Directives de mise en œuvre MNM Etablissements de soins (ISO27001)

A.5 Politique de sécurité de l'information

A.5.1 Orientation de la direction en matière de sécurité de l'information

Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

A.5.1.1 Politiques de sécurité de l'information

Mesure de gestion (ISO 27001)	SOA[1]	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de définir un ensemble de politiques en matière de sécurité de l'information qui soit approuvé par la direction, diffusé et communiqué aux membres du personnel et aux tiers concernés	Y	Il convient que les organisations définissent, à leur plus haut niveau, une «politique de sécurité de l'information», qui soit approuvée par la direction et qui décrive l'approche adoptée pour gérer les objectifs de sécurité de l'information. Il convient que les politiques de sécurité de l'information traitent des exigences créées par : a) la stratégie d'entreprise, b) les réglementations, la législation et les contrats; c) l'environnement réel et anticipé des menaces liées à la sécurité de l'information. Il convient que cette politique de sécurité de l'information comporte des précisions concernant : a) une définition de la sécurité de l'information, ses objectifs et ses principes pour orienter toutes les activités relatives à la sécurité de l'information; b) l'attribution de responsabilités générales et spécifiques en matière de gestion de la sécurité de l'information à des fonctions définies; c) des processus de traitement des dérogations et des exceptions. Il convient qu'à un niveau inférieur, la politique de sécurité de l'information soit étayée par des politiques portant sur des thèmes spécifiques, qui imposent en outre la mise en œuvre de mesures de sécurité de l'information et sont de manière générale structurées pour répondre aux besoins de certains groupes cibles d'une organisation ou pour englober certains thèmes. Quelques exemples de politiques à thèmes : a) le contrôle d'accès (voir le chapitre 9) ; b) la classification (et le traitement) de l'information (voir 8.2) ; c) la sécurité physique et environnementale (voir le chapitre 11) ; d) thèmes axés sur l'utilisateur final : 1) utilisation correcte des actifs (voir 8.1.3) ; 2) 'clear desk' et 'clear screen' (voir 11.2.9); 3) transfert de l'information (voir 13.2.1) ; 4) appareils mobiles et télétravail (voir 6.2) 5) restrictions en matière d'installation et d'utilisation de logiciels (voir 12.6.2); e) sauvegarde (voir 12.3); f) transport de l'information (voir 13.2) ; g) protection contre les logiciels malveillants (voir 12.2); h) gestion des vulnérabilités techniques (voir 12.6.1);	Il convient que la politique de sécurité de l'information comporte des précisions concernant : a) la nécessité d'une protection des données relatives à la santé; b) les objectifs de la protection des données relatives à la santé; c) le champ d'application en ce qui concerne le respect, tel que décrit au chapitre 18; d) les exigences réglementaires et les exigences contractuelles, notamment les exigences de protection des données à caractère personnel relatives à la santé et les responsabilités légales et éthiques des prestataires de soins en ce qui concerne la protection de ces informations; e) un dispositif pour la notification d'incidents de sécurité de l'information, notamment un canal par le biais duquel des inquiétudes au niveau de la confidentialité peuvent être formulées sans peur d'accusations ou de reproches; f) l'identification de processus et systèmes d'importance vitale pour les soins (« vital » signifie que leur interruption peut avoir des conséquences néfastes pour le patient). Idéalement, la révision du contenu de la politique est basée sur les constatations de l'évaluation des risques de l'organisation, même si la politique est uniquement censée orienter, définir des principes et renvoyer à d'autres documents contentant les détails spécifiques (et susceptibles d'être modifiés plus souvent). Lors de la rédaction du document de politique en matière de sécurité de l'information, les établissements de soins doivent prendre en compte les facteurs suivants propres aux soins de santé : g) l'ampleur des informations de santé ;

[1] SOA: Statement of Applicability (ou Déclaration d'applicabilité)

		i) mesures de sécurité cryptographiques (voir le chapitre 10) ; j) sécurité des communications (voir le chapitre 13) ; k) protection de la vie privée et des données à caractère personnel (voir 18.1.4); l) relations avec les fournisseurs (voir le chapitre 15). Il convient que ces politiques soient communiquées aux membres du personnel et aux tiers concernés sous une forme pertinente, accessible et compréhensible par leurs destinataires, par exemple dans le contexte d'un «programme d'apprentissage, de formation et de sensibilisation à la sécurité de l'information» (voir 7.2.2).	h) les droits et les responsabilités éthiques du personnel, comme prévus par la loi et acceptés par les membres des organisations professionnelles; i) si d'application, les droits des patients à la protection de la vie privée et à la consultation de leur dossier j) les obligations des prestataires de soins d'obtenir le consentement éclairé des patients et de respecter la confidentialité des données à caractère personnel relatives à la santé; k) les besoins légitimes de prestataires de soins et établissements de soins de négliger les protocoles de sécurité normaux lorsque des priorités de soins, souvent liées à l'incapacité du patient de faire connaître ses souhaits, l'exigent ; ainsi que les procédures à mettre en œuvre pour permettre ceci ; l) les obligations des établissements de soins et des patients lorsque les soins sont administrés sur la base de « soins partagés » ou de « soins de longue durée »; m) les protocoles et procédures qui doivent être appliqués au partage d'informations dans le cadre de la recherche et d'études cliniques; n) les règlements et limites de compétences du personnel temporaire, tels que remplaçants, étudiants, etc. o) les règlements et restrictions imposées en ce qui concerne l'accès aux données à caractère personnel relatives à la santé par des bénévoles et du personnel de soutien, tels que les prêtres ou institutions caritatives; p) les implications des mesures de sécurité pour la sécurité des patients ; q) les implications des mesures de protection des données pour les prestations des systèmes d'information de la santé; Bon nombre d'établissements de santé ont décidé qu'il était pratique de mettre le document de politique à la disposition du personnel par la voie électronique dans la rubrique « sécurité de l'information » sur l'intranet de l'organisation. Scope : la sécurité de l'information n'est pas limitée aux informations relatives à la santé. La politique du personnel, la comptabilité, etc. sont également concernées. Il est cependant possible d'élaborer des mesures spécifiques et de se concentrer sur les processus qui sont uniquement d'application aux informations relatives à la santé.

A.5.1.2 Évaluation de la politique de sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité des politiques liées à la sécurité de l'information, il convient de revoir ces politiques à intervalles programmés ou en cas de changements majeurs.	Y	Il convient que chaque politique ait un propriétaire ayant accepté la responsabilité de développer, revoir et évaluer cette politique. Il convient que la revue comporte une appréciation des possibilités d'amélioration de la politique de l'organisation et une approche de management de la sécurité de l'information pour répondre aux changements intervenant dans l'environnement organisationnel, aux circonstances liées à l'activité, au contexte juridique ou à l'environnement technique. Il convient que la revue des politiques de sécurité de l'information tienne compte des revues de direction. Une fois révisée, il convient que la politique de sécurité soit approuvée par la direction.	Cette évaluation porte sur les aspects suivants : a) l'évolution de la gestion de l'établissement de santé et les changements consécutifs en ce qui concerne le profil de risque et les besoins de gestions des risques; b) les modifications à l'infrastructure IT de l'organisation et les changements consécutifs du profil de risque de l'organisation; c) les changements identifiés dans l'environnement externe qui ont un impact sur le profil de risque de l'organisation; d) les nouvelles mesures de gestion, les exigences et règles en matière de respect et sécurité qui sont rendues obligatoires par des instances de la santé d'une juridiction ou par une nouvelle législation ou réglementation; e) les nouvelles directives et recommandations d'organisations de prestataires de soins et de membres de commissions de protection de la vie privée en ce qui concerne la protection des données à caractère personnel relatives à la santé; f) les résultats de jugements rendus par le tribunal, qui créent ou infirment des précédents ou sur base desquels des « best practices » sont établies; g) les défis et éléments importants de la politique, tels que communiqués à l'organisation par le personnel, les patients et leurs partenaires ou les prestataires, de soins, les chercheurs et les autorités (p.ex. membres des commissions de protection de la vie privée).; h) les rapports d'incidents relatifs à la sécurité des patients afin d'éviter ces accidents lorsqu'ils sont la conséquence d'une défaillance des mesures de sécurité de l'information.

A.6 Organisation de la sécurité de l'information

A.6.1 Organisation interne

Objectif: Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation.

A.6.1.1 Fonctions et responsabilités liées à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins

Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information.	Y	Il convient d'attribuer les responsabilités en matière de sécurité de l'information conformément à la politique de sécurité de l'information (voir 5.1.1). Il convient de déterminer les responsabilités en ce qui concerne la protection des actifs individuels et la mise en œuvre de processus de sécurité spécifiques. Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et, en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information. Il convient de déterminer les responsabilités locales en ce qui concerne la protection des actifs et la mise en œuvre des processus de sécurité spécifiques. Les personnes auxquelles ont été attribuées des responsabilités en matière de sécurité peuvent déléguer des tâches de sécurité. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée. Il convient de préciser les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes : a) il convient d'identifier et de déterminer les actifs et les processus de sécurité; b) il convient d'affecter une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail (voir 8.1.2); c) il convient de définir et de documenter les différents niveaux d'autorisation; d) pour être à même d'assurer les responsabilités relevant de leur domaine en matière de sécurité, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de possibilités leur permettant de se tenir au courant des évolutions ; e) il convient d'identifier et de documenter les activités de coordination et de supervision relatives aux questions de sécurité liées aux relations avec les fournisseurs.	*Il est important de souligner le caractère essentiel de la responsabilité de gestion dans des organisations qui gèrent des données à caractère personnel relatives à la santé, comme décrit sous B.2. La responsabilité et la coordination ne pourront être maintenues à long terme que si l'organisation dispose explicitement d'une infrastructure de gestion de la sécurité de l'information.* *Quelle que soit la structure organisationnelle, il est essentiel qu'elle soit conçue et structurée de sorte à permettre l'accès des patients (p.ex. demande d'obtention de données à caractère personnel relatives à la santé) et la possibilité de rapportage au sein de* *la structure organisationnelle et à garantir une communication des informations dans les délais requis.* *Comme mentionné sous B.4.3, le délégué à la protection des données (virtuel ou réel) de l'organisation est tenu notamment de rapporter au forum et de lui fournir des services de secrétariat. Le délégué est responsable d'établir, de publier et de commenter les rapports reçus par les membres du forum.* *Les organisations de santé doivent faire connaître les détails du champ d'application au sein de l'organisation, les évaluer et garantir qu'ils soient pris en compte par les groupes au sein de l'organisation qui sont chargés de la gouvernance en matière d'information et de la gouvernance clinique et d'entreprise.* Certaines tâches reviennent plutôt au médiateur et non au DPO. Les responsabilités et tâches accordées à chaque fonction (DPO, conseiller en sécurité) sont définies par la loi. La fonction de médiateur n'a pas rapport à la sécurité de l'information (concerne plutôt le fonctionnement de l'hôpital), cette fonction n'est donc pas abordée ici. Les explications ci-dessus proviennent des normes NEN (Pays-Bas) et la terminologie utilisée diffère de celle employée en Belgique. La situation locale dans les hôpitaux belges peut donc différer de ces directives (qui ne sont d'ailleurs pas contraignantes). Il appartient aux hôpitaux de formuler eux-mêmes une éventuelle proposition adaptée pour les directives de mise en œuvre de cette norme.

A.6.1.2 Séparation des tâches

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de séparer les tâches et les domaines de responsabilité incompatibles pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.	Y	Il convient de veiller à ce que personne ne puisse accéder à, modifier ou utiliser des actifs sans en avoir reçu l'autorisation ou sans avoir été détecté. Il convient de séparer le déclenchement d'un événement de son autorisation. Il convient d'envisager la possibilité de collusion lors de la conception des mesures. Les organisations de petite taille peuvent avoir des difficultés à réaliser une séparation des tâches, mais il convient d'appliquer ce principe dans la mesure du possible. Lorsqu'il est difficile de procéder à la séparation des tâches, il convient d'envisager d'autres mesures comme la surveillance des activités, des systèmes de traçabilité et la supervision de la direction.	

A.6.1.3 Relations avec les autorités

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'entretenir des relations appropriées avec les autorités compétentes.	N	Il convient que les organisations mettent en place des procédures spécifiant quand et comment il convient de contacter les autorités compétentes (par exemple, les autorités chargées de l'application des lois, les organismes de réglementation, les autorités de surveillance). Ces procédures définissent également comment il convient de signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (par exemple, en cas de suspicion de violation de la loi).	Pourquoi est-ce hors du scope ? Motivation. (SOA=N) (Support central ?) Porte uniquement sur la sécurité de l'information, exemple CCB, APD, ... Il convient d'entretenir les contacts ad hoc ou uniquement dans des situations spécifiques (incidents, interrogation concernant ransomware, phishing, cybercriminalité, ...). Est-il utile d'établir des protocoles entre plusieurs parties ? (demande beaucoup de travail, est-ce utile ?) Il existe suffisamment de canaux de communication.

A.6.1.4 Relations avec des groupes de travail spécialisés

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'entretenir des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles.	N	Il convient d'envisager une inscription à des groupes d'intérêt ou à des forums spécialisés aux fins suivantes : a) mieux connaître les bonnes pratiques et se tenir informé de l'évolution des savoirs relatifs à la sécurité; b) s'assurer que la connaissance de l'environnement de la sécurité de l'information est à jour et exhaustive; c) recevoir rapidement des alertes, des conseils et des correctifs logiciels portant sur les attaques et les vulnérabilités ; d) avoir accès à des conseils de spécialistes sur la sécurité de l'information ;	Voir ci-dessus, support central. Mêmes remarques.

		e) partager et échanger des informations sur les nouvelles technologies, les produits, les menaces ou les vulnérabilités ; f) mettre en place des relais d'information appropriés lors du traitement d'incidents liés à la sécurité de l'information .	

A.6.1.5 La sécurité de l'information dans la gestion de projet

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de traiter la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.	Y	Il convient d'intégrer la sécurité de l'information dans la ou les méthodes de gestion de projet de l'organisation pour veiller à ce que les risques de sécurité de l'information soient identifiés et traités dans le cadre du projet Cette préconisation s'applique de manière générale à tout projet quel qu'il soit, indépendamment de sa nature, par exemple un projet lié à un processus clé de l'activité, aux technologies de l'information, à la gestion des installations et autres processus. Il convient que les méthodes de gestion de projet en vigueur imposent que: a) les objectifs en matière de sécurité de l'information soient intégrés aux objectifs du projet; b) une appréciation du risque de sécurité de l'information soit effectuée au commencement du projet pour identifier les mesures nécessaires; c) la sécurité de l'information soit intégrée à toutes les phases de la méthodologie de projet appliquée. Pour tous les projets, il convient de traiter et de revoir régulièrement les incidences sur la sécurité de l'information Il convient de déterminer et d'attribuer les responsabilités en matière de sécurité de l'information à des fonctions spécifiques définies dans les méthodes de gestion de projet	La sécurité du patient est un aspect critique de l'évaluation des risques pour chaque projet où il est question d'un traitement de données à caractère personnel relatives à la santé. Il convient d'analyser en détail les risques pour la sécurité du patient et d'y prêter attention.

A.6.2 Appareils mobiles et télétravail

Objectif: Assurer la sécurité du télétravail et l'utilisation d'appareils mobiles.

A.6.2.1 Politique en matière d'appareils mobiles

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles.	Y	Lors de l'utilisation d'appareils mobiles, il convient de veiller particulièrement à ce que les informations liées à l'activité de l'organisation ne soient pas compromises. Il convient que la politique en matière d'appareils mobiles tienne compte des risques liés au fait de travailler avec des appareils mobiles dans des environnements non protégés. Il convient que la politique en matière d'appareils mobiles envisage: a) l'enregistrement des appareils mobiles; b) les exigences liées à la protection physique; c) les restrictions liées à l'installation de logiciels; d) les exigences liées aux versions logicielles des appareils mobiles et à l'application de correctifs ; e) les restrictions liées aux connexions à des services d'information; f) les contrôles d'accès; g) les techniques cryptographiques; h) la protection contre les logiciels malveillants;	Les organisations sont tenues : a) d'évaluer les risques spécifiques qui vont de pair avec l'utilisation d'appareils mobiles dans les soins; b) de définir une politique en ce qui concerne les mesures de précaution à prendre lors de l'utilisation d'appareils informatiques mobiles, notamment des directives et restrictions en matière d'utilisation d'appareils personnels au sein de l'organisation, ainsi que des mesures de gestion afin de satisfaire aux exigences légales applicables en matière de protection de la vie privée; c) d'imposer aux utilisateurs d'appareils mobiles le respect de cette politique.

		i) la désactivation, l'effacement des données ou le verrouillage à distance; j) les sauvegardes; k) l'utilisation des services web et des applications web. Il convient d'être vigilant lors de l'utilisation d'appareils mobiles dans des lieux publics, des salles de réunions et autres zones non protégées. Il convient de mettre en place des mesures de protection visant à empêcher les accès non autorisés ou la divulgation d'informations stockées et traitées par ces appareils, par exemple en utilisant des techniques cryptographiques (voir chapitre 10) et en imposant l'utilisation d'informations d'authentification secrètes (voir 9.2.4). Il convient également que les appareils mobiles soient physiquement protégés contre le vol, en particulier lorsqu'ils sont laissés, par exemple, dans un véhicule privé ou tout autre moyen de transport, une chambre d'hôtel, un centre de congrès ou une salle de réunion Il convient d'établir une procédure spécifique tenant compte des exigences juridiques, des exigences liées aux assurances et des exigences de sécurité de l'organisation, en cas de vol ou de perte d'appareils mobiles. Il convient de ne pas laisser sans surveillance les appareils dans lesquels sont stockées des informations importantes, sensibles ou critiques liées à l'activité de l'organisation et, si possible, de les mettre sous clé ou de les doter de systèmes de verrouillage spéciaux. Il convient d'organiser, à destination des personnes utilisant des appareils mobiles, des formations de sensibilisation aux risques supplémentaires liés à ce mode de travail et aux mesures de sécurité qu'il convient de mettre en œuvre. Lorsque la politique en matière d'appareils mobiles autorise l'utilisation d'appareils mobiles personnels, il convient que la politique et les mesures de sécurité complémentaires envisagent également: a) une séparation entre l'utilisation privée et l'utilisation professionnelle des appareils, impliquant la mise en œuvre d'un logiciel pour faciliter cette séparation et protéger les données liées à l'activité de l'organisation figurant sur un appareil privé; b) de ne permettre l'accès aux informations de l'organisation que lorsque l'utilisateur a signé un contrat d'utilisateur final par lequel il prend acte de ses missions (protection physique, mise à jour des logiciels, etc.), renonce à la propriété des données de l'organisation et autorise l'entreprise à effacer ses données à distance en cas de perte ou de vol de l'appareil, ou lorsque son utilisation n'est plus autorisée. Cette politique doit tenir compte de la législation en vigueur sur la protection de la vie privée.	Les connexions sans fil, bien que comparables aux réseaux câblés, présentent quelques différences du point de vue de la sécurité de l'information. Certains protocoles de chiffrement sans fil, tels que Wired Equivalent Privacy (WEP), sont toujours utilisés bien qu'ils soient peu efficaces en raison de leurs point faibles connus. Par ailleurs, les informations enregistrées sur les appareils mobiles ne font pas toujours l'objet de sauvegardes (p.ex. en raison de la largeur de bande limitée ou parce que l'appareil n'est pas connecté aux moments de prise de sauvegardes).

