein des organisations responsables d'un ou plusieurs des domaines suivants: soins de santé, recherche clinique, enseignement, éducation et formation.

g) La nécessité pour certains services de santé d'être disponibles en permanence (24 heures sur 24, tous les jours) dans des circonstances normales. En outre, les catastrophes naturelles et autres événements inhabituels qui peuvent entraîner une augmentation de la demande de services de soins de santé.

h) Les organismes fournissant des services de santé ainsi que les fabricants ou fournisseurs de systèmes, d'appareils et d'équipements sont tous soumis à un large éventail d'exigences légales, statutaires, réglementaires et contractuelles qui peuvent varier d'une juridiction à l'autre.

i) Exigences superposées ou incomplètes en matière d'obligation de rendre compte et de responsabilité professionnelle entre différentes professions (telles que le personnel des TIC et des dispositifs médicaux) pour assurer la sécurité et la sûreté des systèmes, des dispositifs et des équipements.

Dans ce contexte général, les soins de santé ont un certain nombre d'exigences spécifiques, voire uniques, en matière de sécurité de l'information. Toutefois, les contrôles figurant dans la norme ISO/IEC 27002:2022 sont intentionnellement génériques, d'où la nécessité du présent document.

0.3 Public et utilisations

Le présent document s'adresse aux organisations qui:

— fournissent des services de soins de santé ou sont dépositaires d'informations personnelles sur la santé pour d'autres raisons;

— fournir des logiciels, des systèmes, des dispositifs, des équipements ou des services qui sont utilisés pour traiter les informations de santé à caractère personnel;