



**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*

iTeh Standards
[**\(https://standards.iteh.ai\)**](https://standards.iteh.ai)
Document Preview

[ISO 27799:2025](#)

<https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-27799-2025>

iTeh Standards

(<https://standards.iteh.ai>)

Document Preview

[ISO 27799:2025](#)

<https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-27799-2025>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2025

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, 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, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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	vi
Introduction	vii
1 Domaine d'application	1
2 Références normatives	1
3 Termes, définitions et abréviations	2
3.1 Termes et définitions	2
3.2 Abréviations	3
4 Généralités	3
4.1 Structure du présent document	3
4.2 Sécurité	4
4.3 Sélection et application des contrôles	4
4.3.1 Détermination des contrôles	4
4.3.2 Recommandations pour l'application de la loi	4
4.3.3 Utilisation avec la norme ISO/IEC 27001:2022	5
5 Contrôles organisationnels	5
5.1 Politiques de sécurité de l'information	5
5.2 Rôles et responsabilités en matière de sécurité de l'information	7
5.3 Séparation des tâches	7
5.4 Responsabilités de la direction	8
5.5 Contact avec les autorités	8
5.6 Contact avec des groupes d'intérêt	8
5.7 Renseignements sur les menaces	8
5.8 Sécurité de l'information dans la gestion de projet	9
5.9 Inventaire des informations et autres actifs associés	9
5.10 Utilisation acceptable de l'information et des autres actifs associés	9
5.11 Rendement des actifs	9
5.12 Classification des informations	10
5.13 Marquage des informations	11
5.14 Transfert d'informations	11
5.15 Contrôle d'accès	12
5.16 Gestion de l'identité	12
5.17 Informations d'authentification	13
5.18 Droits d'accès	13
5.19 Sécurité de l'information dans les relations avec les fournisseurs	14
5.20 Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs	15
5.21 Gérer la sécurité de l'information dans la chaîne d'approvisionnement des TIC	15
5.22 Suivi, révision et gestion des changements des services des fournisseurs	15
5.23 Sécurité de l'information dans l'utilisation de services en nuage	15
5.24 Planification et préparation de la gestion des incidents de sécurité de l'information	15
5.25 Évaluation et décision sur les événements liés à la sécurité de l'information	15
5.26 Réponse aux incidents liés à la sécurité de l'information	16
5.27 Tirer les leçons des incidents liés à la sécurité de l'information	16
5.28 Recueil de preuves	16
5.29 Sécurité de l'information en cas de perturbation	16
5.30 Préparation des TIC pour la continuité d'activité	16
5.31 Exigences légales, statutaires, réglementaires et contractuelles	17
5.32 Droits de propriété intellectuelle	17
5.33 Protection des enregistrements	17
5.34 Vie privée et protection des IPI	17
5.35 Examen indépendant de la sécurité de l'information	19
5.36 Conformité aux politiques, règles et normes de sécurité de l'information	19
5.37 Procédures d'exploitation documentées	19

5.38	HLT – Analyse et spécification des exigences en matière de sécurité de l'information.....	20
5.39	HLT – Identification unique des sujets de soins.....	21
5.40	HLT – Validation des données affichées/imprimées.....	22
5.41	HLT – Informations sur la santé accessibles au public.....	22
5.42	HLT – Communication d'urgence.....	23
5.43	HLT – Rapport d'incident externe.....	24
6	Contrôle des personnes.....	24
6.1	Présélection.....	24
6.2	Conditions d'emploi.....	25
6.3	Sensibilisation, apprentissage et formation à la sécurité de l'information.....	25
6.4	Processus disciplinaire.....	25
6.5	Responsabilités après un licenciement ou un changement d'emploi.....	26
6.6	Accords de confidentialité ou de non-divulgation.....	26
6.7	Travail à distance.....	26
6.8	Rapport sur les événements liés à la sécurité de l'information.....	27
6.9	HLT – Formation à la gestion.....	27
7	Contrôles physiques.....	28
7.1	Périmètres de sécurité physique.....	28
7.2	Entrée physique.....	28
7.3	Sécurisation des bureaux, des salles et des équipements.....	28
7.4	Surveillance de la sécurité physique.....	29
7.5	Protection contre les menaces physiques et environnementales.....	29
7.6	Travail dans les zones sécurisées.....	29
7.7	Bureau et écran dégagés.....	29
7.8	Emplacement et protection du matériel.....	29
7.9	Sécurité des actifs hors des locaux.....	29
7.10	Supports de stockage.....	30
7.11	Services généraux.....	30
7.12	Sécurité du câblage.....	31
7.13	Maintenance du matériel.....	31
7.14	Élimination ou réutilisation des équipements en toute sécurité.....	31
8	Contrôles technologiques.....	32
8.1	Terminaux finaux des utilisateurs.....	32
8.2	Droits d'accès privilégiés.....	32
8.3	Restriction d'accès à l'information.....	32
8.4	Accès au code source.....	32
8.5	Authentification sécurisée.....	32
8.6	Dimensionnement.....	33
8.7	Protection contre les logiciels malveillants.....	33
8.8	Gestion des vulnérabilités techniques.....	33
8.9	Gestion de la configuration.....	34
8.10	Suppression d'informations.....	34
8.11	Masquage des données.....	34
8.12	Prévention de la fuite de données.....	35
8.13	Sauvegarde de l'information.....	35
8.14	Redondance des moyens de traitement de l'information.....	35
8.15	Journalisation.....	35
8.16	Activités de surveillance.....	35
8.17	Synchronisation des horloges.....	35
8.18	Utilisation de programmes utilitaires à priviléges.....	36
8.19	Installation de logiciels sur des systèmes en exploitation.....	36
8.20	Sécurité des réseaux.....	36
8.21	Sécurité des services de réseau.....	36
8.22	Cloisonnement des réseaux.....	36
8.23	Filtrage du web.....	37
8.24	Utilisation de la cryptographie.....	37
8.25	Cycle de vie de développement sécurisé.....	37

8.26	Exigences de sécurité des applications.....	37
8.27	Principes d'architecture et d'ingénierie des systèmes sécurisés.....	37
8.28	Codage sécurisé	38
8.29	Tests de sécurité dans le développement et l'acceptation	38
8.30	Développement externalisé	38
8.31	Séparation des environnements de développement, de test et de production.....	38
8.32	Gestion des changements.....	38
8.33	Informations sur les tests.....	38
8.34	Protection des systèmes d'information pendant les tests d'audit.....	39
8.35	HLT – Principes de la confiance zéro.....	39
	Annexe A (informative) Contrôles de sécurité de l'information pour les références de santé	40
	Annexe B (informative) Correspondance du présent document avec la norme ISO 27799:2016.....	42
	Annexe C (informative) Sécurité de l'information dans les organismes de santé	43
	Annexe D (informative) Exemples d'exigences en matière de sécurité et de confidentialité pour les systèmes d'information sur la santé et leur mise en correspondance avec les contrôles ISO 27799 et les capacités de sécurité IEC/TS 81001-2-2	55
	Bibliographie.....	81

iTeh Standards

(<https://standards.iteh.ai>)

Document Preview

[ISO 27799:2025](https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-27799-2025)

<https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-27799-2025>

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). standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-27799-2025

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 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;