A.6.2.2 Télétravail

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en oeuvre une politique et des mesures de sécurité complémentaires pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.	Y	Il convient que les organisations autorisant les activités de télétravail émettent une politique définissant les conditions et les restrictions d'utilisation liées au télétravail. Il convient d'envisager les aspects suivants si la loi l'autorise et que l'on estime qu'ils sont pertinents: a) le niveau de sécurité physique en place sur le site de télétravail, y compris le niveau de sécurité physique du bâtiment et de l'environnement immédiat; b) l'environnement physique de télétravail proposé; c) les exigences en matière de sécurité des communications, en tenant compte de la nécessité d'accéder à distance aux systèmes internes de l'organisation, de la sensibilité	Les organisations sont tenues : a) de définir une politique en ce qui concerne les mesures de précaution à prendre en cas de télétravail; b) de veiller à ce que les utilisateurs de systèmes d'information de la santé qui font du télétravail respectent cette politique.

		des informations consultées ou transmises via le réseau de communication et de la sensibilité du système interne d) la fourniture de l'accès à un bureau virtuel, évitant le traitement et le stockage des informations sur un équipement détenu à titre privé; e) la menace que représente l'accès non autorisé aux informations ou ressources par d'autres personnes présentes dans l'espace, par exemple des membres de la famille, des amis; f) l'utilisation de réseaux domestiques et les exigences ou les restrictions relatives à la configuration des réseaux sans fil; g) les politiques et procédures mises au point pour prévenir tout litige relatif aux droits de propriété intellectuelle sur des actifs créés sur un matériel détenu à titre privé; h) l'accès au matériel détenu à titre privé (pour vérifier le niveau de sécurité de la machine ou lors d'une enquête), susceptible d'être interdit par la loi; i) les contrats de licence logicielle pouvant rendre l'organisation responsable de l'octroi des licences pour les logiciels clients des postes de travail détenus à titre privé par des salariés et des utilisateurs tiers; j) les exigences relatives à la protection antivirus et au pare-feu. Il convient d'inclure aux lignes directrices et aux dispositions à prendre en compte: a) la fourniture des matériels et des meubles de rangement adaptés aux activités de télétravail, en cas d'interdiction d'utilisation d'un matériel détenu à titre privé et non soumis au contrôle de l'organisation; b) la définition des tâches autorisées, les heures de travail, la classification des informations susceptibles d'être détenues, ainsi que les systèmes et services internes auxquels le télétravailleur est autorisé à accéder; c) la fourniture d'un appareil de communication approprié, ainsi que des méthodes de sécurisation de l'accès à distance; d) la sécurité physique; e) les règles et préconisations concernant l'accès de la famille et des visiteurs au matériel et aux informations; f) la fourniture de services d'assistance et de maintenance matérielles et logicielles; g) la souscription d'une assurance; h) les procédures relatives à la sauvegarde et à la continuité de l'activité; i) l'audit et la surveillance liée à la sécurité; j) la révocation des droits d'utilisation et des droits d'accès, ainsi que la restitution du matériel au terme des activités de télétravail.	Certaines juridictions (p.ex. en Allemagne) ont déjà mis des restrictions au télétravail par des prestataires de soins. Il faut tenir compte du fait que le télétravail dans les soins est susceptible de passer les frontières d'une juridiction et peut même être effectué à bord d'un avion ou navire se situant en dehors de toute juridiction nationale. Il se peut que les équipes internationales qui prêtent de l'aide lors de calamités utilisent à l'avenir des systèmes d'information de la santé de juridictions autres que celle de leur pays d'origine. Les considérations juridiques et éthiques doivent être prises en compte lors de la conception et mise en œuvre de systèmes d'information de la santé (systèmes nationaux) qui pourraient être utilisés de la sorte.

A.7 La sécurité des ressources humaines

A.7.1 Avant l'embauche

Objectif: S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

A.7.1.1 Sélection des candidats

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	Y	Il convient que les vérifications prennent en compte le droit du travail et la législation relative à la protection de la vie privée et des données à caractère personnel, et que les vérifications comportent, dans les limites permises, les aspects suivants: a) une vérification du curriculum vitæ du candidat; b) la confirmation des formations et des qualifications professionnelles alléguées; c) un contrôle d'identité indépendant (passeport ou document similaire); d) une vérification plus détaillée, par exemple un examen de la solvabilité ou du casier judiciaire pour autant que ce soit requis par la fonction et juridiquement contraignant. (p.ex. contacts avec des mineurs dans un hôpital pédiatrique) e) Les règles de protection de la vie privée cf. RGPD - sont-elles bien respectées? Lorsqu'une personne est embauchée pour assumer des fonctions spécifiques liées à la sécurité de l'information, il convient que l'organisation s'assure que le candidat: a) possède les compétences nécessaires pour remplir ses fonctions; b) est digne de confiance, notamment si ses fonctions sont d'une grande importance pour l'organisation. Qu'il s'agisse d'une première embauche ou d'une promotion, lorsqu'un poste implique l'accès aux moyens de traitement de l'information, et, en particulier, s'il s'agit d'informations confidentielles, par exemple financières ou hautement confidentielles, il convient que l'organisation envisage de procéder à des vérifications plus approfondies. Il convient que les procédures définissent des critères et des limites à la réalisation des vérifications, par exemple qu'elles déterminent qui est habilité à contrôler les candidats, de quelle manière, à quel moment et pour quelles raisons. Il convient que ce processus de sélection soit également appliqué pour les contractants. Dans ces cas là, il convient que le contrat passé entre l'organisation et le contractant spécifie les responsabilités en matière de sélection, ainsi que les procédures de notification à suivre si la sélection n'a pas abouti ou si les résultats sont source d'inquiétude ou de doute. Il convient de rassembler et de traiter les informations sur tous les candidats envisagés pour des fonctions au sein de l'organisation conformément à toute législation appropriée en vigueur dans la juridiction concernée. En fonction de la législation applicable, il convient ou non d'informer au préalable les candidats de la procédure de sélection sur dossier	Remarque: L'application de la législation est une matière juridique. « comportent, dans les limites permises, les aspects suivants »: qu'est-ce qui est permis ou non ? La procédure de sélection peut varier en fonction du niveau ou de l'importance de la fonction. Il est logique qu'une sélection pour une fonction de haut niveau soit réalisée par une partie externe spécialisée (moyennant clauses de confidentialité) et neutre.

A.7.1.2 Termes et conditions d'embauche

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins

Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information	Y	Il convient que les obligations contractuelles des salariés ou des contractants stipulent et précisent clairement les aspects suivants, en mettant en évidence les politiques de sécurité de l'information de l'organisation: a) il convient que tous les salariés et contractants ayant accès à des informations confidentielles signent un engagement de confidentialité ou de non-divulgation avant d'obtenir l'accès aux moyens de traitement de l'information (voir 13.2.4); b) les responsabilités juridiques et les droits des salariés ou des contractants concernant par exemple les droits de reproduction et la législation sur la protection des données (voir 18.1.2 et 18.1.4); c) les responsabilités relatives à la classification des informations et à la gestion des actifs de l'organisation liés aux informations, aux systèmes de traitement des informations et aux services d'information que le salarié ou le contractant utilise (voir chapitre 8); d) les responsabilités du salarié ou du contractant quant à la manipulation de l'information reçue de la part d'autres organisations ou tiers; e) les actions à engager si le salarié ou le contractant ne tient pas compte des exigences en matière de sécurité de l'organisation (voir 7.2.3). Lors du processus de préembauche, il convient d'informer clairement les candidats à l'embauche des rôles et des responsabilités en matière de sécurité. Il convient que l'organisation s'assure que les salariés et les contractants approuvent les dispositions relatives à la sécurité de l'information concernant la nature et l'étendue de leur futur accès aux actifs de l'organisation liés aux services et aux systèmes d'information. Si nécessaire, il convient que les responsabilités stipulées dans le contrat de travail continuent à s'appliquer pendant une durée définie après la fin du contrat (voir 7.3).	Les organisations qui traitent des données à caractère personnel relatives à la santé doivent veiller à ce que leurs travailleurs ou contractants soient tenus de signaler toute atteinte à la sécurité des données relatives à la santé ou à la vie privée des patients. En cas d'urgence, on peut essayer de contacter un 'collaborateur' et celui-ci peut prêter sa collaboration, en fonction de la nécessité d'intervention. Une exception peut être accordée à des 'spécialistes' ou 'responsables' spécifiques, mais ceci doit être stipulé contractuellement. Les organisations de santé doivent veiller à recueillir un nombre suffisant de références et à exécuter d'autres formes de contrôle, par exemple par des organisations professionnelles et centres académiques. Dans la mesure du possible, un contrôle quant à l'existence ou non d'un casier judiciaire doit être effectué (lorsqu'il s'agit d'une obligation légale). Attention: il est possible que ceci ait déjà été effectué dans le cadre de l'accréditation des prestataires de soins. Voir 7.1.1. Voir également 'sélection'.

A.7.2 Pendant la durée du contrat

Objectif: S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

A.7.2.1 Responsabilités de la direction

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que la direction demande à tous les salariés et contractants d'appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.	Y	Il convient qu'il relève des responsabilités de la direction de s'assurer que les salariés et les contractants: a) sont correctement informés sur leurs fonctions et leurs responsabilités en matière de sécurité de l'information avant de se voir accorder l'accès à l'information confidentielle ou aux systèmes d'information; b) prennent connaissance des lignes directrices spécifiant les attentes en matière de sécurité de l'information qu'impliquent leurs fonctions au sein de l'organisation; c) sont incités à appliquer les politiques de sécurité de l'information de l'organisation; d) acquièrent un niveau de sensibilisation à la sécurité en adéquation avec leurs fonctions et leurs responsabilités au sein de l'organisation (voir 7.2.2); e) respectent les conditions de leur embauche, ce qui intègre notamment la politique de sécurité de l'information de l'organisation et les méthodes de travail appropriées; f) maintiennent leur savoir-faire et leurs qualifications à niveau et suivent régulièrement des formations;	Une attention particulière doit être apportée aux aspects de soins des patients qui ne souhaitent pas que leurs données à caractère personnel relatives à la santé puissent être consultées par des prestataires de soins qui sont des collègues, proches ou voisins. Ces aspects constituent une part importante des plaintes introduites par des personnes qui craignent une atteinte à la confidentialité de leurs données à caractère personnel relatives à la santé. Souvent les membres du personnel ne souhaitent pas non plus se trouver dans une position où ils soient amenés à évaluer des informations relatives à des membres de leur famille, amis ou voisins. Une gestion adéquate des systèmes d'information de la santé doit aborder ces aspects.

		g) ont accès à un moyen de communication anonyme permettant de rapporter les violations à l'encontre des politiques ou des procédures de sécurité de l'information («dénonciation de dysfonctionnements»). Il convient que la direction manifeste son soutien aux politiques, aux procédures et aux mesures relatives à la sécurité de l'information et serve de modèle.	Les directives de mise en œuvre spécifiques aux soins ne sont pas axées sur la situation en Belgique (remarque générale), peuvent-elles être reformulées en fonction de la situation des hôpitaux en Belgique ?

A.7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'ensemble des salariés de l'organisation et, le cas échéant, les contractants suivent un apprentissage et des formations de sensibilisation adaptés et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.	Y	Il convient que le programme de sensibilisation à la sécurité de l'information vise à sensibiliser le personnel et, le cas échéant, les contractants aux responsabilités qui leur incombent en matière de sécurité de l'information et aux moyens dont ils disposent pour s'acquitter de ces responsabilités. Il convient d'établir un programme de sensibilisation à la sécurité de l'information qui soit cohérent avec les politiques de l'organisation relatives à la sécurité de l'information et avec les procédures associées, et qui tienne compte des informations à protéger et des mesures mises en œuvre pour assurer cette protection. Il convient que le programme de sensibilisation comporte un certain nombre d'activités de sensibilisation telles que des campagnes (par exemple, une « journée de la sécurité de l'information ») et la diffusion de livrets ou de bulletins d'information. Il convient que le programme de sensibilisation soit planifié en tenant compte des fonctions des salariés au sein de l'organisation et, le cas échéant, de ce que l'organisation attend des contractants. Il convient que les activités prévues dans le programme de sensibilisation soient programmées dans le temps, de préférence à échéances régulières, de manière à se répéter afin d'inclure les nouveaux salariés et contractants. Il convient également que le programme de sensibilisation soit mis à jour régulièrement pour rester cohérent avec les politiques et les procédures de l'organisation, et qu'il s'appuie sur les enseignements tirés des incidents de sécurité. Il convient que la formation de sensibilisation soit assurée comme spécifié par le programme de sensibilisation à la sécurité de l'information de l'organisation. La formation de sensibilisation peut être assurée de différentes manières, par exemple en salle de cours, par apprentissage à distance, apprentissage en ligne, auto-apprentissage, etc. Il convient que l'apprentissage et la formation à la sécurité de l'information couvrent également des aspects plus généraux tels que: a) la démonstration de l'engagement de la direction en matière de sécurité de l'information à tous les niveaux de l'organisation; b) la nécessité de se familiariser avec les règles et les obligations applicables à la sécurité de l'information, telles que définies dans les politiques, les normes, la loi, les règlements, les contrats et les accords, et de s'y conformer c) l'imputabilité à chacun de ses actions et de son inaction, et les responsabilités générales en matière de sécurisation ou de protection des informations appartenant à l'organisation et aux tiers; d) les procédures élémentaires en matière de sécurité de l'information (telles que le signalement des incidents liés à la sécurité de l'information) et les mesures de référence (telles que la sécurité des mots de passe, les mesures à l'encontre des logiciels malveillants et la politique du bureau propre);	

		e) les points de contact et les ressources permettant d'obtenir des informations complémentaires et des conseils sur les questions de sécurité de l'information, y compris des documents complémentaires de formation et d'apprentissage Il convient que les sessions d'apprentissage et de formation à la sécurité de l'information aient lieu périodiquement. L'apprentissage et la formation initiaux concernent les personnes nommées à de nouveaux postes ou à de nouvelles fonctions présentant des exigences de sécurité de l'information très différentes, et non pas seulement aux débutants. Il convient qu'elles soient assurées avant la date de prise d'effet du nouveau poste ou des nouvelles fonctions. Il convient que l'organisation élabore un programme d'apprentissage et de formation permettant d'assurer un apprentissage et une formation efficaces. Il convient d'établir un programme qui soit cohérent avec les politiques de l'organisation relatives à la sécurité de l'information et avec les procédures associées, et qui tienne compte des informations à protéger et des mesures mises en œuvre pour assurer cette protection. Il convient que le programme couvre différents modes d'apprentissage et de formation, tels que l'organisation de cours ou l'autoapprentissage.	

A.7.2.3 Processus disciplinaire

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient qu'il existe un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.	Y	Il convient de ne pas déclencher le processus disciplinaire avant d'avoir d'abord vérifié l'existence de l'infraction (voir 16.1.7). Il convient que le processus disciplinaire formel garantisse un traitement correct et juste des salariés suspectés d'avoir enfreint les règles de sécurité. Il convient que le processus disciplinaire formel fournisse une réponse graduée prenant en considération des facteurs tels que la nature et la gravité de la violation, ainsi que son impact sur l'activité de l'organisation. Il convient également de préciser s'il s'agit d'une première infraction ou d'une récidive, si le contrevenant a reçu la formation adéquate, et de tenir compte des dispositions légales applicables, des contrats commerciaux et de tout autre facteur nécessaire. Il convient également que le processus disciplinaire constitue un élément dissuasif empêchant les salariés d'enfreindre les politiques et procédures relatives à la sécurité de l'organisation, ainsi que toute autre règle de sécurité. Les violations délibérées des règles peuvent nécessiter des actions immédiates.	Les processus disciplinaires des organisations de santé par rapport aux infractions à la sécurité de l'information doivent suivre des procédures reflétées dans la politique et dès lors connues des personnes auxquelles s'applique la procédure disciplinaire. De tels processus doivent non seulement être conformes à la législation, mais également aux accords intervenus entre les prestataires de soins et les organisations de prestataires de soins.

A.7.3 Rupture, terme ou modification du contrat de travail

Objectif: Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.

A.7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en	Y	Il convient que les responsabilités liées aux fins de contrats incluent les exigences permanentes liées à la sécurité et les responsabilités légales ainsi que, le cas échéant, les responsabilités figurant dans tout engagement de confidentialité (voir 13.2.4) et dans les conditions d'embauche (voir 7.1.2) se poursuivant pendant une période de temps définie après le départ du salarié ou du contractant de l'organisation.	Il est important de souligner qu'il est courant dans le secteur des soins que divers types de personnel, p.ex. médecins et personnel infirmier, suivent des programmes de formation autres 'changements' susceptibles de modifier fondamentalement leurs droits d'accès. Pour garantir qu'il soit mis fin aux droits antérieurs qui ne sont plus

informer le salarié ou le contractant et de veiller à leur application.		Il convient que les responsabilités et les missions encore valables au-delà de la rupture ou du terme du contrat de travail figurent dans les conditions du contrat du salarié ou du contractant (voir 7.1.2). Il convient de gérer les changements de poste ou de responsabilités comme un terme mis au poste ou aux responsabilités en question, et de déterminer les nouvelles responsabilités ou les nouvelles fonctions.	d'application pour leur rôle, de tels changement doivent en principe être traités de la même façon que lorsqu'il s'agit de personnes dont le contrat prend fin.

A.8 Gestion des actifs

A.8.1 Responsabilités relatives aux actifs

Objectif: Identifier les actifs dee l'organisation et définir les responsabilités appropriées en de protection.

A.8.1.1 Inventaire des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'identifier les actifs associés à l'information et aux moyens de traitement de l'information et de dresser et tenir à jour un inventaire de ces actifs.	Y	Il convient que l'organisation identifie les actifs pertinents impliqués dans le cycle de vie de l'information et documente leur importance. Il convient que le cycle de vie de l'information englobe sa création, son traitement, son stockage, sa transmission, sa suppression et sa destruction. Il convient que la documentation soit tenue à jour dans des inventaires dédiés ou déjà en place selon le cas. Il convient que l'inventaire des actifs soit précis, à jour, cohérent et en adéquation avec les autres inventaires. Il convient d'attribuer à chaque actif identifié un propriétaire (voir 8.1.2) et d'identifier la classification (voir 8.2).	Les organisations qui traitent des données relatives à la santé doivent disposer de règles pour la mise à jour des ressources d'information (p.ex. banque de données de médicaments) et le maintien de l'intégrité de ces ressources (p.ex. intégrité fonctionnelle des appareils médicaux utilisés pour l'enregistrement de données ou l'établissement de rapports). Les appareils médicaux utilisés pour l'enregistrement ou le rapportage (p.ex. MRI) peuvent demander des mesures de sécurité spéciales par rapport à l'environnement où ils sont utilisés et aux émissions électromagnétiques lors de leur utilisation. Ce genre d'appareils doivent être identifiés de manière unique. Il convient de décrire sur quel support l'information (médicale) est enregistrée (fixe, mobile, accès via réseau) et comment celui-ci est sécurisé. Remarque: L'information est également une ressource et doit donc aussi être inventoriée.

A.8.1.2 Propriété des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les actifs figurant à l'inventaire aient un propriétaire.	Y	Une personne ou une entité qui a accepté la responsabilité d'assurer la gestion du cycle de vie d'un actif remplit les conditions pour être désignée propriétaire de l'actif. Il est généralement prévu un processus permettant de garantir l'attribution en temps et en heure d'un propriétaire à l'actif. Il convient d'attribuer un propriétaire aux actifs à leur création ou lorsqu'ils sont transférés à l'organisation. Il convient que le propriétaire de l'actif soit responsable de la bonne gestion de cet actif tout au long de son cycle de vie. Il convient que le propriétaire de l'actif:	Bien que bon nombre de ressources puissent constituer une propriété au sens conventionnel, le concept de propriété de données à caractère personnel relatives à la santé implique des aspects juridiques, éthiques et politiques. Dans bon nombre de juridictions, les individus possèdent des droits par rapport à leurs données relatives à la santé qui dépassent ou limitent la simple notion de 'propriété ' d'un établissement de soins ou d'un prestataire de soins. Les établissements de

		a) s'assure que les actifs soient inventoriés; b) s'assure que les actifs sont correctement classés et protégés; c) définisse et revoit périodiquement les classifications et les restrictions d'accès aux actifs importants, en tenant compte des politiques de contrôle d'accès applicables; d) s'assure que les manipulations de suppression ou de destruction des actifs soient réalisées correctement.	soins et prestataires de soins sont plutôt considérés comme des gestionnaires ou gardiens de ces données à caractère personnel relatives à la santé.

A.8.1.3 Utilisation correcte des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'identifier, de documenter et de mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.	Y	Il convient que les salariés et les utilisateurs tiers utilisant ou ayant accès aux actifs de l'organisation soient conscients des exigences de sécurité de l'information liées aux actifs de l'organisation associés à l'information, aux moyens de traitement de l'information et aux ressources. Il convient qu'ils soient responsables de l'utilisation qu'ils font de toute ressource de traitement de l'information et de toute utilisation effectuée sous leur responsabilité.	

A.8.1.4 Restitution des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que tous les salariés et utilisateurs tiers restituent la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.	Y	Il convient de formaliser le processus de fin de mission ou d'emploi pour qu'il inclue la restitution de tous les actifs physiques et électroniques créés, appartenant à l'organisation ou lui ayant été confiés. Si un salarié ou un utilisateur tiers achète du matériel à l'organisation ou utilise son propre matériel, il convient de suivre des procédures pour garantir que toutes les informations pertinentes sont transférées à l'organisation et correctement effacées du matériel (voir mesure 11.2.7). Si un salarié ou un utilisateur tiers détient des connaissances importantes pour les activités en cours, il convient que cette information soit documentée et transférée à l'organisation. Lors de la période de préavis, il convient que l'organisation vérifie que les salariés et les contractants quittant l'organisation ne procèdent pas à des copies non autorisées d'information utile (par exemple en matière de propriété intellectuelle).	

A.8.2 Classification de l'information

Objectif: S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.

A.8.2.1 Classification des informations

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité ou de leur caractère critique pour l'entreprise.	Y	Il convient que la classification de l'information et les mesures de protection associées tiennent compte des besoins de l'organisation en matière de partage ou de limitation de l'information, ainsi que des exigences légales. D'autres actifs que l'information peuvent également être classés conformément à la classification de l'information qu'ils stockent, traitent ou manipulent de quelque autre façon et qu'ils protègent. Il convient que les propriétaires des actifs liés à l'information soient responsables de leur classification.	La détermination des niveaux de protection pour les informations dans le secteur des soins est un processus complexe et des comparaisons avec des classifications pour les données des pouvoirs publics ou les données militaires peuvent être trompeuses. Les caractéristiques suivantes sont importantes au niveau des informations dans le secteur des soins :

		Il convient que le plan de classification comporte des conventions de classification et des critères de revue de cette classification dans le temps. Il convient que le niveau de protection du plan de classification soit apprécié en analysant la confidentialité, l'intégrité, la disponibilité et toute autre exigence relative à l'information à évaluer. Il convient que le plan de classification soit cohérent avec la politique de contrôle d'accès (voir 9.1.1). Il convient d'attribuer à chaque niveau un nom significatif et logique dans le contexte de l'application du plan de classification. Il convient que le plan soit identique pour toute l'organisation, de sorte que tout le monde puisse classer l'information et les actifs associés de la même façon, comprenne les exigences de protection de la même manière et applique la protection appropriée. Il convient que la classification soit intégrée aux processus de l'organisation et qu'elle soit cohérente et identique pour toute l'organisation. Il convient que les résultats de la classification traduisent la valeur des actifs en fonction de leur sensibilité et de leur caractère critique pour l'organisation, par exemple en termes de confidentialité, d'intégrité et de disponibilité. Il convient que les résultats de la classification soient mis à jour en fonction des évolutions de leur valeur, de leur sensibilité et de leur caractère critique tout au long de leur cycle de vie. Etablir une proposition de schéma de classification: quels types de classification (p.ex. public, interne, médical, ...) Il faut tenir compte du fait que certains hôpitaux utilisent déjà un système de classification propre (p.ex. confidentiel, non-confidentiel, ...). Il semble invraisemblable que les hôpitaux implémentent tous sans plus le même système, mais il faut néanmoins viser une certaine compatibilité dans un souci d'échange d'informations. Une concertation doit avoir lieu à cet effet. Proposition ou exemple à titre d'inspiration: les normes minimales de la sécurité sociale https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/bld_data_data_classificatie.pdf	a) La confidentialité des données à caractère personnel relatives à la santé est souvent subjective plutôt qu'objective. En d'autres termes: seule la personne à qui les données ont trait (càd le patient) est en mesure de déterminer la confidentialité relative des divers champs ou groupes de données. Une personne qui a fui d'une relation où elle était maltraitée attachera beaucoup plus d'importance à la confidentialité de sa nouvelle adresse et de son numéro de téléphone qu'à la confidentialité de ses données cliniques concernant son bras cassé. b) La confidentialité des données à caractère personnel relatives à la santé dépend du contexte. Ainsi, il se peut que la mention du nom et de l'adresse d'un patient sur une liste de personnes admises au service de premiers soins de l'hôpital ne soit pas directement considérée comme confidentielle, tandis que cette même mention pour une personne admise dans une clinique où sont traitées des personnes souffrant d'impuissance sexuelle sera considérée comme très confidentielle par cette personne. c) La confidentialité des données à caractère personnel relatives à la santé peut changer au cours du cycle de vie du dossier médical. Ainsi, l'évolution des attitudes au cours de ces vingt dernières années a pour conséquence que bon nombre de patients ne considèrent plus leur orientation sexuelle comme une information confidentielle. L'attitude envers la toxicomanie et l'alcoolisme fait que certains patients considèrent l'information relative au traitement de ces dépendances encore plus confidentielle que ce n'était le cas il y a vingt ans. Etant donné qu'il est impossible de prédire dans quelle mesure un élément d'information personnelle relative à la santé est sensible par rapport à toutes les applications et toutes les phases du cycle de vie de cet élément, il convient de toujours dûment protéger toutes les données à caractère personnel relatives à la santé. Attention: bien que toutes les données à caractère personnel relatives à santé doivent être classifiées de manière uniforme comme confidentielles, des considérations pratiques peuvent rendre nécessaire l'identification des dossiers de patients pour lesquels il existe un risque accru que des personnes non autorisées y aient accès. Il peut notamment s'agir de collaborateurs de l'organisation (lorsque leur état entraîne des comportements émotionnels), de chefs de gouvernement, de personnes

			célèbres, de responsables politiques et de membres de groupes qui courent un risque accru (par exemple personnes atteintes de maladies sexuellement transmissibles ou personnes dont les données à caractère personnel relatives à la santé révèlent une prédisposition génétique pour une maladie grave). Il peut s'avérer nécessaire de pourvoir les dossiers de ces personnes d'un label spécial de sorte à permettre un monitoring de l'accès. La mise en place de telles règles doit être effectuée de manière précise, car l'apport d'un label pourrait même aggraver le problème que l'on souhaite justement éviter, c'est-à-dire attirer l'attention sur les données. Il est aussi important de souligner que les données à caractère personnel relatives à la santé de certains patients qui courent un risque accru ne sont pas par définition plus confidentielles que les données des autres patients. *Toutes* les données à caractère personnel relatives à la santé sont confidentielles et doivent être traitées comme telles. Voir également l'explication sous la directive de mise en œuvre spécifique aux soins 7.2.1. L'identification du caractère confidentiel et (au besoin) l'ajout d'un label d'un point de vue de sécurité peuvent constituer un instrument important dans le cadre de la sensibilisation du personnel et du respect de la politique. Ceci fonctionne le mieux lorsque la classification constitue un indicateur des pratiques requises dans le cadre du traitement de l'information. La classification peut aussi être un élément important des contrats en matière de protection des données entre juridictions et avec des organisations tierces et le personnel de ces organisations. L'identification et l'ajout de labels aux informations est un composant essentiel de ISO/IEC 27002. En complément de la classification traditionnelle des données sur la base de leur caractère sensible, il est également nécessaire de classifier la criticité de l'information, c'est-à-dire la mesure dans laquelle la disponibilité et l'intégrité de l'information sont essentielles pour la continuité des soins. Des facteurs temporels dans le cadre de processus cliniques jouent un rôle essentiel lors de la détermination des exigences de disponibilité des données à caractère personnel relatives à la santé. La classification en termes de disponibilité, intégrité et criticité doit aussi être appliquée aux processus, aux dispositifs IT, aux logiciels, aux espaces et au personnel. La criticité doit être identifiée par le biais d'une évaluation des risques.

			Etablir une proposition de schéma de classification: quels types de classification (p.ex. public, interne, médical, ...) Certains hôpitaux ont déjà un système de classification propre (p.ex. confidentiel, non-confidentiel). Il semble peu probable que les hôpitaux implémentent tous sans plus le même système, mais il faut néanmoins viser une certaine compatibilité dans un souci d'échange d'informations. P.ex. une donnée 'médicale' ne peut pas soudainement devenir 'publique' après transmission. Remarque: La classification doit être inscrite dans le registre de traitement des processus dans le cadre du RGPD et doit être couplée au délai de conservation des données.

A.8.2.2 Marquage des informations

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'élaborer et de mettre en oeuvre un ensemble approprié de procédures pour le marquage de l'information, conformément au plan de classification de l'information adopté par l'organisation.	Y	Les procédures de marquage de l'information doivent s'appliquer à l'information et aux actifs associés présentés sous un format physique ou électronique. Il convient que le marquage respecte le plan de classification défini en 8.2.1. Il convient que les marques soient facilement reconnaissables. Il convient que les procédures donnent des indications sur l'endroit et la façon dont les marques sont fixées, compte tenu de la manière dont on accède à l'information ou de la façon de manipuler les actifs, en fonction des types de support. Les procédures peuvent définir des cas pour lesquels le marquage n'est pas indispensable, par exemple dans le cas d'information non confidentielle en vue d'alléger la charge de travail. Il convient que les salariés et les contractants soient sensibilisés aux procédures de marquage. Il convient que les données délivrées par des systèmes contenant de l'information classée comme sensible ou critique portent des marques appropriées.	Les informations relatives à la santé ne sont pas toutes confidentielles et les systèmes d'information de la santé n'offrent pas tous accès à des données à caractère personnel relatives à la santé dans le chef des utilisateurs. Les utilisateurs des systèmes d'information de la santé doivent être informés lorsque les informations auxquelles ils accèdent contiennent des données à caractère personnel relatives à la santé. L'apport d'un label semble simple à réaliser lorsqu'il s'agit de supports physiques, tels que des classeurs, mais comment faut-il l'implémenter sur des données numériques ? Ne s'agit-il pas plutôt d'un processus d'authentification et d'accessibilité ? Qui décide de l'accès à des niveaux de classification spécifiques ? Qui est chargé de la maintenance ?

A.8.2.3 Manipulation des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'élaborer et de mettre en oeuvre des procédures de traitement des actifs, conformément au plan de	Y	Il convient de rédiger des procédures spécifiant comment manipuler, traiter, stocker et communiquer l'information en fonction de sa classification (voir 8.2.1). Il convient d'envisager les éléments suivants:	

classification de l'information adopté par l'organisation.		a) restreindre les accès pour renforcer les exigences de protection à chaque niveau de la classification; b) tenir à jour un enregistrement formel des personnes autorisées à recevoir des actifs; c) protection des copies temporaires ou permanentes de l'information à un niveau en adéquation avec le niveau de protection de l'information originale; d) stockage des actifs informatiques selon les spécifications du fabricant; e) marquer clairement toutes les copies de support du nom de la personne autorisée à les recevoir. Le plan de classification utilisé par l'organisation peut ne pas correspondre aux plans utilisés par d'autres organisations, même si les noms affectés aux niveaux sont similaires. En outre, la classification de l'information circulant entre les organisations peut varier en fonction du contexte de chaque organisation, même si les plans de classification sont identiques. Il convient que les accords conclus avec d'autres organisations incluant un partage d'information prévoient des procédures afin d'identifier la classification de cette information et d'interpréter les marques de classification apposées par ces autres organisations.	

A.8.3 Manipulation des supports

Objectif: Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.

A.8.3.1 Gestion des supports amovibles

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en œuvre des procédures de gestion des supports amovibles conformément au plan de classification adopté par l'organisation.	Y	Il convient de tenir compte des directives suivantes concernant la gestion des supports amovibles: a) il convient de rendre impossible toute récupération du contenu d'un support réutilisable devant être retiré de l'organisation, si ce contenu n'est plus indispensable; b) si nécessaire et réalisable, il convient d'exiger une autorisation pour le retrait de supports de l'organisation et de garder un enregistrement de ces retraits pour en assurer la traçabilité; c) il convient de stocker tous les supports dans un environnement sûr, sécurisé et conforme aux spécifications du fabricant; d) si la confidentialité ou l'intégrité des données constituent des facteurs importants, il convient d'utiliser des techniques cryptographiques pour protéger les données figurant sur le support amovible; e) pour limiter les risques liés à la dégradation du support lorsque les données stockées sont encore nécessaires, il convient de transférer ces données sur un support neuf, avant qu'elles ne deviennent illisibles; f) il convient de stocker diverses copies de données de valeur sur des supports séparés pour réduire les risques concomitants d'endommagement ou de perte de données; g) il convient d'envisager de tenir un registre des supports amovibles pour limiter les risques de perte de données; h) il convient de n'activer les lecteurs de supports amovibles que si l'activité le nécessite; i) lorsqu'il est nécessaire d'utiliser des supports amovibles, il convient de contrôler le transfert de l'information sur ces supports. j) Il convient de documenter les procédures et les niveaux d'autorisation.	Les organisations qui traitent des données à caractère personnel relatives à la santé doivent garantir que toutes les données à caractère personnel relatives à la santé qui sont enregistrées sur des supports amovibles : a) soient chiffrées pendant le transfert des supports en question ou b) soient protégées contre le vol pendant le transfert des supports en question. c) Une description des délais de conservation légitimes doit être élaborée sur la base des réglementations existantes et doit être documentée dans le registre de traitement au niveau des schémas de classification. Cette classification doit être approuvée par la direction de l'institution, avec un support juridique.

A.8.3.2 Mise au rebut des supports

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de procéder à une mise au rebut sécurisée des supports qui ne servent plus, en suivant des procédures formelles.	Y	Il convient que les procédures formelles de mise au rebut sécurisée des supports réduisent au minimum le risque de fuites d'information confidentielle vers des personnes non autorisées. Il convient que les procédures de mise au rebut sécurisée des supports contenant de l'information confidentielle soient proportionnelles à la sensibilité de cette information. Il convient d'envisager les éléments suivants: a) il convient de stocker les supports contenant de l'information confidentielle et de les mettre au rebut de façon sûre et sécurisée, par exemple par incinération ou déchiquetage, ou d'en effacer les données utilisées dans d'autres applications de l'organisation; b) il convient de mettre en place des procédures d'identification des éléments pouvant nécessiter une mise au rebut sécurisé; c) il peut s'avérer plus facile d'organiser la collecte et la mise au rebut sécurisées de l'ensemble des supports, plutôt que de tenter d'isoler les supports sensibles; d) de nombreuses organisations proposent des services de collecte et d'enlèvement des supports; il convient de sélectionner avec soin le prestataire approprié disposant de mesures de sécurité et d'une expérience suffisantes; e) il convient de journaliser la mise au rebut des éléments sensibles pour en assurer la traçabilité. En cas d'accumulation de supports en vue de leur mise au rebut, il convient de prendre en compte l'effet d'agrégation qui peut rendre sensible une grande quantité d'information à l'origine non confidentielle.	La mise au rebut inadéquate de supports constitue une source de violation de la confidentialité pour les patients. Cette mesure de gestion doit être appliquée préalablement à toute réparation ou suppression du support en question. Cette exigence s'applique également aux appareils médicaux qui sont utilisés pour enregistrer des données ou pour le rapportage. Pour chaque type d'appareil, il convient d'examiner la façon la plus appropriée pour supprimer correctement les données de sorte qu'elles ne soient pas accessibles à des tiers.

A.8.3.3 Transfert physique des supports

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger les supports contenant de l'information contre les accès non autorisés, l'utilisation frauduleuse ou l'altération lors du transport.	Y	Il convient de prendre en compte les directives suivantes pour protéger les supports d'information lors de leur transport: a) il convient que le transporteur ou le coursier employé soit fiable; b) il convient d'établir, en accord avec la direction, la liste des coursiers autorisés; c) il convient de mettre au point des procédures de contrôle de l'identification des coursiers; d) il convient que l'emballage choisi soit suffisant pour protéger son contenu de tout dommage physique susceptible de survenir lors du transit et qu'il soit conforme aux spécifications du fabricant en fournissant par exemple une protection contre tout facteur environnemental pouvant diminuer l'efficacité de la restauration du support, comme l'exposition à de fortes températures, à une forte humidité ou à des champs électromagnétiques; e) il convient de conserver les journaux identifiant le contenu du support, la protection appliquée, ainsi que les dates et heures de remise aux responsables du transport et de réception par le destinataire.	

A.9 Contrôle d'accès

A.9.1 Exigences métier en matière de contrôle d'accès

Objectif: Limiter l'accès à l'information et aux moyens de traitement de l'information.

A.9.1.1 Politique de contrôle d'accès

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'établir, de documenter et de revoir une politique du contrôle d'accès sur la base des exigences métier et de sécurité de l'information.	Y	Il convient que les propriétaires des actifs déterminent des règles de contrôle d'accès, des droits d'accès et des restrictions d'accès appropriés aux fonctions spécifiques de l'utilisateur des actifs, avec la quantité de détails et la rigueur des mesures correspondant aux risques associés en matière de sécurité de l'information. Les contrôles d'accès sont à la fois logiques et physiques (voir chapitre 11) et il convient de les envisager conjointement. Il convient que les utilisateurs et les prestataires de services soient clairement informés des exigences de l'organisation auxquelles doivent répondre les contrôles d'accès. Il convient que la politique tienne compte des exigences suivantes: a) exigences en matière de sécurité des applications métier; b) politiques relatives à la diffusion de l'information et aux autorisations, par exemple nécessité de connaître le principe, les niveaux de sécurité de l'information et la classification de l'information (voir 8.2); c) cohérence entre la politique des droits d'accès et la politique de classification de l'information des différents systèmes et réseaux; d) législation et obligations contractuelles applicables relatives à la limitation de l'accès aux données ou aux services (voir 18.1); e) gestion des droits d'accès dans un environnement décentralisé mis en réseau qui reconnaît tous les types de connexions disponibles; f) cloisonnement des rôles pour le contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès; g) exigences en matière d'autorisation formelle des requêtes d'accès (voir 9.2.1 et 9.2.2); h) exigences en matière de revue régulière des droits d'accès (voir 9.2.5); i) annulation de droits d'accès (voir 9.2.6); j) archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et à la gestion des identités des utilisateurs et des informations d'authentification secrètes; k) fonctions avec accès privilégié (voir 9.2.3).	Pour éviter un retard ou arrêt de la prestation de soins, des exigences plus strictes sont applicables, avec l'autorisation y relative, afin de contourner les règles de contrôle d'accès 'normales' en cas de situation d'urgence. Les organisations de santé sont invitées à envisager l'implémentation d'une solution fédérée de gestion des accès et de l'identité compte tenu du support complémentaire et des frais de gestion inférieures qu'une telle solution peut apporter pour la politique de contrôle des accès. Par ailleurs, ceci soutiendra les processus de protection des accès à un niveau supérieur, par exemple l'accès basé sur des smartcards et la fonctionnalité 'single sign on'. Des directives complémentaires en matière de contrôle des accès dans le cadre d'applications de soins de santé figurent dans ISO 22600.

A.9.1.2 Accès aux réseaux et aux services en réseau

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les utilisateurs aient uniquement accès au réseau et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation.	Y	Il convient de définir une politique relative à l'utilisation des réseaux et des services en réseau. Il convient que cette politique couvre: a) les réseaux et les services en réseau pour lesquels l'accès a été accordé; b) les procédures d'autorisation désignant les personnes autorisées à accéder à tels ou tels réseau et service en réseau;	

		c) les procédures et mesures de gestion destinées à protéger l'accès aux connexions réseau et aux services en réseau; d) les moyens utilisés pour accéder aux réseaux et aux services en réseau (par exemple réseau privé virtuel ou réseau sans fil); e) les exigences d'authentification de l'utilisateur pour l'accès à différents services en réseau; f) la surveillance de l'utilisation faite de ces services en réseau. Il convient que la politique d'utilisation des services en réseau soit cohérente avec la politique de contrôle d'accès de l'organisation (voir 9.1).	

A.9.2 Gestion de l'accès utilisateur

Objectif: Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

A.9.2.1 Enregistrement et désinscription des utilisateurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en œuvre une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès.	Y	Il convient que la procédure de gestion des identifiants utilisateurs inclue: a) la création d'identifiants utilisateurs uniques permettant de relier les utilisateurs à leurs actions et de les leur imputer; il convient de n'autoriser l'utilisation d'identifiants communs que lorsque les aspects opérationnels et liés à l'activité de l'organisation l'exigent; il convient que ces identifiants communs soient approuvés et documentés; b) la suppression ou le blocage immédiats des identifiants des utilisateurs qui ont quitté l'organisation (voir 9.2.6); c) la détection périodique des identifiants utilisateurs redondants, suivie de leur suppression ou de leur blocage; d) l'assurance que des identifiants utilisateurs redondants ne sont pas attribués à d'autres utilisateurs.	Il est important de comprendre que la tâche d'identification et d'enregistrement des utilisateurs de systèmes d'information de la santé comprend également tous les aspects suivants : a) la détermination précise de l'identité d'un utilisateur (p.ex. Jan Smit, né le 26 mars 1982, domicilié à une adresse spécifique); b) la détermination précise, après vérification, des données professionnelles permanentes d'un utilisateur (p.ex. Suzan Jansen, cardiologue) et/ou de la dénomination de la fonction (p.ex. Jan Smit, réceptionniste médical); c) L'attribution d'un code d'identification de l'utilisateur univoque. Attention: les patients ne sont généralement pas des utilisateurs du système, bien qu'ils aient accès en ligne à (une partie de) leurs données à caractère personnel (p.ex. via un portail) et pourraient à ce titre être des utilisateurs du système (avec un accès limité). Il existe aussi des applications de santé permettant à l'utilisateur de rechercher des conseils et des informations générales en matière de santé. Bien que ce type de demande d'information puisse faire l'objet d'un enregistrement, l'utilisateur qui a accès au système reste anonyme. De nombreux sites web qui fournissent des informations sur la grossesse, le sida ou d'autres sujets de santé fonctionnent ainsi. Les utilisateurs de ce type de sites informatifs ne doivent généralement pas s'enregistrer et ne sont donc pas pris en compte dans ce qui suit. Voir 7.2.1.

A.9.2.2 Maîtrise de la gestion des accès utilisateur

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en oeuvre un processus formel de maîtrise de la gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous les systèmes et de tous les services d'information.	Y	Il convient que le processus de maîtrise de la gestion des attributions ou des révocations des droits d'accès accordés à des identifiants utilisateurs inclue: a) l'obtention de l'autorisation d'utilisation du système ou du service d'information de la part du propriétaire de ce système ou de ce service d'information (voir 8.1.2); il peut également s'avérer approprié de séparer l'approbation des droits d'accès de leur gestion; b) la vérification que le niveau d'accès accordé est adapté aux politiques d'accès (voir 9.1) et qu'il est cohérent avec les autres exigences telles que la séparation des tâches (voir 6.1.2); c) l'assurance que les droits d'accès ne sont pas activés (par exemple, par les prestataires de services) tant que le processus d'autorisation n'est pas terminé; d) la tenue à jour d'un enregistrement centralisé de tous les droits d'accès accordés aux identifiants utilisateurs pour leur permettre d'utiliser des systèmes et des services; e) l'adaptation des droits d'accès des utilisateurs qui ont changé de fonction ou de poste et la suppression ou le blocage immédiat des droits d'accès des utilisateurs qui ont quitté l'organisation; f) une revue régulière des droits d'accès avec les propriétaires des systèmes ou des services d'information (voir 9.2.5).	Dans les procédures relatives à l'octroi d'accès, il convient de préciser clairement si les utilisateurs obtiennent accès à des données à caractère personnel relatives à la santé.

A.9.2.3 Gestion des privilèges d'accès

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges d'accès.	Y	Il convient de contrôler l'attribution des privilèges d'accès par le biais d'une procédure formelle d'autorisation, conformément à la politique de contrôle des accès applicable (voir 9.1.1). Il convient d'envisager les étapes suivantes: a) il convient d'identifier les privilèges d'accès associés à chaque système ou chaque processus, par exemple le système d'exploitation, le système de gestion de la base de données et chaque application, ainsi que les utilisateurs auxquels il est nécessaire d'attribuer ces privilèges; b) il convient d'attribuer des privilèges d'accès aux utilisateurs en suivant les impératifs liés à leur activité et au cas par cas, conformément à la politique de contrôle d'accès (voir 9.1.1), c'est-à-dire en fonction de l'exigence minimale requise par leur rôle fonctionnel; c) il convient de tenir à jour une procédure d'autorisation et un enregistrement de tous les privilèges qui ont été attribués. Il convient de ne pas attribuer de privilèges d'accès tant que le processus d'autorisation n'est pas terminé; d) il convient de définir les exigences en matière d'expiration des privilèges d'accès; e) il convient d'associer les privilèges d'accès à un identifiant utilisateur différent de l'identifiant utilisateur employé pour les tâches ordinaires. Il convient que les tâches ordinaires des utilisateurs ne soient pas réalisées à l'aide d'un identifiant doté de privilèges; f) il convient de procéder à une revue régulière des compétences des utilisateurs bénéficiant de privilèges d'accès afin de vérifier qu'elles sont conformes à leurs tâches;	Dans ce qui suit, nous spécifions une série de stratégies en matière de mesures de gestion de l'accès susceptibles de contribuer considérablement à la confidentialité et à l'intégrité des données à caractère personnel relatives à la santé. Il s'agit des stratégies suivantes : a) contrôle d'accès basé sur des rôles, qui a recours aux données professionnelles et/ou dénominations de fonctions des utilisateurs spécifiées lors de l'enregistrement afin de limiter les droits d'accès des utilisateurs aux droits requis pour assurer un ou plusieurs rôles définis; b) contrôle d'accès basé sur des groupes de travail, dans le cadre duquel des utilisateurs sont attribués à des groupes de travail (p.ex. équipes cliniques) pour déterminer à quels enregistrements ils ont accès; c) contrôle d'accès discrétionnaire, permettant aux utilisateurs des systèmes d'informations de la santé qui ont une relation légitime avec les données à caractère personnel relatives à la santé du patient (p.ex. médecin généraliste) de donner accès à d'autres utilisateurs qui n'ont pas encore de relation avec les données à

		g) il convient d'établir et de tenir à jour des procédures spécifiques afin d'éviter l'utilisation non autorisée d'identifiants génériques d'administration, selon les capacités de configuration du système; h) en ce qui concerne les identifiants génériques d'administration, il convient de préserver la confidentialité des informations secrètes d'authentification lorsque ces identifiants sont partagés (par exemple, changer fréquemment de mots de passe et dès que possible lorsqu'un utilisateur privilégié quitte l'organisation ou change de fonction, les communiquer à l'aide de mécanismes appropriés aux utilisateurs privilégiés).	caractère personnel relatives à la santé du patient (p.ex. spécialiste). Les systèmes d'information de la santé qui contiennent des données à caractère personnel relatives à la santé sont censés supporter le contrôle d'accès basé sur des rôles, dans le cadre duquel un ou plusieurs rôles sont attribués à chaque utilisateur et une ou plusieurs fonctions système sont attribuées à chaque rôle. Un utilisateur d'un système d'information de la santé contenant des données à caractère personnel relatives à la santé doit, dans le cadre d'un rôle, avoir accès aux services associés à ce rôle (les utilisateurs ayant plus d'un rôle doivent indiquer pour chaque session le rôle dans le cadre duquel ils accèdent au système d'information de la santé). Les systèmes d'information de la santé doivent coupler les utilisateurs (notamment prestataires de soins, personnel de soutien et autres) aux enregistrements de patients et permettre l'accès futur sur base de ce couplage. Des directives complémentaires en matière de gestion des droits dans les soins de santé figurent dans ISO 22600-1 et ISO 22600-2.

A.9.2.4 Gestion des informations secrètes d'authentification des utilisateurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.	Y	Il convient que ce processus prévoie les exigences suivantes: a) il convient d'exiger des utilisateurs qu'ils signent une déclaration par laquelle ils s'engagent à ne pas divulguer leurs informations secrètes d'authentification personnelle et à communiquer leurs informations secrètes d'authentification de groupe (à savoir les informations partagées) aux seuls utilisateurs du groupe; il est possible d'inclure cette déclaration signée dans le contrat de travail (voir 7.1.2); b) lorsqu'il est demandé aux utilisateurs de définir eux-mêmes leurs informations secrètes d'authentification, il convient de leur fournir au préalable des informations secrètes d'authentification sécurisées et temporaires qu'ils doivent changer dès la première utilisation; c) il convient d'établir des procédures permettant de vérifier l'identité d'un utilisateur avant d'attribuer des nouvelles informations secrètes d'authentification ou des informations secrètes d'authentification temporaires; d) il convient que la communication des informations secrètes d'authentification temporaires soit sécurisée; il convient d'éviter de les envoyer par courrier électronique non protégé (texte en clair) ou de la transmettre par l'intermédiaire de tiers; e) il convient que les informations secrètes d'authentification temporaires soient uniques pour chaque personne et qu'il ne soit pas possible, par déduction, de les deviner; f) il convient que les utilisateurs accusent réception des informations secrètes d'authentification;	Il n'existe pas de directive complémentaire pour la gestion de sécurité de l'information dans les soins de santé. Il est à noter que les situations d'urgence dans les soins font que la gestion efficace des mots de passe est compliquée. Bon nombre d'organisations de santé ont envisagé le recours à des technologies d'authentification alternatives pour répondre à ce problème.

		g) il convient que les informations secrètes d'authentification par défaut définies par les constructeurs et éditeurs soient modifiées après installation des systèmes ou logiciels.	

A.9.2.5 Revue des droits d'accès utilisateurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers.	Y	Il convient que la revue des droits d'accès utilisateurs tienne compte de ce qui suit: a) il convient de revoir les droits d'accès utilisateurs à intervalles réguliers et après tout changement tel qu'une promotion, une rétrogradation ou le départ d'un salarié (voir chapitre 7); b) il convient de revoir et de réattribuer les droits d'accès utilisateurs en cas de changement de fonction au sein de l'organisation; c) il convient de revoir, à des intervalles de temps plus fréquents, les autorisations liées à des droits d'accès privilégiés; d) il convient de vérifier l'attribution de privilèges à intervalles réguliers pour s'assurer qu'aucun privilège non autorisé n'a été accordé; e) il convient de journaliser les modifications apportées aux comptes dotés de privilèges aux fins de revue périodique.	Il convient de tenir compte en particulier des utilisateurs appelés à donner des soins d'urgence, pour lesquels il peut être nécessaire d'accéder à des données à caractère personnel relatives à la santé sans que le patient ne puisse donner son consentement à cet effet.

A.9.2.6 Suppression ou adaptation des droits d'accès

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les droits d'accès de l'ensemble des salariés et utilisateurs tiers à l'information et aux moyens de traitement de l'information soient supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.	Y	Il convient qu'à l'achèvement de la période d'emploi, les droits d'accès d'une personne à l'information et aux actifs associés aux services et aux moyens de traitement de l'information soient supprimés ou suspendus. Cela permettra de déterminer s'il est nécessaire de supprimer les droits d'accès. Il convient que les modifications apportées à un contrat entraînent le retrait de tous les droits d'accès n'ayant pas été approuvés dans le cadre du nouveau contrat. Il convient que les droits d'accès à supprimer ou à adapter concernent les accès physiques et logiques. La suppression ou l'adaptation peuvent être réalisées par suppression, révocation ou remplacement des clés, des cartes d'identification, des moyens de traitement de l'information ou des abonnements. Il convient que toute documentation recensant les droits d'accès des salariés et des contractants rende compte de leur suppression ou de leur adaptation. Si un salarié ou un utilisateur tiers quittant l'organisation connaît les mots de passe d'identifiants utilisateurs toujours actifs, il convient de changer ces mots de passe à l'achèvement de la période d'emploi ou dès la modification du contrat ou de l'accord. Il convient que les droits d'accès à l'information et aux actifs associés aux moyens de traitement de l'information soient restreints ou supprimés avant la fin de la période d'emploi ou la modification du contrat en fonction de l'évaluation des facteurs de risque suivants: a) s'agit-il d'une résiliation ou d'une modification du contrat intervenue à l'initiative du salarié, de l'utilisateur tiers ou de la direction, et pour quel motif? b) quelles sont les responsabilités du salarié, de l'utilisateur tiers ou autre utilisateur? c) quelle est la valeur des actifs accessibles?	Il est important d'attirer l'attention sur les nombreux exemples d'étudiants, stagiaires et remplaçants dans les soins, qui ont maintenu leurs droits d'accès à l'issue de leur stage, remplacement, etc. Dans les grands hôpitaux, un grand nombre de collaborateurs temporaires ont momentanément accès à des données à caractère personnel relatives à la santé. Il convient de gérer minutieusement la suppression des droits d'accès de ce personnel. En même temps, bon nombre de transactions ont lieu longtemps après avoir administré les soins (p.ex. signature des transcriptions médicales) Ceci complique le processus de suppression des droits d'accès dans les délais requis. Il faut donc tenir compte de ces transactions lors de l'élaboration et de la mise en œuvre des procédures de suppression des droits d'accès. Les organisations de santé doivent bien réfléchir à la suppression immédiate des droits d'accès suite à la réception ou à l'envoi d'une lettre de licenciement/démission lorsqu'elles sont d'avis que prolonger le droit comporte un risque accru.

A.9.3 Responsabilités des utilisateurs

Objectif: Rendre les utilisateurs responsables de la protection de leurs informations d'authentification

A.9.3.1 Utilisation d'informations secrètes d'authentification

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'exiger des utilisateurs des informations secrètes d'authentification qu'ils appliquent les pratiques de l'organisation en la matière.	Y	Il convient de recommander aux utilisateurs de prendre les précautions suivantes: a) préserver la confidentialité de l'authentification secrète, en s'assurant de ne pas la divulguer à des tiers, ni même à leurs supérieurs; b) ne pas conserver d'enregistrement des informations secrètes d'authentification (par exemple sur support papier, fichier électronique ou équipement portable), sauf si le support de stockage est sûr et si la méthode de stockage a été approuvée (par exemple, un coffre-fort pour mots de passe); c) changer les informations secrètes d'authentification à chaque fois que quelque chose indique qu'elles pourraient être compromises; d) en cas d'utilisation de mots de passe comme information secrète d'authentification, choisir des mots de passe de qualité, d'une longueur minimale suffisante, qui: 1) sont faciles à retenir; 2) ne peuvent pas être rattachés à une information personnelle facile à deviner ou à obtenir, par exemple: noms, numéros de téléphone, dates d'anniversaire, etc.; 3) sont invulnérables à une attaque par dictionnaire (c'est-à-dire un mot de passe uniquement composé de mots figurant dans des dictionnaires); et 4) ne sont pas composés de caractères consécutifs identiques, totalement numériques ou totalement alphabétiques; 5) doivent être changés à la première connexion s'ils sont temporaires; e) ne pas partager les informations secrètes d'authentification d'une personne; f) assurer une protection correcte des mots de passe lorsqu'ils sont utilisés comme information secrète d'authentification dans des procédures de connexion automatique et qu'ils sont stockés; g) ne pas utiliser les mêmes informations secrètes d'authentification pour les activités professionnelles et extra-professionnelles.	Lors de la détermination des responsabilités des utilisateurs, les organisations qui traitent des données relatives à la santé sont tenues de respecter les droits et responsabilités éthiques des prestataires de soins, comme prévus par la loi et acceptés par les membres des organisations de prestataires de santé.

A.9.4 Contrôle de l'accès au système et aux applications

Objectif: Empêcher les accès non autorisés aux systèmes et aux applications

A.9.4.1 Restriction d'accès à l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de restreindre l'accès à l'information et aux fonctions d'application système conformément à la politique de contrôle d'accès.	Y	Il convient que les restrictions d'accès soient fonction des exigences de chaque application métier et conformes à la politique de contrôle d'accès définie. Pour soutenir les exigences relatives aux restrictions d'accès, il convient d'envisager de: a) créer des menus permettant de contrôler l'accès aux fonctions d'application système; b) contrôler les données auxquelles peut accéder un utilisateur donné; c) contrôler les droits d'accès des utilisateurs, par exemple: lecture, écriture, suppression et exécution; d) contrôler les droits d'accès aux autres applications;	Il convient d'apporter une attention particulière aux mesures techniques permettant d'établir l'identité d'un patient de manière sécurisée lorsque celui-ci accède à (une partie de) ses propres données (dans les systèmes d'information de la santé qui permettent ce type d'accès). Il convient de souligner la convivialité de telles mesures, en particulier pour les patients handicapés et de prêter attention à l'accès par des représentants légaux.

		e) limiter les informations contenues dans les éléments de sortie: f) fournir des contrôles d'accès physiques ou logiques permettant d'isoler les applications, les données des applications ou les systèmes sensibles.	

A.9.4.2 Sécuriser les procédures de connexion

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Lorsque la politique de contrôle d'accès l'exige, il convient que l'accès aux systèmes et aux applications soit contrôlé par une procédure de connexion sécurisée.	Y	Il convient de choisir une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur. Lorsqu'un niveau élevé d'authentification et d'identification est requis, il convient d'utiliser des méthodes d'authentification autres que l'utilisation de mots de passe: par exemple un procédé cryptographique, une carte à puce, des jetons d'authentification ou des techniques de biométrie. Il convient que la procédure de connexion à un système ou à une application soit conçue de manière à réduire au minimum les possibilités d'accès non autorisé. Par conséquent, il convient que cette procédure de connexion ne dévoile qu'un minimum d'information sur le système ou l'application, afin d'éviter de faciliter la tâche d'un éventuel utilisateur non autorisé. Il convient qu'une bonne procédure de connexion: a) n'affiche pas les identifiants du système ou de l'application tant que le processus de connexion n'est pas terminé; b) affiche un avertissement précisant que l'accès de l'ordinateur est limité aux seuls utilisateurs autorisés; c) ne propose pas, pendant la procédure de connexion, de messages d'aide qui pourraient faciliter un accès non autorisé; d) valide l'information de connexion seulement lorsque toutes les données d'entrée ont été saisies. Si une condition d'erreur survient, il convient que le système n'indique pas quelle partie des données est correcte ou incorrecte; e) assure une protection contre les tentatives de connexion par force brute; f) enregistre les tentatives réussies et avortées; g) lance une alerte de sécurité en cas de détection d'une brèche possible, réussie ou avortée, dans les contrôles de connexion; h) affiche les informations suivantes après une connexion réussie: 1) la date et l'heure de la dernière connexion réussie; 2) les détails relatifs à toute tentative de connexion avortée depuis la dernière tentative réussie; i) n'affiche pas le mot de passe qui est entré; j) ne transmette pas les mots de passe au sein d'un réseau sous la forme d'un texte en clair; k) mette fin aux sessions inactives au bout d'une période définie d'inactivité, notamment dans les endroits présentant des risques élevés, comme les lieux publics ou à l'extérieur des locaux soumis au management de la sécurité de l'organisation, ou à l'occasion de l'utilisation d'appareils mobiles; l) restreigne les temps de connexion pour apporter une sécurité supplémentaire aux applications à haut risque et réduire les risques de tentatives d'accès non autorisé.	

A.9.4.3 Système de gestion des mots de passe

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins

Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.	Y	Il convient qu'un système de gestion des mots de passe: a) impose l'utilisation d'identifiants et de mots de passe utilisateurs individuels afin de garantir l'imputabilité; b) autorise l'utilisateur à choisir et à modifier ses mots de passe, et prévoie une procédure de confirmation afin de tenir compte des erreurs de saisie; c) impose le choix de mots de passe de qualité; d) impose aux utilisateurs de changer leur mot de passe à la première connexion; e) impose des changements réguliers de mot de passe au besoin; f) tienne à jour un enregistrement des anciens mots de passe et empêche leur réutilisation; g) n'affiche pas les mots de passe à l'écran lors de leur saisie; h) stocke les fichiers de mots de passe à d'autres emplacements que les données d'application système; i) stocke et transmette les mots de passe sous une forme protégée.	

A.9.4.4 Utilisation de programmes utilitaires à privilèges

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de limiter et de contrôler étroitement l'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application.	***N***	Il convient de prendre en compte les directives suivantes en matière d'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application: a) utiliser des procédures d'identification, d'authentification et d'autorisation spécifiques aux programmes utilitaires; b) séparer les programmes utilitaires des logiciels d'application; c) limiter l'emploi des programmes utilitaires à un nombre minimal acceptable d'utilisateurs de confiance bénéficiant d'une autorisation (voir 9.2.3); d) autoriser une utilisation ad hoc des programmes utilitaires; e) poser des limites à la disponibilité des programmes utilitaires, par exemple limiter la durée d'une autorisation de modification; f) journaliser toutes les utilisations de programmes utilitaires; g) définir et documenter les niveaux d'autorisation relatifs aux programmes utilitaires; h) désinstaller ou désactiver tous les programmes utilitaires inutiles; i) ne pas mettre de programmes utilitaires à la disposition des utilisateurs ayant accès à des applications relatives à des systèmes pour lesquels la séparation des tâches est requise.	

A.9.4.5 Contrôle d'accès au code source des programmes

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de restreindre l'accès au code source des programmes.	***N***	Il convient d'exercer un contrôle strict de l'accès au code source des programmes et aux éléments associés (tels que les exigences de conception, les spécifications, les programmes de vérification et de validation), afin d'empêcher l'introduction d'une fonctionnalité non autorisée et d'éviter toute modification involontaire, ainsi que préserver la confidentialité en matière de propriété intellectuelle de valeur. En ce qui concerne le code source des programmes, ce contrôle peut prendre la forme d'un stockage centralisé du code, de préférence dans les bibliothèques de programmes sources. Il convient de prendre en compte les lignes directrices suivantes pour contrôler l'accès aux bibliothèques de programmes sources en vue de réduire les risques d'altération des programmes informatiques:	

		a) lorsque cela est possible, il convient que les bibliothèques de programmes sources ne soient pas stockées sur les systèmes en exploitation; b) il convient que le code source du programme et les bibliothèques de programmes sources soient gérés conformément aux procédures établies; c) il convient que le personnel chargé de l'assistance technique ne dispose pas d'un accès illimité aux bibliothèques de programmes sources; d) il convient que la mise à jour des bibliothèques de programmes sources et des éléments associés, ainsi que la délivrance des programmes sources aux programmeurs ne soient réalisées qu'après attribution d'une autorisation appropriée; e) il convient de stocker les listings de programmes dans un environnement sécurisé; f) il convient de tenir à jour un journal d'audit de tous les accès aux bibliothèques de programmes sources; g) il convient de soumettre les processus de maintenance et de copie des bibliothèques de programmes sources à des procédures strictes de contrôle des modifications (voir 14.2.2). Si le code source du programme est destiné à être publié, il convient d'envisager des mesures supplémentaires pour garantir son intégrité (par exemple, une signature électronique).	

A.10 Cryptographie

A.10.1 Mesures cryptographiques

Objectif: Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

A.10.1.1 Politique d'utilisation des mesures cryptographiques

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.	***N***	Lors de l'élaboration d'une politique cryptographique, il convient de prendre en compte les points suivants: a) l'approche de la direction en ce qui concerne l'utilisation de mesures cryptographiques au sein de l'organisation, y compris les principes généraux de protection en fonction desquels il convient que l'information liée à l'activité de l'organisation soit protégée; b) sur la base d'une appréciation du risque, il convient d'identifier le niveau de protection requis en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement requis; c) l'utilisation d'une technique de chiffrement, en vue de protéger les informations transportées au moyen d'un support sur des appareils amovibles ou mobiles, ou acheminées par des voies d'intercommunication; d) l'approche de gestion des clés, notamment les méthodes à utiliser pour protéger les clés de chiffrement et récupérer des informations chiffrées en cas de perte, de compromission ou d'endommagement des clés; e) les rôles et les responsabilités, par exemple qui est responsable: 1) de la mise en œuvre de la politique;	Des directives relatives à la politique de délivrance et d'utilisation de certificats numériques dans les soins de santé et relatives à la gestion des clés figurent dans la norme ISO 17090-3.

		2) de la gestion des clés, notamment la génération des clés (voir 10.1.2); f) les normes à adopter pour une mise en œuvre efficace dans l'ensemble de l'organisation (quelle solution pour quel processus métier?); g) l'incidence du chiffrement de l'information dans le cas des mesures reposant sur l'analyse de contenu (par exemple, la détection de logiciels malveillants). Lors de la mise en œuvre de la politique cryptographique de l'organisation, il convient de tenir compte de la réglementation et des restrictions nationales pouvant s'appliquer aux techniques cryptographiques dans différentes régions du monde, ainsi que des questions de circulation transfrontalière d'informations chiffrées (voir 18.1.5). Il est possible d'utiliser des mesures cryptographiques pour répondre à différents objectifs de sécurité de l'information tels que: a) la confidentialité: le chiffrement des données permet de protéger l'information sensible ou critique, durant son stockage ou sa transmission; b) l'intégrité/l'authenticité: l'utilisation de signatures électroniques ou de codes d'authentification de message permet de vérifier l'authenticité ou l'intégrité de l'information sensible ou critique, durant son stockage ou sa transmission; c) non-répudiation: l'utilisation de techniques cryptographiques permet d'apporter la preuve de la survenue ou de la non-survenue d'un événement ou d'une action; d) authentification: l'utilisation de techniques cryptographiques permet d'authentifier les utilisateurs et les autres entités système demandant un accès ou engageant une transaction avec des utilisateurs, des entités et des ressources du système.	

A.10.1.2 Gestion des clés

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'élaborer et de mettre en œuvre tout au long de leur cycle de vie une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques.	***Y***	Il convient que la politique comporte des exigences de gestion des clés cryptographiques couvrant l'ensemble de leur cycle de vie: génération, stockage, archivage, extraction, attribution, retrait et destruction des clés. Il convient de sélectionner les algorithmes de chiffrement, la longueur des clés et les pratiques d'utilisation conformément aux bonnes pratiques. Une gestion appropriée des clés exige des processus sécurisés de génération, de stockage, d'archivage, d'extraction, d'attribution, de retrait et de destruction des clés cryptographiques. Il convient de protéger toutes les clés cryptographiques contre tout risque de modification ou de perte. En outre, il est nécessaire de protéger les clés secrètes et privées contre toute utilisation, ainsi que contre toute divulgation non autorisées. Il convient de prévoir une protection physique du matériel utilisé pour générer, stocker et archiver les clés. Il convient que le système de gestion des clés repose sur une série convenue de normes, de procédures et de méthodes sécurisées en vue de: a) générer des clés pour divers systèmes cryptographiques et diverses applications; b) générer et obtenir des certificats de clés publiques; c) attribuer les clés aux utilisateurs prévus et leur indiquer le mode d'activation à la réception des clés; d) stocker les clés, et notamment définir comment les utilisateurs autorisés peuvent accéder aux clés; e) mettre à jour ou remplacer les clés, en prévoyant des règles portant sur les moments auxquels il convient de changer les clés et la façon de procéder;	Des directives relatives à la gestion des clés figurent dans la norme ISO 17090-3. Dans le cadre de ces directives, il convient de se limiter à la gestion de certificats

		f) traiter les clés compromises; g) révoquer les clés, définir notamment le mode de retrait ou de désactivation des clés, par exemple lorsque les clés sont compromises ou lorsqu'un utilisateur quitte l'organisation (dans ce cas, il convient également d'archiver les clés); h) récupérer les clés perdues ou altérées; i) sauvegarder ou archiver les clés; j) détruire les clés; k) journaliser et auditer les activités liées à la gestion des clés. Afin de réduire la probabilité d'utilisation abusive des clefs, il convient de fixer des dates d'activation et de désactivation, de sorte que les clés ne puissent être utilisées que pendant la période de temps définie dans la politique de gestion des clés correspondante. Outre la gestion sécurisée des clés secrètes et privées, il convient de tenir compte de l'authenticité des clés publiques. Ce processus d'authentification peut être mis en œuvre à l'aide de certificats de clés publiques généralement délivrés par une autorité de certification. Il convient que cette dernière soit une organisation reconnue disposant de mesures et de procédures appropriées garantissant le degré de fiabilité requis. Il convient que les accords de service ou les contrats conclus avec des fournisseurs externes de services cryptographiques, par exemple une autorité de certification, couvrent les questions de responsabilité juridique, de fiabilité des services et de réactivité dans la fourniture de ces services (voir 15.2).	

A.11 Sécurité physique et environnementale

A.11.1 Zones sécurisées

Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.

A.11.1.1 Périmètre de sécurité physique

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de définir des périmètres de sécurité servant à protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.	Y	Le cas échéant, il convient d'envisager et de mettre en œuvre les directives suivantes concernant les périmètres de sécurité physique: a) il convient de définir des périmètres de sécurité et il convient que l'emplacement et le niveau de résistance de chacun des périmètres soient fonction des exigences relatives à la sécurité des actifs situés à l'intérieur et des conclusions de l'appréciation du risque; b) il convient que le périmètre d'un bâtiment ou d'un site abritant des moyens de traitement de l'information soit physiquement solide (il convient que le périmètre ou les zones ne présentent aucune faille susceptible de faciliter une intrusion). Il convient que le toit, les murs extérieurs et le sol du site soient construits de manière solide et que les portes extérieures soient toutes convenablement protégées contre les accès non autorisés par des mécanismes de contrôle, par exemple des barres, des alarmes, des verrous. Il convient également de verrouiller les portes et les fenêtres non gardées, et d'envisager une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée; c) il convient de placer du personnel à l'accueil ou des moyens de contrôle d'accès physique au site ou au bâtiment. Il convient de limiter l'accès aux sites et aux bâtiments aux seules personnes autorisées;	Il est important de reconnaître que la création de périmètres de sécurité dans de nombreuses situations de soins pose d'énormes défis. En effet, les patients sont présents dans de nombreux endroits opérationnels. Dans aucune branche d'activité, le public a tant accès aux espaces opérationnels que dans les secteurs des soins de santé. Dans le même temps, il y a lieu de maintenir un environnement sécurisé qui garantit la sécurité physique et la protection des patients et des données et des systèmes accessibles au sein de cet environnement. Il est par exemple possible qu'un patient soit laissé seul dans une salle d'examen (pour que le patient mette un tablier en vue de passer un examen médical), tandis qu'un poste de travail actif est présent dans la salle. La protection des postes de travail dans le secteur des soins ne peut dès lors pas reposer complètement sur l'exclusion d'accès des patients de zones sécurisées. Et ceci contrairement à une banque par exemple où les clients ne

		d) s'il y a lieu, il convient d'ériger des barrières physiques pour empêcher l'accès physique non autorisé et la contamination de l'environnement; e) il convient d'équiper d'une alarme l'ensemble des portes-coupe-feu du périmètre de sécurité, de surveiller ces portes et de les tester en même temps que les murs, pour atteindre le niveau de résistance requis conformément aux normes régionales, nationales et internationales appropriées. Il convient qu'elles fonctionnent conformément au code local de prévention des incendies et de manière infaillible; f) il convient d'installer des systèmes de détection d'intrus adaptés, conformes aux normes nationales, régionales et internationales, et de les tester régulièrement pour s'assurer qu'ils englobent l'ensemble des portes extérieures et des fenêtres accessibles. Il convient que les alarmes des zones inoccupées soient activées en permanence. Il convient également de couvrir les autres zones, comme la salle informatique ou la salle des télécommunications; il convient de séparer physiquement les moyens de traitement de l'information gérés par l'organisation de ceux gérés par des tiers.	sont sans doute jamais laissés seuls dans un environnement avec un poste de travail actif. Par ailleurs, les patients pris en charge médicalement, contrairement aux patients dans d'autres branches d'activités, ne sont souvent pas en mesure d'assurer leur propre sécurité physique et protection. Les mesures de protection physique des informations doivent être rendues conformes aux mesures de protection et de sécurité pour les patients. Les établissements de soins ont le devoir de protéger les deux.

A.11.1.2 Contrôles physiques des accès

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger les zones sécurisées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis..	Y	Il convient de tenir compte des directives suivantes: a) il convient de consigner la date et l'heure d'arrivée et de départ des visiteurs et il convient que tous les visiteurs soient encadrés, sauf si leur accès a déjà été autorisé. Il convient de leur accorder l'accès uniquement à des fins précises ayant fait l'objet d'une autorisation et de leur remettre les instructions relatives aux exigences de sécurité de la zone et aux procédures d'urgence associées. Il convient d'authentifier l'identité des visiteurs à l'aide d'un moyen approprié; b) il convient de restreindre l'accès aux zones de traitement ou de stockage de l'information confidentielle uniquement aux personnes autorisées en mettant en œuvre des contrôles d'accès appropriés, par exemple un système d'authentification à deux facteurs, tels qu'une carte d'accès et un code PIN secret; c) il convient de conserver de manière sécurisée et de contrôler régulièrement un journal physique ou un système de traçabilité électronique de tous les accès; d) il convient d'exiger de l'ensemble des salariés, des contractants et des tiers le port d'un moyen d'identification visible. Il convient qu'ils informent immédiatement le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d'identification visible; e) il convient d'accorder au personnel d'une organisation tiers chargé de l'assistance technique un accès limité aux zones sécurisées ou aux moyens de traitement de l'information confidentielle et uniquement en fonction des nécessités. Il convient que cet accès fasse l'objet d'une autorisation et d'une surveillance; f) il convient de revoir et de mettre à jour régulièrement les droits d'accès aux zones sécurisées et de les révoquer au besoin (voir 9.2.5 et 9.2.6).	Les organisations qui traitent des données personnelles relatives à la santé, sont tenues de prendre des mesures judicieuses pour que le public ne puisse s'approcher des équipements informatiques (serveurs, dispositifs de stockage, terminaux et écrans) que dans la mesure où les contraintes physiques et les processus cliniques l'exigent

A.11.1.3 Sécurisation des bureaux, des salles et des équipements

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins

Il convient de concevoir et d'appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements.	Y	Il convient de prendre en compte les directives suivantes sur la sécurisation des bureaux, des salles et des équipements: a) pour les équipements-clés, il convient de choisir un emplacement non accessible au public; b) dans la mesure du possible, il convient que les bâtiments soient discrets et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur, qui permette d'identifier la présence d'activités de traitement de l'information; c) il convient que les équipements soient configurés de manière à empêcher que l'information confidentielle ou les activités soient visibles et audibles de l'extérieur. Si nécessaire, il convient d'envisager la mise en place d'un bouclier électromagnétique; d) il convient que les répertoires et annuaires téléphoniques internes identifiant l'emplacement des moyens de traitement de l'information confidentielle ne soient pas accessibles sans autorisation.	

A.11.1.4 Protection contre les menaces extérieures et environnementales

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de concevoir et d'appliquer des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents..	Y	Il convient de solliciter les conseils de spécialistes sur la façon d'éviter les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou d'origine humaine.	

A.11.1.5 Travail dans les zones sécurisées

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de concevoir et d'appliquer des procédures pour le travail en zone sécurisée.	***N***	Il convient de tenir compte des directives suivantes: a) il convient que le personnel soit informé de l'existence de zones sécurisées ou des activités qui s'y pratiquent, sur la seule base du besoin d'en connaître; b) il convient d'éviter le travail non supervisé/encadré en zone sécurisée, tant pour des raisons de sécurité personnelle que pour prévenir toute possibilité d'acte malveillant; c) il convient de verrouiller physiquement et de contrôler périodiquement les zones sécurisées inoccupées; d) il convient d'interdire tout équipement photographique, vidéo, audio ou autres dispositifs d'enregistrement, tels que les appareils photos intégrés à des appareils mobiles, sauf autorisation. Les dispositions relatives au travail en zone sécurisée prévoient des mesures applicables aux salariés et aux tiers rattachés aux zones sécurisées; elles concernent toutes les activités se déroulant dans ces zones.	

A.11.1.6 Zones de livraison et de chargement

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de contrôler les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux et, si possible, de les isoler des moyens de	Y	Il convient de tenir compte des directives suivantes: a) il convient que l'accès à une zone de livraison et de chargement depuis l'extérieur du bâtiment soit limité au personnel identifié et autorisé; b) il convient de concevoir la zone de livraison et de chargement de sorte que les marchandises puissent être chargées et déchargées sans que le personnel ait accès aux autres parties du bâtiment;	Il est important de souligner que lors de la prestation de soins, le public (les patients et leurs accompagnateurs) est, dans différentes circonstances, admis physiquement dans des zones où se trouvent de grandes quantités d'informations sensibles (p.ex. expériences dans des laboratoires où le flux de travail exige que des données

traitement de l'information, de façon à éviter les accès non autorisés.		c) il convient de sécuriser les portes extérieures de la zone de livraison et de chargement lorsque les portes intérieures sont ouvertes; d) il convient de contrôler les matières entrantes pour vérifier la présence éventuelle de substances explosives, chimiques ou autres substances dangereuses, avant qu'elles ne quittent la zone de livraison et de chargement; e) il convient d'enregistrer les matières entrantes conformément aux procédures de gestion des actifs (voir l'article 8) dès leur arrivée sur le site; f) dans la mesure du possible, il convient de séparer physiquement les livraisons des expéditions; g) il convient d'examiner les matières entrantes pour vérifier la présence d'éventuelles altérations survenues lors de leur acheminement. Il convient de prévenir immédiatement le personnel de sécurité de toute découverte de ce type.	relatives aux patients soient collectées dans le même local où des données relatives à des patients antérieurs sont également traitées; salle de traitement pour les premiers secours où les accompagnateurs ou membres de la famille sont, le cas échéant, exposés à d'énormes quantités d'informations visuelles et orales sensibles relatives à d'autres patients; postes de travail/postes de travail des infirmiers qui se trouvent directement à côté des chambres des patients). Les espaces physiques dans le secteur des soins où des informations relatives à la santé sont collectées au moyen de conversations et où des systèmes sont présents qui permettent de visualiser des données à l'écran, doivent bénéficier d'une surveillance accrue. Afin de garantir que la vie privée des patients soit respectée, il est souvent requis dans le secteur des soins que des notifications soient apposées dans les ascenseurs, sur les portes dernière lesquelles des conversations ont lieu et à d'autres endroits. Ces notifications servent de rappel qu'il faut limiter au strict minimum de parler de patients dans des zones publiques.

A.11.2 Matériels

Objectif: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

A.11.2.1 Emplacement et protection du matériel

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de déterminer l'emplacement du matériel et de le protéger de manière à réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé.	Y	Il convient de prendre en compte les directives suivantes pour protéger le matériel: a) il convient de déterminer un emplacement pour le matériel permettant de réduire au minimum les accès inutiles aux zones de travail; b) il convient de positionner avec soin les moyens de traitement de l'information manipulant des données sensibles, en vue de réduire le risque que cette information puisse être vue par des personnes non autorisées; c) il convient de sécuriser les moyens de stockage contre tout accès non autorisé; d) il convient de protéger les éléments nécessitant une protection particulière pour abaisser le niveau général de protection requis; e) il convient d'adopter des mesures visant à réduire au minimum les risques de menaces physiques et environnementales potentielles, comme le vol, l'incendie, les explosions, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau), la poussière, les vibrations, les effets engendrés par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme; f) il convient de fixer des directives sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information;	Les organisations qui traitent des informations personnelles relatives à la santé sont tenues de placer les postes de travail éventuels qui offrent un accès à des informations personnelles relatives à la santé, de la sorte à prévenir une consultation ou un accès non intentionnel par des patients et le public. Les appareils médicaux utilisés pour enregistrer ou rapporter des données, peuvent aussi faire l'objet de considérations spéciales en ce qui concerne l'environnement dans lequel ils sont utilisés et les émissions électromagnétiques qui ont lieu pendant leur usage. Les établissements de soins, en particulier les hôpitaux, sont tenus de garantir que les directives de placement et de protection des équipements IT minimalisent l'exposition à ce type d'émissions.

		g) il convient de surveiller les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information; h) il convient d'équiper l'ensemble des bâtiments d'un paratonnerre et il convient d'équiper toutes les lignes électriques et de télécommunication entrantes de parafoudres; i) il convient d'envisager l'utilisation de méthodes spéciales de protection, telles que les claviers à membrane, pour le matériel utilisé en environnement industriel; j) il convient de protéger les moyens de traitement de l'information confidentielle pour réduire au minimum les risques de fuites d'information dues aux émissions électromagnétiques.	

A.11.2.2 Services généraux

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux..	Y	Il convient que les services généraux (tels que l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation et la climatisation): a) soient conformes aux spécifications du fabricant du matériel et aux exigences légales locales; b) fassent l'objet d'une évaluation régulière pour vérifier leur capacité à répondre à la croissance de l'organisation et aux interactions avec les autres services généraux; c) soient examinés et testés de manière régulière pour s'assurer de leur fonctionnement correct; d) soient équipés, si nécessaire, d'alarmes de détection des dysfonctionnements; e) disposent, si nécessaire, d'alimentations multiples sur les réseaux physiques d'acheminement. Il convient que soient prévus des systèmes d'éclairage et de communication d'urgence. Il convient de placer les interrupteurs et les robinets de secours destinés à couper le courant, l'eau, le gaz ou autres services près des sorties de secours et/ou des salles contenant le matériel.	

A.11.2.3 Sécurité du câblage

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information contre toute interception, interférence ou dommage..	***N***	Il convient de prendre en compte les directives suivantes sur la sécurité du câblage: a) il convient d'enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou de les soumettre à toute autre forme de protection adéquate; b) il convient de séparer les câbles électriques des câbles de télécommunication pour éviter toute interférence; c) pour les systèmes sensibles ou critiques, les mesures supplémentaires à envisager comprennent: 1) l'installation d'un conduit de câbles blindé et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités; 2) l'utilisation d'un blindage électromagnétique pour assurer la protection des câbles; 3) le déclenchement de balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles;	Les organisations de santé sont tenues d'accorder une attention particulière à la protection des réseaux et autres câblages dans les zones à hautes émissions provenant d'appareils médicaux.

		4) un accès contrôlé aux panneaux de répartition et aux chambres de câblage.	

A.11.2.4 Maintenance du matériel

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité..	***N***	Il convient de prendre en compte les directives suivantes sur la maintenance du matériel: a) il convient d'entretenir le matériel selon les spécifications et la périodicité recommandées par le fournisseur; b) il convient que seul un personnel de maintenance autorisé assure les réparations et l'entretien du matériel; c) il convient de conserver un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventives ou correctives; d) il convient de mettre en œuvre des mesures appropriées lorsque la maintenance d'un matériel est planifiée en prenant en compte le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'organisation; lorsque cela est nécessaire, il convient que l'information confidentielle contenue dans le matériel soit effacée ou que le personnel de maintenance ait reçu les autorisations suffisantes; e) il convient de respecter toutes les exigences de maintenance qu'imposent les polices d'assurance; f) avant de remettre le matériel en service à l'issue de sa maintenance, il convient de l'inspecter pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement.	Les organisations de santé sont tenues d'accorder une attention particulière à la protection des équipements dans les zones à hautes émissions provenant d'appareils médicaux.

A.11.2.5 Sortie des actifs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisation sans autorisation préalable..	***N***	Il convient de tenir compte des directives suivantes: a) il convient d'identifier clairement les salariés et les tiers qui ont autorité pour permettre le retrait des actifs du site; b) il convient de fixer des limites dans le temps pour la sortie des actifs et de vérifier que la date de retour est respectée; c) le cas échéant, si nécessaire, il convient d'enregistrer la sortie des actifs et leur retour dans les locaux de l'organisation; d) il convient de documenter l'identité, la fonction et l'affiliation de toute personne qui manipule ou utilise les actifs. Il convient que ces documents accompagnent le retour du matériel, de l'information ou des logiciels.	Ces directives sont traitées dans le sujet « télétravail ».

A.11.2.6 Sécurité du matériel et des actifs hors des locaux

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant	***Y***	Il convient que ce soit la direction qui autorise l'utilisation de matériels de traitement et de stockage de l'information hors des locaux de l'organisation. Cela s'applique aux matériels détenus par l'organisation et aux matériels détenus à titre privé, mais utilisés pour le compte de l'organisation.	Spécifiquement dans le secteur des soins, il existe des appareils que les patients doivent parfois emporter. P.ex.

compte des différents risques associés au travail hors site.		Il convient de prendre en compte les directives suivantes concernant la protection du matériel hors site: a) il convient de ne pas laisser le matériel et les supports de données sortis des locaux sans surveillance dans des lieux publics; b) il convient d'observer à tout instant les instructions du fabricant visant à protéger le matériel, par exemple celles sur la protection contre les champs électromagnétiques forts; c) il convient de déterminer des mesures pour les emplacements de travail hors site, comme le travail à domicile, le télétravail et les sites temporaires, en réalisant une appréciation du risque et d'appliquer les mesures nécessaires le cas échéant, par exemple armoires de classement fermant à clé, politique du bureau propre, contrôles d'accès aux ordinateurs et communication sécurisée avec les bureaux de l'organisation (voir également l'ISO/CEI 27033); d) lorsque du matériel circule hors des locaux de l'organisation entre différentes personnes ou entre des tiers, il convient de tenir à jour un journal détaillant la chaîne de traçabilité du matériel, mentionnant au minimum les noms des personnes responsables du matériel, ainsi que les organisations dont elles relèvent. Il convient de tenir compte des risques, comme l'endommagement, le vol ou la mise sur écoute, qui peuvent varier considérablement en fonction des lieux, pour déterminer les mesures les plus appropriées.	Appareil médical pour dialyse, monitoring du rythme cardiaque, … Les applis de santé sur le smarthphone/la tablette, l'ordinateur jouent un rôle de plus en plus important. Il faudra surtout en tenir compte à l'avenir. Voir aussi le sujet 'télétravail'

A.11.2.7 Mise au rebut ou recyclage sécurisé(e) du matériel

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.	Y	Avant la mise au rebut ou la réutilisation du matériel, il convient de vérifier s'il contient ou non un support de stockage. Il convient de détruire physiquement les supports de stockage contenant de l'information confidentielle ou protégée par le droit d'auteur, ou bien de détruire, supprimer ou écraser cette information en privilégiant les techniques rendant l'information d'origine irrécupérable plutôt qu'en utilisant la fonction standard de suppression ou de formatage.	

A.11.2.8 Matériel utilisateur laissé sans surveillance

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les utilisateurs s'assurent que le matériel non surveillé est doté d'une protection appropriée.	Y	Il convient que tous les utilisateurs soient sensibilisés aux exigences et aux procédures de sécurité destinées à protéger les matériels laissés sans surveillance, ainsi qu'aux responsabilités qui leur incombent pour assurer la mise en œuvre de cette protection. Il convient de recommander aux utilisateurs: a) de fermer les sessions actives lorsqu'ils ont terminé, sauf si les sessions peuvent être sécurisées par un mécanisme de verrouillage approprié, par exemple un économiseur d'écran protégé par un mot de passe; b) de se déconnecter des applications ou des services en réseau lorsqu'ils n'en ont plus besoin;	Voir aussi le point 9.3 (responsabilités des utilisateurs)

		c) lorsqu'ils ne s'en servent pas, de protéger les ordinateurs ou les appareils mobiles contre toute utilisation non autorisée par une clé ou un dispositif équivalent tel qu'un mot de passe.	

A.11.2.9 Politique du bureau propre et de l'écran vide

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.	Y	Il convient que la politique du bureau propre et de l'écran vide tienne compte des classes d'information (voir 8.2), des exigences légales et contractuelles (voir 18.1), des risques associés et de la culture de l'organisation. Il convient de tenir compte des directives suivantes: a) lorsque l'information sensible ou critique liée à l'activité de l'organisation n'est pas utilisée, qu'elle soit sous format papier ou sur un support de stockage électronique, il convient de la mettre sous clé (de préférence dans un coffre-fort, une armoire ou tout autre meuble de sécurité), notamment lorsque les locaux sont vides; b) lorsque les ordinateurs et les terminaux sont laissés sans surveillance, il convient de les déconnecter ou de les protéger par un verrouillage de l'écran ou du clavier contrôlé par un mot de passe, un jeton ou un autre mécanisme d'authentification de l'utilisateur. c) Il convient également qu'ils soient protégés par des clés, des mots de passe ou d'autres mesures de sécurité lorsqu'ils ne servent pas; d) il convient d'empêcher l'utilisation non autorisée des photocopieurs et autres appareils de reproduction (par exemple les scanneurs ou les appareils photo numériques);	Il convient que les organisations qui traitent des données relatives à la santé respectent, lors de la détermination des responsabilités des utilisateurs, les droits et responsabilités éthiques des prestataires de soins préves dans la loi et approuvées par les organisations représentatives des prestataires de soins. Voir aussi 9.3 (responsabilités des utilisateurs)

A.12 Sécurité liée à l'exploitation

A.12.1 Procédures et responsabilités liées à l'exploitation

Objectif: S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

A.12.1.1 Procédures d'exploitation documentées

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés.	***Y***	Il convient d'établir des procédures documentées pour les activités d'exploitation liées aux moyens de traitement de l'information et de la communication, telles que les procédures de démarrage et d'arrêt des ordinateurs, la sauvegarde, la maintenance du matériel, la manipulation des supports, la gestion du courrier et de la salle informatique, et la sécurité. Il convient que les procédures d'exploitation précisent les instructions relatives aux activités d'exploitation, notamment: a) la sauvegarde (voir 12.3); b) les relations avec l'assistance technique et la hiérarchie, incluant les relations avec l'assistance technique externe, en cas de difficultés techniques ou d'exploitation inattendues; c) la procédure de redémarrage et de récupération du système à appliquer en cas de défaillance du système; d) la gestion du système de traçabilité et de l'information des journaux système (voir 12.4); e) procédures de monitoring des activités.	Surtout pour les procédures ou applications critiques. Facultatif pour les autres afin d'augmenter la maturité.

A.12.1.2 Gestion des changements

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de contrôler les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information.	Y	Il convient de prendre en compte notamment les éléments suivants: a) l'identification et la consignation des changements significatifs; b) la planification des changements et de la phase de test; c) l'appréciation des incidences potentielles de ces changements, y compris les incidences sur la sécurité de l'information; d) la procédure d'autorisation formelle des changements proposés; e) la vérification que les exigences de sécurité de l'information sont respectées; f) la transmission des informations détaillées sur les changements apportés à toutes les personnes concernées; g) les procédures de repli, incluant les procédures et les responsabilités en cas d'abandon et de récupération suite à l'échec des changements ou à des événements imprévus; h) la mise en place maîtrisée d'un processus de modification d'urgence permettant une mise en œuvre rapide et contrôlée des modifications nécessitées par la résolution d'un incident (voir 16.1). Il convient de mettre en place des procédures et des responsabilités de gestion formelles pour assurer un contrôle satisfaisant de tous les changements apportés. Lorsque des changements sont effectués, il convient de conserver un journal d'audit contenant toute l'information pertinente.	Il est important de signaler que des modifications non correctes, non suffisamment contrôlées ou inappropriées apportées au traitement des données à caractère personnel relatives à la santé peuvent avoir un impact désastreux pour la prise en charge des soins des patients et leur sécurité. Le processus de changement doit évaluer et enregistrer explicitement les risques du changement. La norme ISO/TS 14441 contient des directives détaillées pour tester la conformité des systèmes EHR, dont l'utilisation de données de test. Surtout pour les procédures ou applications critiques. Facultatif pour les autres afin d'augmenter la maturité.

A.12.1.3 Dimensionnement

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour garantir les performances exigées du système.	***N***	Il convient d'identifier les exigences de dimensionnement en tenant compte du caractère critique du système concerné pour l'organisation. Il convient d'appliquer un ajustement au plus près et une surveillance des systèmes pour assurer, et s'il y a lieu améliorer, leur disponibilité et leur efficacité. Il convient de mettre en place des mesures de détection pour identifier les problèmes en temps voulu. Il convient que les projections en matière de dimensionnement futur tiennent compte des nouvelles exigences métier et système, et des orientations présentes et projetées de l'organisation en matière de capacité de traitement de l'information. Il est nécessaire de porter une attention particulière aux ressources pour lesquelles les délais d'approvisionnement sont longs ou les coûts élevés: il convient donc que les responsables surveillent l'utilisation des ressources-clés du système. Il convient que les responsables identifient les évolutions d'utilisation, en particulier en ce qui concerne les applications métier ou les outils de gestion des systèmes d'information. Il convient que les responsables utilisent cette information pour identifier et éviter les goulots d'étranglement potentiels, et pour éviter d'avoir à dépendre de personnel-clé, ce qui peut représenter une menace pour la sécurité du système ou pour les services, et qu'ils planifient l'action appropriée. Il est possible d'atteindre un dimensionnement suffisant en augmentant la capacité du système ou en réduisant la demande. Voici des exemples de gestion de la demande en dimensionnement: a) suppression des données obsolètes (espace disque);	

		b) mise hors service d'applications, de systèmes, de bases de données ou d'environnements; c) optimisation des traitements par lots et de la planification; d) optimisation de la logique des applications ou des requêtes de bases de données; e) refus des services gourmands en ressources ou limitation de la bande passante, si ceux-ci ne sont pas considérés comme critiques pour l'activité (par exemple, les retransmissions vidéo). Il convient d'étudier un plan documenté de la gestion du dimensionnement pour les systèmes critiques.	

A.12.1.4 Séparation des environnements de développement, de test et d'exploitation

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.	Y	Il convient de déterminer et de mettre en œuvre un niveau de séparation entre les environnements d'exploitation, de test et de développement pour prévenir les problèmes d'exploitation. Il convient d'envisager les éléments suivants: a) il convient de définir et de documenter les règles concernant le passage des logiciels du stade de développement au stade d'exploitation; b) il convient d'exécuter les logiciels de développement et les logiciels d'exploitation sur des systèmes ou des microprocesseurs informatiques différents et dans des domaines ou répertoires différents; c) il convient de tester les modifications apportées aux systèmes et aux applications en exploitation dans un environnement de test ou de préproduction avant de les appliquer aux systèmes en exploitation; d) en dehors de circonstances exceptionnelles, il convient de ne pas procéder à des tests sur des systèmes en exploitation. e) il convient que les compilateurs, éditeurs et autres outils de développement ou utilitaires système ne soient accessibles depuis les systèmes en exploitation que lorsque cela est nécessaire; f) il convient que les utilisateurs utilisent des profils utilisateurs différents pour les systèmes en exploitation et les systèmes de test et que les menus affichent les messages d'identification adéquats pour réduire le risque d'erreur; g) il convient de ne pas copier de données sensibles dans l'environnement du système de test, à moins que le système de test soit doté de mesures de sécurité équivalentes (voir 14.3).	Tout hôpital doit définir ce que l'on entend par les différents environnements: • Production • Acceptation • Test • Simulation • Intégration • Développement • … ainsi que les processus peuvent être exécutés dans ces environnements. Il serait par ailleurs intéressant de parvenir à un point de vue commun pour les différentes institutions.

A.12.2 Protection contre les logiciels malveillants

Objectif: Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.

A.12.2.1 Mesures contre les logiciels malveillants

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en œuvre des mesures de détection, de prévention et	Y	Il convient que la protection contre les logiciels malveillants soit fondée sur les programmes de détection de logiciels malveillants et de réparation, la sensibilisation à la sécurité de	

de récupération, conjuguées à une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants.		l'information, et des mesures adéquates de gestion des changements et de l'accès au système. Il convient d'envisager les préconisations suivantes: a) établir une politique formelle prohibant l'utilisation de logiciels non autorisés (voir 12.6.2 et 14.2); b) mettre en œuvre des contrôles destinés à empêcher ou à détecter l'utilisation de logiciels non autorisés (par exemple, listes blanches d'applications); c) mettre en œuvre des contrôles destinés à empêcher ou à détecter l'utilisation de sites web connus pour leur malveillance ou suspectés en tant que tels (par exemple, liste noire); d) établir une politique formelle indiquant les mesures de protection qu'il convient de prendre pour se protéger des risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via les réseaux externes que sur tout autre support; e) réduire les vulnérabilités pouvant être exploitées par des logiciels malveillants, par exemple grâce à une gestion des vulnérabilités techniques (voir 12.6); f) mener des revues régulières des logiciels et du contenu de données des systèmes soutenant les processus métier cruciaux. Il convient de mener une investigation formelle sur la présence de tout fichier non approuvé ou de modifications non autorisées; g) procéder à l'installation et à la mise à jour régulière de logiciels de détection et de réparation pour analyser les ordinateurs et les supports à titre de mesure de précaution ou comme tâche de routine. Il convient que les analyses réalisées incluent: 1) une analyse de tout fichier reçu sur les réseaux ou via toute forme de support de stockage, pour s'assurer de l'absence de logiciels malveillants avant utilisation; 2) une analyse des pièces jointes aux courriers électroniques et des fichiers téléchargés pour s'assurer de l'absence de logiciels malveillants avant utilisation. Il convient de mener cette analyse en différents endroits, par exemple sur les serveurs de messagerie électronique, les ordinateurs de bureau et à l'entrée du réseau de l'organisation; 3) une analyse des pages web pour s'assurer de l'absence de logiciels malveillants; h) définir des procédures et des responsabilités pour assurer la protection des systèmes contre les logiciels malveillants, la formation à l'utilisation de ces systèmes, le signalement et la récupération après une attaque par des logiciels malveillants; i) élaborer des plans appropriés de continuité de l'activité en vue de la récupération après une attaque par logiciel malveillant, comprenant les sauvegardes de tous les logiciels et données nécessaires, et les dispositions de récupération (voir 12.3); j) mettre en œuvre des procédures pour recueillir régulièrement de l'information, comme l'inscription à des listes de diffusion ou la consultation de sites web apportant de l'information sur les nouveaux logiciels malveillants; k) mettre en œuvre des procédures pour vérifier l'information en rapport avec les logiciels malveillants et s'assurer que les bulletins d'alerte sont exacts et informatifs. Il convient que les responsables veillent à l'utilisation de sources qualifiées, telles que des publications réputées, des sites Internet fiables ou des éditeurs de logiciels de protection contre les logiciels malveillants, afin de distinguer les canulars des menaces réelles. Il convient d'informer tous les utilisateurs de l'existence des canulars et de la marche à suivre s'ils en reçoivent; l) isoler les environnements au sein desquels les conséquences peuvent s'avérer désastreuses.	

A.12.3 Sauvegarde

Objectif: Se protéger de la perte de données.

A.12.3.1 Sauvegarde des informations

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de réaliser des copies de sauvegarde de l'information, des logiciels et des images systèmes, et de les tester régulièrement conformément à une politique de sauvegarde convenue.	Y	Il convient d'établir une politique de sauvegarde destinée à définir les exigences de l'organisation en matière de sauvegarde de l'information, des logiciels et des systèmes. Il convient que la politique de sauvegarde définisse les exigences en matière de conservation et de protection des copies de sauvegarde. Il convient de prévoir des équipements de sauvegarde adéquats pour s'assurer que toute l'information et tous les logiciels essentiels peuvent être récupérés en cas de sinistre ou de défaillance d'un support. Lors de la conception d'un plan de sauvegarde, il convient de tenir compte des éléments suivants: a) il convient de produire des enregistrements exacts et complets des copies de sauvegarde effectuées ainsi que des procédures de restauration documentées; b) il convient que l'étendue des sauvegardes (par exemple, sauvegarde totale ou différentielle) et leur fréquence rendent compte des exigences métier de l'organisation, des exigences relatives à la sécurité de l'information concernée, et du caractère critique de l'information pour le maintien de l'activité de l'organisation; c) il convient de placer les sauvegardes à un endroit suffisamment distant du site principal pour échapper à tout dommage résultant d'un sinistre sur le site principal; d) il convient de doter l'information sauvegardée d'un niveau de protection physique et environnementale approprié (voir l'article 11) cohérent avec les normes appliquées sur le site principal; e) il convient de tester régulièrement les supports de sauvegarde pour s'assurer qu'il est possible de s'en servir, le cas échéant, en situation d'urgence. Il convient de combiner cette opération à un test des procédures de restauration et de vérifier le temps de restauration requis. Il convient de tester la capacité de restauration de données sauvegardées sur des supports de test dédiés et de ne pas écraser les supports d'origine au cas où la sauvegarde ou le processus de restauration échouerait, causant la perte de données ou endommageant celles-ci de manière irréversible; f) dans les situations où la confidentialité est importante, il convient de protéger les sauvegardes en les chiffrant. Il convient que les procédures d'exploitation assurent une surveillance de l'exécution des sauvegardes et remédient aux défaillances rencontrées par les sauvegardes programmées, pour garantir l'intégrité des sauvegardes conformément à la politique de sauvegarde. Il convient de tester régulièrement les dispositions de sauvegarde concernant les systèmes et les services individuels, pour s'assurer qu'elles répondent aux plans de continuité de l'activité. Pour les systèmes et les services critiques, il convient que les dispositions relatives aux sauvegardes couvrent toute l'information système, les applications et les données nécessaires à la récupération totale du système en cas de sinistre.	

		Il convient de déterminer la durée de conservation de l'information essentielle à l'activité de l'organisation, en prenant en compte toute éventuelle exigence de conservation à titre permanent de copies d'archivage.	

A.12.4 Journalisation et surveillance

Objectif: Enregistrer les événements et générer des preuves.

A.12.4.1 Journalisation des événements

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de créer, de tenir à jour et de revoir régulièrement les journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information..	Y	Il convient que les journaux d'événement contiennent, lorsque c'est pertinent, les informations suivantes: a) les identifiants utilisateurs; b) les activités du système; c) la date, l'heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session; d) l'identité ou l'emplacement du terminal si possible et l'identifiant du système; e) les enregistrements des tentatives d'accès au système, réussies et avortées; f) les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées; g) les modifications apportées à la configuration du système; h) l'utilisation des privilèges; i) l'emploi des utilitaires et des applications; j) les fichiers qui ont fait l'objet d'un accès et la nature de l'accès; k) les adresses et les protocoles du réseau; l) les alarmes déclenchées par le système de contrôle d'accès; m) l'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection des intrusions; n) les enregistrements des transactions réalisées par les utilisateurs dans les applications. La journalisation des événements pose les fondations des systèmes de surveillance automatisés, capables de générer des rapports consolidés et des alertes relatives à la sécurité du système.	Il convient que les systèmes d'information de la santé qui traitent des données personnelles relatives à la santé créent un rapport d'audit sécurisé chaque fois qu'un utilisateur réalise via le système un accès à des données personnelles de santé, les crée, les met à jour ou les archive. Il convient que le rapport d'audit identifie, de manière unique, l'utilisateur et la personne à laquelle les données ont trait (c.-à-d. le patient), identifie la fonction réalisée par l'utilisateur (créer, accéder à et mettre à jour des enregistrements, etc.) et mentionne la date et l'heure d'exécution de la fonction. Si des informations personnelles relatives à la santé sont mises à jour, il convient de conserver un enregistrement de l'ancien contenu de données et de l'enregistrement d'audit y afférent (c.-à-d. qui a introduit les données à quelle date). Il convient que les systèmes de messageries utilisés pour le transfert de messages contenant des données personnelles relatives à la santé tiennent à jour un enregistrement du transfert des messages (il convient que cet enregistrement mentionne l'heure, la date, l'origine et la destination du message, mais non le contenu). Il convient que l'organisation évalue et détermine scrupuleusement la période de conservation de ces rapports d'audit et tienne notamment compte de normes professionnelles cliniques et d'obligations légales afin de permettre la réalisation d'investigations et la fourniture, le cas échéant, de preuves d'abus. Il convient que la fonctionnalité de rapports d'audit du système d'information de la santé soit opérationnelle à tout moment, alors que le système d'information de la santé qui est contrôlé, est disponible pour être utilisé. Il convient que les systèmes d'information de la santé soient équipés de fonctionnalités d'analyse de rapports et de trajets d'audit qui: a) permettent d'identifier les utilisateurs systèmes ayant consulté ou modifié le dossier de soins d'un patient déterminé au cours d'une période déterminée;

			b) permettent d'identifier tous les patients dont le dossier de soins a été consulté ou modifié au cours d'une période donnée. Les exigences en matière d'enregistrement et de réalisation d'audits constituent les exigences principales pour la protection des données personnelles. Ces exigences constituent une garantie pour les patients qui confient leurs informations aux systèmes d'enregistrement électroniques de dossiers médicaux et constituent également un important stimulant pour les utilisateurs de tels systèmes de respecter la politique en matière d'usage acceptable de ces systèmes. L'enregistrement et la réalisation d'audits efficaces contribuent à démontrer des abus des systèmes d'information de la santé ou des données personnelles relatives à la santé. Ces processus peuvent également aider les organisations et les patients à obtenir un dédommagement par les utilisateurs qui abusent de leurs droits d'accès. Les exigences en matière d'enregistrement des événements sont détaillées dans la norme NEN 7513 et la norme ISO 27789.

A.12.4.2 Protection de l'information journalisée

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger les moyens de journalisation et l'information journalisée contre les risques de falsification ou d'accès non autorisé.	Y	Il convient que des mesures soient conçues pour protéger le moyen de journalisation contre les modifications non autorisées de la journalisation des informations et les dysfonctionnements, à savoir: a) l'altération des types de message enregistrés; b) la modification ou la suppression des fichiers journaux; c) le dépassement de la capacité du support de stockage du fichier journal, qui a pour effet d'empêcher l'enregistrement des événements ou d'écraser les événements déjà enregistrés. Il peut être nécessaire d'archiver certains journaux d'audit dans le cadre de la politique de conservation des enregistrements ou à des fins de collecte et de conservation de preuves (voir 16.1.7).	Il est important d'observer que l'intégrité des enregistrements d'audit en tant que matériel de preuve peut jouer un rôle essentiel lors d'examens par un pathologiste, des investigations concernant des erreurs médicales ou dans d'autres procédures judiciaires ou quasi judiciaires. Dans ces procédures, les prestations par les prestataires de soins et la date et l'heure des événements sont parfois constatés à l'aide d'une analyse des modifications des informations personnelles relatives à la santé d'un individu et de leur mise à jour. Pour garantir la confidentialité et l'intégrité des dossiers médicaux et l'intégrité et la disponibilité des systèmes d'information de la santé, les critères suivants sont repris dans le document IETF RFC 3881. 'Les données d'audit doivent au moins être protégées de la même manière que les données sous-jacentes et les activités contrôlées. Ceci implique des mesures de gestion des accès ainsi que des fonctions de réparation et d'intégrité des données. Le présent document reconnaît la nécessité de la politique et des méthodes

			techniques permettant de réaliser celles-ci sans toutefois les prescrire. Il est concevable qu'il puisse y avoir des utilisations non intentionnelles des données d'audit, par exemple le suivi de la fréquence et de la nature de l'utilisation des systèmes de mesure de la productivité. La norme ASTM E2147-01 prévoit dans son paragraphe 05-03-10 "Verbied gebruik om andere redenen dan het handhaven van beveiliging en het opsporen van schendingen van de beveiliging in gezondheidsinformatieregistratiesystemen, bijvoorbeeld de audits mogen niet worden gebruikt voor het verkennen van activiteiten- of bewegingsprofielen van werknemers." ' (traduction libre – « interdisez l'usage pour des raisons autres que le maintien de la sécurité et la détection de violations de la protection des systèmes d'enregistrement des données relatives à la santé. Il est par exemple interdit d'utiliser les audits pour explorer les profils d'actitivés ou de déplacement des travailleurs »). Il convient que la direction des enregistrements d'audit respecte les normes internationales relatives à la gestion des enregistrements, ISO 15489. Les exigences de sécurité pour l'archivage des enregistrements d'audit sont comparables aux exigences de sécurité pour l'archivage des dossiers médicaux informatisés qui sont spécifiées dans la norme ISO/TS 21547. Il convient d'accorder une attention spéciale à la protection des trajets d'audit distribués. Les dossiers médicaux informatisés peuvent être répartis sur plusieurs systèmes d'information et peuvent avoir trait à différents domaines de la politique de sécurisation; ceci vaut aussi pour les trajets d'audit. Il convient de garantir la protection des trajets d'audit logique. Il convient que le système d'audit prévoie des mesures efficaces permettant de garantir que la mise en exploitation du système d'information de la santé est enregistrée dans le trajet d'audit. Chaque fois que le trajet d'audit est hors service ou déconnecté ou qu'il n'est pas opérationnel suite à une erreur système, il convient de documenter cela dans le système d'audit. Le système d'audit convient d'indiquer ou de mentionner quels audits sont actifs ou inactifs à un moment donné.

			Il convient que l'organisation qui est responsable pour la tenue à jour d'un rapport d'audit définisse la politique de conservation des enregistrements d'audit applicable. Il convient que la conservation des enregistrements d'audit respecte les prescriptions légales et la politique pertinente. Il convient que la conservation des enregistrements d'audit soutienne la durée de vie des dossiers, des données et des documents médicaux. Il convient que le système d'audit prévoit des mesures de protection suffisantes pour protéger les rapports d'audit contre toute falsification. Il convient en particulier que ce système: a) protège l'accès aux enregistrements d'audit; b) protège l'accès aux dispositifs pour réaliser des audits de systèmes et aux trajets d'audit afin de prévenir les abus ou la compromission; c) conserve toutes les activités du trajet d'audit par un enregistrement sécurisé fixant la date et l'heure, la prestation et l'exécutant; d) documente toutes les circonstances dans lesquelles le trajet d'audit est hors service ou déconnecté ou ne fonctionne pas à cause d'une erreur système; e) indique quels audits sont actifs ou inactifs à un moment donné. Il convient que l'accès aux données d'audit soit strictement contrôlé et que ce contrôle soit aussi soumis à un contrôle. Il convient que l'accès ait lieu au moyen d'un système d'information adéquat qui permet de maintenir ces mesures de gestion au lieu d'offrir un accès direct au trajet d'audit. Il convient que les fonctionnalités d'audit prévoient une analyse du trajet d'audit grâce à des champs de données dans l'enregistrement à remplir, le cas échéant par la date/la période, à titre individuel ou en combinaison (par exemple, tous les accès par l'utilisateur X, tous les événements de suppression par les utilisateurs du rôle Y, tous les événements relatifs au patient Z dans le mois écoulé, etc.). Dans certains cas, il se peut qu'un utilisateur de l'audit ait, complémentairement au trajet d'audit, accès à des sources d'information, par exemple pour constater des modèles (p.ex. toutes les requêtes de recherche réalisées par un utilisateur qui n'est pas un pédiatre ou qui n'est pas actif dans la pédiatrie). Des directives relatives à l'archivage de longue durée et à l'intégrité des données sont aussi disponibles dans les

			documents IETF RFC 4810 *Long-Term Archive Service Requirements* et IETF RFC 4998 *Evidence Record Syntax (ERS).*

A.12.4.3 Journaux administrateur et opérateur

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de journaliser les activités de l'administrateur système et de l'opérateur système, ainsi que de protéger et de revoir régulièrement les journaux.	Y	Les détenteurs de comptes utilisateur dotés de privilèges peuvent être à même de manipuler les journaux sur les moyens de traitement de l'information qu'ils contrôlent directement: il est donc nécessaire de protéger et de revoir les journaux afin de garantir l'imputabilité des utilisateurs dotés de privilèges.	

A.12.4.4 Synchronisation des horloges

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de synchroniser les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité sur une source de référence temporelle unique.	***Y***	Il convient de documenter les exigences internes et externes liées à la représentation de l'heure, la synchronisation et la précision. Ces exigences peuvent être des exigences légales, réglementaires, contractuelles, des exigences de conformité à des normes ou des exigences liées à la surveillance interne. Il convient de définir pour l'organisation une heure de référence standard. Il convient de documenter et de mettre en œuvre la méthode utilisée par l'organisation pour obtenir une heure de référence à partir d'une ou des sources externes et la méthode utilisée pour synchroniser de manière fiable les horloges internes.	Il est important d'observer que la date et l'heure des événements qui sont fixés électroniquement dans des informations personnelles relatives à la santé et dans des enregistrements d'audit jouent un rôle essentiel dans les procédures telles que des examens par un pathologiste, des investigations relatives à des erreurs médicales et dans d'autres procédures judiciaires et quasi judiciaires pour lesquelles il est essentiel de fixer avec précision l'ordre clinique des événements. La synchronisation des horloges constitue par ailleurs une condition absolue lorsque l'horodatage est ou doit être utilisé.

A.12.5 Maîtrise des logiciels en exploitation

Objectif: Garantir l'intégrité des systèmes en exploitation.

A.12.5.1 Installation de logiciels sur des systèmes en exploitation

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en œuvre des procédures pour contrôler l'installation de logiciels sur des systèmes en exploitation	Y	Pour contrôler les changements de logiciels sur des systèmes en exploitation, il convient de prendre en compte les directives suivantes: a) il convient que la mise à jour du logiciel en exploitation, des applications et des bibliothèques de programmes soit réalisée uniquement par des administrateurs qualifiés, après autorisation de la direction (voir 9.4.5); b) il convient que les systèmes en exploitation contiennent uniquement des codes exécutables approuvés et non des codes en développement ou des compilateurs; c) il convient de mettre en œuvre les applications et le logiciel du système d'exploitation seulement au terme d'une série complète de tests ayant donné des résultats satisfaisants. Il convient que la batterie de tests porte sur l'aptitude à l'emploi, la sécurité, les effets sur les autres systèmes et la convivialité. Il convient que les tests	Point h) interprétation: en cas de remplacement de logiciels (autre produit par exemple), les données de votre ancien logiciel doivent tout de même encore être disponibles sous certaines conditions, par exemple pour un audit.

		soient réalisés sur des systèmes séparés (voir 12.1.4). Il convient de vérifier que toutes les bibliothèques de programmes sources ont été mises à jour; d) il convient d'utiliser un système de contrôle de la configuration afin de conserver le contrôle de tous les logiciels mis en œuvre, ainsi que de la documentation système; e) il convient de mettre en place une stratégie de retour en arrière avant d'appliquer des modifications; f) il convient de tenir à jour un journal d'audit de toutes les mises à jour réalisées sur les bibliothèques de programmes en exploitation; g) il convient de conserver les versions antérieures du logiciel d'application à titre de mesure de secours; h) il convient d'archiver les versions antérieures du logiciel, ainsi que toute l'information nécessaire, les paramètres, les procédures, les détails de configuration et les logiciels complémentaires associés pendant toute la durée d'archivage des données. Pour les logiciels fournis par l'éditeur et installés sur les systèmes en exploitation, il convient d'assurer une maintenance permettant de bénéficier de l'assistance technique de l'éditeur. Au fil du temps, les éditeurs de logiciels cessent de fournir une assistance technique pour les anciennes versions. Il convient que l'organisation tienne compte des risques associés à l'utilisation de logiciels dont la maintenance n'est pas prise en charge par l'éditeur. Il convient que toute décision d'acquérir une nouvelle version tienne compte des exigences métier à l'origine du changement, ainsi que des questions de sécurité liées à la nouvelle version, à savoir l'introduction d'une nouvelle fonction de sécurité de l'information ou le nombre et la gravité des problèmes de sécurité de l'information liés à cette version. Il convient d'appliquer des correctifs logiciels chaque fois qu'ils permettent de supprimer ou de réduire les failles de sécurité de l'information (voir 12.6). Il convient d'accorder l'accès physique ou logique aux éditeurs uniquement lorsque c'est nécessaire pour répondre aux besoins de l'assistance technique, après autorisation de la direction. Il convient de surveiller les activités de l'éditeur (voir 15.2.1). Les logiciels peuvent dépendre de logiciels et modules fournis par un tiers qu'il convient de surveiller et de contrôler, afin d'éviter tout changement non autorisé susceptible d'introduire des failles de sécurité.	

A.12.6 Gestion des vulnérabilités techniques

Objectif: Empêcher toute exploitation des vulnérabilités techniques.

A.12.6.1 Gestion des vulnérabilités techniques

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'être informé en temps voulu des vulnérabilités techniques des systèmes d'information en exploitation, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les	Y	Pour une gestion efficace des vulnérabilités techniques, il est indispensable de disposer d'un inventaire des actifs, exhaustif et à jour (voir l'article 8). L'information spécifique nécessaire à la gestion des vulnérabilités techniques comporte le nom de l'éditeur du logiciel, les numéros de version, l'état de déploiement (par exemple, quel logiciel est installé sur quels systèmes) et le nom de la ou des personne(s) responsable(s) du logiciel au sein de l'organisation.	Surtout pour les procédures ou applications critiques. Facultatif pour les autres afin d'augmenter la maturité. Quelles sont les applications critiques? Il est préférable d'établir une liste des principales applications critiques pour les hôpitaux. Il y a lieu d'adopter à ce propos un point de vue commun.

mesures appropriées pour traiter le risque associé.		Dès l'identification de vulnérabilités techniques potentielles, il convient d'engager l'action appropriée dans les meilleurs délais. Il convient d'appliquer les recommandations suivantes pour établir un processus efficace de gestion des vulnérabilités techniques: a) il convient que l'organisation définisse et établisse les rôles et les responsabilités associés à la gestion des vulnérabilités techniques, notamment la veille en matière de vulnérabilités, l'appréciation du risque, l'application de correctifs logiciels, le suivi des actifs, ainsi que toute responsabilité de coordination requise; b) il convient de déterminer les ressources d'information permettant d'identifier les vulnérabilités techniques pertinentes et de sensibiliser les intervenants sur ces vulnérabilités, pour les logiciels et les autres technologies (sur la base de l'inventaire des actifs, voir 8.1.1). Il convient de tenir à jour ces ressources d'information sur la base des changements effectués dans l'inventaire ou lorsque des ressources nouvelles ou utiles sont découvertes; c) il convient de définir un délai de réaction aux notifications relatives à d'éventuelles vulnérabilités techniques pertinentes; d) lorsqu'une vulnérabilité technique potentielle est identifiée, il convient que l'organisation détermine les risques associés et les actions à entreprendre: cela peut consister à installer un correctif logiciel sur les systèmes vulnérables ou à appliquer d'autres mesures; e) en fonction du caractère d'urgence présenté par la vulnérabilité technique, il convient que l'action soit entreprise conformément aux mesures de gestion des changements (voir 12.1.2) ou en appliquant les procédures de réponse aux incidents liés à la sécurité de l'information (voir 16.1.5); f) si un correctif logiciel d'une source autorisée est disponible, il convient d'évaluer les risques associés à l'installation de ce correctif (il convient de comparer les risques découlant de la vulnérabilité et les risques associés à l'installation du correctif logiciel); g) il convient d'évaluer et de tester les correctifs logiciels avant de les installer afin de vérifier leur efficacité et de s'assurer qu'ils n'entraînent pas d'effets collatéraux inacceptables. Si aucun correctif logiciel n'est disponible, il convient d'envisager d'autres mesures, telles que: 1) la désactivation des services ou des fonctions liés à la vulnérabilité; 2) l'adaptation ou l'ajout de contrôles d'accès, par exemple des pare-feu, aux limites du réseau (voir 13.1); 3) le renforcement du dispositif de surveillance visant à détecter les attaques réelles; 4) le renforcement de la politique de sensibilisation aux vulnérabilités; h) il convient de tenir un journal d'audit de toutes les procédures entreprises; i) il convient de surveiller et d'évaluer à intervalles réguliers le processus de gestion des vulnérabilités techniques afin de s'assurer de son efficacité; j) il convient de traiter en priorité les systèmes à haut risque; k) il convient d'harmoniser les activités de gestion des incidents avec un processus efficace de gestion des vulnérabilités techniques, pour communiquer les données relatives aux vulnérabilités à la fonction de réponse aux incidents et fournir des procédures techniques à exécuter en cas d'incident; l) définir une procédure s'appliquant aux situations dans lesquelles une vulnérabilité a été identifiée et pour laquelle il n'existe pas de contre-mesure appropriée. Dans cette situation, il convient que l'organisation évalue les risques liés à	

		la vulnérabilité connue et détermine des actions d'investigation et des actions correctives appropriées.	

A.12.6.2 Restrictions liées à l'installation de logiciels

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'établir et de mettre en œuvre des règles régissant l'installation de logiciels par les utilisateurs.	Y	Il convient que l'organisation détermine et impose une politique stricte sur le type de logiciels que les utilisateurs peuvent installer. Il convient d'appliquer le principe du moindre privilège. Les utilisateurs auxquels ont été accordés certains privilèges peuvent avoir la possibilité d'installer des logiciels. Il convient que l'organisation détermine les types de logiciels dont l'installation est autorisée (par exemple l'installation des mises à jour ou de correctifs à des logiciels existants) et les types d'installation qui sont interdits (par exemple, l'installation de logiciels destinés uniquement à un usage personnel, ou de logiciels dont on ignore s'ils sont potentiellement malveillants ou pour lesquels on éprouve des doutes). Il convient d'accorder ces privilèges en tenant compte des fonctions des utilisateurs concernés.	

A.12.7 Considérations sur l'audit du système d'information

Objectif: Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation

.

A.12.7.1 Mesures relatives à l'audit des systèmes d'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Pour réduire au minimum les perturbations subies par les processus métier, il convient de planifier avec soin et d'arrêter avec les personnes intéressées les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation.	***N***	Il convient d'envisager les préconisations suivantes: a) il convient d'arrêter avec la direction concernée les exigences d'audit liées à l'accès aux systèmes et aux données; b) il convient d'arrêter le domaine d'application des tests techniques d'audit et de le contrôler; c) il convient de limiter les tests d'audit à un accès en lecture seule des logiciels et des données; d) il convient que les accès autres qu'en lecture seule ne soient autorisés que pour les copies séparées des fichiers système. Une fois l'audit terminé, il convient soit de les effacer, soit de les protéger de manière appropriée si les exigences de documentation de l'audit imposent de les conserver; e) il convient d'identifier et d'arrêter les exigences relatives aux traitements particuliers ou supplémentaires; f) Il convient que les tests d'audit pouvant compromettre la disponibilité du système soient réalisés en dehors des heures de travail; g) il convient de contrôler et de journaliser tous les accès afin de disposer d'une traçabilité faisant référence.	

A.13 Sécurité des communications

A.13.1 Management de la sécurité des réseaux

Objectif: Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

A.13.1.1 Contrôle des réseaux

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de gérer et de contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications.	Y	Il convient de mettre en œuvre des mesures pour assurer la sécurité de l'information sur les réseaux et la protection des services connectés contre les accès non autorisés. Il convient d'envisager en particulier ce qui suit: a) il convient de définir les responsabilités et les procédures de gestion de l'équipement réseau; b) le cas échéant, il convient de séparer la responsabilité d'exploitation des réseaux et celle de l'exploitation des ordinateurs (voir 6.1.2); c) il convient de définir des mesures spéciales pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics ou les réseaux sans fil et de protéger les systèmes et applications connectés (voir l'article 10 et 13.2). Des mesures spéciales peuvent aussi s'avérer nécessaires pour maintenir la disponibilité des services réseau et des ordinateurs connectés; d) il convient de procéder à une journalisation et d'assurer une surveillance appropriées permettant l'enregistrement et la détection d'actions susceptibles d'affecter la sécurité de l'information ou qui s'avèrent pertinentes pour la sécurité de l'information; e) il convient de coordonner étroitement les activités de gestion à la fois pour optimiser le service fourni à l'organisation et pour s'assurer que les mesures sont appliquées de façon homogène à travers toute l'infrastructure de traitement de l'information; f) il convient d'authentifier les systèmes sur le réseau;	

A.13.1.2 Sécurité des services de réseau

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.	Y	Il convient de déterminer et de surveiller régulièrement la capacité du fournisseur de services de réseau à gérer ses services de façon sécurisée et il convient de conclure un accord sur le droit à auditer. Il convient d'identifier les dispositions de sécurité nécessaires à des services en particulier, telles que les fonctions de sécurité, les niveaux de service et les exigences de gestion. Il convient que l'organisation s'assure que les fournisseurs de services de réseau mettent ces mesures en œuvre.	Il convient que les organisations qui traitent des données personnelles relatives à la santé déterminent de manière précise quel est l'impact de la non-disponibilité de services réseau pour la pratique clinique. Voir aussi le point 17.

A.13.1.3 Cloisonnement des réseaux

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les groupes de services d'information, d'utilisateurs et de	***N***	Une méthode de management de la sécurité des grands réseaux consiste à les diviser en domaines séparés. Les domaines peuvent être choisis à partir des niveaux de sécurisation (par exemple domaine d'accès public, domaine poste de travail, domaine serveur), par	

systèmes d'information soient cloisonnés sur les réseaux.		service administratif (par exemple ressources humaines, financier, marketing) ou par combinaison (par exemple connexion du domaine serveur à de nombreux services administratifs). Le cloisonnement peut être réalisé en utilisant des réseaux physiques différents ou des réseaux logiques différents (par exemple réseau privé virtuel). Il convient de bien définir le périmètre de chaque domaine. L'accès entre les différents domaines du réseau est autorisé, mais il convient de le contrôler au niveau du périmètre en utilisant une passerelle (exemple: pare-feu, routeur-filtre). Il convient de déterminer les critères de cloisonnement des réseaux en domaines et l'accès autorisé au-delà des passerelles en s'appuyant sur une appréciation des exigences de sécurité propres à chaque domaine. Il convient que cette appréciation soit en conformité avec la politique du contrôle d'accès (voir 9.1.1), les exigences d'accès, la valeur et la classification de l'information traitée et qu'elle prenne également en compte le coût relatif et les répercussions sur les performances de l'incorporation d'une technologie de passerelle appropriée. À noter que les réseaux sans fil nécessitent un traitement spécial en raison d'une mauvaise définition du périmètre du réseau. Dans le cas des environnements sensibles, il convient de veiller à traiter l'ensemble des accès sans fil comme des connexions externes et de séparer ces accès des réseaux internes jusqu'à franchissement de la passerelle conformément à la politique de contrôle des réseaux (voir 13.1.1) avant d'accorder l'accès aux systèmes internes. Les technologies d'authentification, de chiffrement et de contrôle d'accès réseau au niveau utilisateur propres aux réseaux sans fil modernes normalisés peuvent être suffisantes pour permettre une connexion directe au réseau interne de l'organisation, lorsqu'elles sont correctement mises en œuvre.	

A.13.2 Transfert de l'information

Objectif: Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

A.13.2 Politique et procédures de transport de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en place des politiques, des procédures et des mesures de transfert formelles pour protéger les transferts d'information transitant par tous types d'équipements de communication.	Y	Il convient que les procédures et mesures à suivre pour utiliser les équipements de communication servant aux transferts de l'information prennent en compte les points suivants: a) les procédures conçues pour protéger l'information transférée contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction; b) les procédures de détection et de protection contre les logiciels malveillants qui peuvent être transmis via l'utilisation des communications électroniques (voir 12.2.1); c) les procédures de protection de l'information électronique sensible communiquée sous forme de pièce jointe; d) une politique ou des directives décrivant succinctement l'utilisation acceptable des équipements de communication (voir 8.1.3); e) les responsabilités incombant aux salariés, aux tiers ou à tout autre utilisateur de ne pas compromette l'organisation, par exemple par diffamation, harcèlement, usurpation d'identité, renvoi de chaînes de messages, achats non autorisés, etc.; f) l'utilisation de techniques de cryptographie, par exemple pour protéger la confidentialité, l'intégrité et l'authenticité de l'information (voir l'article 10);	Il convient que les organisations garantissent que la protection de ces échanges d'informations fassent l'objet du développement d'une politique et d'audits concernant son respect (voir le point 18). La protection des échanges d'informations peut être fortement soutenue par le recours à des contrats relatifs à l'échange de données prescrivant les mesures de gestion qui doivent au minimum être mises en place. Il convient d'accorder une attention spéciale à l'utilisation de moyens cryptographiques. Si ces moyens s'avèrent trop complexes, les utilisateurs dans le secteur des soins pourraient renoncer à leur usage. Voir aussi la directive de mise en œuvre spécifique aux soins définie au point 8.2.1. Des directives spécifiques relatives à la politique d'échange d'informations relatives à la santé sont disponibles dans la

		g) les directives sur la conservation et la mise au rebut de toutes les correspondances commerciales, dont les messages, conformément aux législations et réglementations nationales et locales applicables; h) les mesures et les restrictions liées à l'utilisation des équipements de communication, comme le renvoi automatique de courriers électroniques vers des adresses électroniques extérieures; i) rappeler au personnel de prendre les précautions appropriées pour ne pas divulguer l'information confidentielle; j) ne pas laisser de messages comportant de l'information sensible sur les répondeurs puisque ces derniers peuvent être réécoutés par des personnes non autorisées, stockés sur des systèmes à usage collectif ou incorrectement mémorisés à la suite d'une erreur de numérotation; k) rappeler au personnel les problèmes qu'entraîne l'utilisation de télécopieurs ou de services de télécopie, à savoir: 1) l'accès non autorisé aux mémoires de messages intégrées pour récupérer des messages; 2) la programmation délibérée ou accidentelle de machines pour qu'elles envoient des messages à des numéros précis; 3) l'envoi de documents et de messages au mauvais numéro soit par erreur de numérotation, soit par utilisation d'un numéro mémorisé erroné. En outre, il convient de rappeler au personnel qu'il est recommandé de ne pas tenir de conversation confidentielle dans des lieux publics, sur des réseaux de communication non sécurisés, dans des bureaux ouverts ou des lieux de réunion. Il convient que les équipements de transfert de l'information soient conformes aux exigences légales applicables (voir 18.1).	norme ISO 22857. Bien que la norme internationale renvoie explicitement à un échange transfrontalier de données personnelles relatives à la santé (dans ce contexte, les frontières correspondent aux domaines juridiques relatifs aux soins et non systématiquement aux frontières des pays), de nombreux avis peuvent, le cas échéant, être adaptés en vue de l'échange de données entre organisations.

A.13.2.2 Accords en matière de transfert d'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les accords traitent du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.	***N***	Il convient que les accords en matière de transfert intègrent les aspects suivants: a) les responsabilités de gestion pour contrôler et informer de la transmission, de la répartition et de la réception; b) les procédures pour garantir la traçabilité et la non-répudiation; c) les normes techniques minimales pour l'encapsulation et la transmission; d) les accords de séquestre; e) les normes d'identification coursiers; f) les obligations et les responsabilités en cas d'incident lié à la sécurité de l'information, comme la perte de données; g) l'utilisation convenue d'un système de marquage pour l'information sensible ou critique, permettant de garantir une compréhension immédiate des marques et la protection appropriée de l'information (voir 8.2); h) les normes techniques pour l'enregistrement et la lecture de l'information et des logiciels; i) toutes mesures particulières pouvant s'avérer nécessaires pour la protection des pièces sensibles, comme l'utilisation de la cryptographie (voir l'article 10);	

		j) tenir à jour la traçabilité de l'information en transit; k) les niveaux acceptables de contrôle d'accès. Il convient d'établir et de tenir à jour des politiques, des procédures et des normes pour protéger l'information et les supports physiques en transit (voir 8.3.3), et il convient de les mentionner dans les accords de transfert. Il convient que la partie sécurité de l'information de tout accord mette en évidence la sensibilité de l'information concernée.	

A.13.2.3 Messagerie électronique

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger de manière appropriée l'information transitant par la messagerie électronique.	Y	Il convient que la partie sécurité de l'information de tout accord mette en évidence la sensibilité de l'information concernée. a) une protection des messages contre tout accès non autorisé, toute modification ou déni de service en corrélation avec le plan de classification adopté par l'organisation; b) la qualité de l'adressage et du transport du message; c) la disponibilité et la fiabilité du service; d) les questions juridiques, comme les exigences en matière de signatures numériques; e) l'obtention d'une autorisation avant d'utiliser des services externes publics comme une messagerie instantanée, un réseau social ou le partage de fichiers; f) des niveaux plus élevés d'authentification permettant de contrôler l'accès depuis les réseaux accessibles au public.	Il convient aux organisations qui transfèrent des informations personnelles relatives à la santé au moyen d'une messagerie électronique d'entreprendre des démarches afin de garantir la confidentialité et l'intégrité de ces informations. Il est important d'observer que la protection de la messagerie électronique et des messages contenant des informations personnelles relatives à la santé envoyés via la messagerie instantanée, peut donner lieu à des procédures pour le personnel de la santé qui ne peuvent pas être imposées aux patients et au public. Il convient que l'échange de courriels contenant des informations personnelles relatives à la santé entre prestataires de soins soit chiffré. Il existe à cet effet une approche qui a recours à des certificats numériques. Voir aussi le point 18.1.4 pour un examen du consentement préalable à la communication en dehors de l'organisation.

A.13.2.4 Engagements de confidentialité ou de non-divulgation

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'identifier, de revoir régulièrement et de documenter les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information.	***N***	Il convient que les modalités des engagements de confidentialité ou de non-divulgation spécifient des exigences de protection de l'information confidentielle en des termes juridiquement exécutoires. Les engagements de confidentialité ou de non-divulgation sont applicables aux tiers et aux salariés de l'organisation. Il convient de sélectionner ou d'ajouter des éléments en tenant compte de la catégorie du tiers et des accès ou du traitement de l'information confidentielle acceptables pour sa catégorie. Pour identifier les exigences en matière de confidentialité et de non-divulgation, il convient de tenir compte des éléments suivants: a) une définition de l'information à protéger (par exemple information confidentielle); b) la durée prévue de l'engagement, y compris les cas où il peut s'avérer nécessaire de poursuivre cette durée indéfiniment; c) les actions à entreprendre lorsqu'un engagement arrive à expiration; d) les responsabilités et les tâches des signataires visant à éviter une divulgation non autorisée de l'information;	Il convient que le contrat précité contienne un renvoi aux sanctions possibles en cas de violation de la politique de sécurité de l'information.

		e) la propriété de l'information, des secrets de fabrication et la propriété intellectuelle, ainsi que leurs liens avec la protection de l'information confidentielle; f) l'utilisation autorisée de l'information confidentielle et les droits du signataire relatifs à l'utilisation de cette information; g) le droit d'auditer et de contrôler des activités impliquant l'utilisation de l'information confidentielle; h) le processus de notification et de signalement d'une divulgation non autorisée ou d'une fuite de l'information confidentielle; i) les modalités de retour ou de destruction de l'information à l'expiration de l'engagement; j) les actions à entreprendre en cas de violation de l'engagement. En fonction des exigences de sécurité de l'information de l'organisation, il peut s'avérer nécessaire d'inclure d'autres dispositions dans les engagements de confidentialité ou de non-divulgation. Il convient que les engagements de confidentialité et de non-divulgation soient conformes aux lois et règlements en vigueur dans la juridiction dont ils relèvent (voir 18.1). Il convient de revoir les engagements de confidentialité et de non-divulgation à intervalles réguliers et en cas de changements ayant une incidence sur ces exigences.	

A.14 Acquisition, développement et maintenance des systèmes d'information

A.14.1 Exigences de sécurité applicables aux systèmes d'information

Objectif: Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie.
Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.

A.14.1.1 Analyse et spécification des exigences de sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les exigences liées à la sécurité de l'information figurent dans les exigences des nouveaux systèmes d'information ou des changements apportés aux systèmes existants.	Y	Il convient d'identifier les exigences liées à la sécurité de l'information en utilisant différentes méthodes telles que la prise en compte d'exigences de conformité découlant des règlements et des politiques, les revues, la modélisation des menaces, la revue des incidents et les seuils de vulnérabilité. Il convient de documenter les conclusions de l'identification et de les faire revoir par toutes les parties prenantes. Il convient que les exigences de sécurité de l'information et les mesures rendent compte de la valeur de l'information concernée (voir 8.2), ainsi que des éventuels préjudices pour l'activité de l'organisation pouvant résulter de l'absence d'une sécurité adéquate. Il convient d'intégrer l'identification et la gestion des exigences de sécurité de l'information, ainsi que les processus associés, aux premières phases des projets de système d'information. Tenir compte des exigences de sécurité de l'information au tout début, par exemple dès la phase de conception, peut permettre d'adopter des solutions plus efficaces et plus rentables. En ce qui concerne les exigences de sécurité de l'information, il convient également de prendre en compte les éléments suivants:	ISO/TS 14441 contient un ensemble détaillé d'exigences fonctionnelles relatives à la sécurité et à la vie privée pour les systèmes EHR.

		a) le niveau de confiance requis en ce qui concerne l'identité déclarée des utilisateurs, afin d'en déduire les exigences d'authentification utilisateur; b) la maîtrise de la gestion des accès et des processus d'autorisation pour les utilisateurs de l'organisation ainsi que pour les utilisateurs techniques ou dotés de privilèges; c) l'information des utilisateurs et des opérateurs sur les devoirs et les responsabilités qui leur incombent; d) les exigences de protection que requièrent les actifs impliqués, notamment en ce qui concerne la disponibilité, la confidentialité, l'intégrité; e) les exigences découlant des processus de l'organisation, tels que la journalisation et la surveillance des transactions, les exigences de non-répudiation; f) les exigences spécifiées par les autres mesures de sécurité, telles que les interfaces pour la journalisation et la surveillance ou les systèmes de détection de fuite de données. En ce qui concerne les applications fournissant des services sur les réseaux publics ou mettant en œuvre des transactions, il convient de tenir compte des mesures spéciales des points 14.1.2 et 14.1.3. Lors de l'achat de produits, il convient de suivre un processus formel de test et d'acquisition. Dans les contrats conclus avec le fournisseur, il convient de reprendre les exigences de sécurité définies. Lorsque le produit proposé dispose d'une fonctionnalité de sécurité insuffisante au regard des exigences spécifiées, alors il convient de réexaminer le risque et les mesures associées avant d'acheter ce produit. Il convient d'évaluer et de mettre en œuvre les recommandations liées à la configuration de la sécurité fournies avec le produit en harmonie avec le logiciel final et/ou la pile de services du système. Il convient de définir les critères d'acceptation des produits, par exemple en termes de fonctionnalité, qui garantissent que les exigences de sécurité identifiées sont respectées. Il convient d'évaluer les produits au regard de ces critères avant de procéder à l'achat. Il convient de revoir toute nouvelle fonctionnalité pour s'assurer qu'elle n'entraîne pas de risques supplémentaires inacceptables.	

A.14.1.1.1 Identifier les bénéficiaires de soins de manière unique

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
		Il convient que les systèmes d'information de la santé qui traitent des informations personnelles relatives à la santé, a) garantissent que tout patient puisse être identifié de manière unique dans le système; b) soient en mesure de fusionner des enregistrements doubles ou multiples en cas de constatation de la création non intentionnelle de plusieurs enregistrements pour un seul et même patient ou pendant une urgence médicale.	La prestation de soins dans des cas d'urgence ou autres situations dans lesquelles une identification suffisante des patients n'aura sans doute pas été possible, donne inévitablement lieu à la création de plusieurs enregistrements pour un seul et même patient. Il convient que le système d'information de la santé dispose de la capacité utile pour fusionner les enregistrements de patients multiples en un seul enregistrement. Il convient que cette fusion soit réalisée avec la plus grande précaution. Cette fusion requiert dès lors non seulement du personnel formé à cet effet, mais aussi des moyens techniques pour garantir une meilleure intégration des informations provenant des enregistrements initiaux en un seul tout. Il convient que les organisations qui traitent des informations personnelles relatives à la santé, garantissent que les

			données permettant l'identification des personnes soient uniquement conservées si cela s'avère nécessaire et que des techniques de pseudonymisation, d'anonymisation et de suppression soient utilisées de manière appropriée et de façon aussi générale que possible pour minimaliser le risque de publication non intentionnelle d'informations personnelles.

A.14.1.1.2 Validation des données d'output

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
		Il convient que les systèmes d'information de la santé qui traitent des données personnelles relatives à la santé prévoient des données d'identification de la personne afin d'aider les prestataires de soins à confirmer que l'enregistrement électronique relatif à la santé consulté appartient au patient pris en charge.	Il est nécessaire de prendre en considération plusieurs facteurs complémentaires importants. Avant de faire confiance aux informations personnelles relatives à la santé fournies par un système d'information de la santé, il convient que suffisamment d'informations soient visualisées aux prestataires de soins afin de garantir que les informations consultées appartiennent au patient qu'ils prennent en charge. Le couplage d'un dossier existant à un patient ne constitue pas toujours une tâche banale. Certains systèmes augmentent la sécurité en enregistrant une identification sur la base d'une photo dans tout dossier de patient. Ces améliorations en soi peuvent donner lieu à des problèmes au niveau de la vie privée, étant donné qu'elles autorisent implicitement la détermination de caractéristiques faciales telles la race, qui ne sont pas reprises comme des champs de données. Les conditions d'identification des patients et la disponibilité des données utilisées à cet effet, peuvent varier d'une juridiction à l'autre. Il convient que le développement des systèmes d'information de la santé fassent l'objet d'une attention particulière afin de garantir aux prestataires de soins qu'ils peuvent avoir confiance dans le système qui leur offrira les informations nécessaires pour confirmer que tout dossier consulté appartient bien à la personne qu'ils prennent en charge. Il convient que les systèmes d'information de la santé permettent de contrôler que les impressions sur papier soient complètes (p.ex. page 3/5).

A.14.1.2 Sécurisation des services d'application sur les réseaux publics

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger l'information liée aux services d'application transmise sur les réseaux publics contre les activités frauduleuses, les différends contractuels,	***N***	Pour la sécurité de l'information des services d'application utilisant les réseaux publics, il convient de prendre en compte: a) le niveau de confiance requis par chaque partie en ce qui concerne l'identité déclarée des autres, par exemple par une authentification;	Il est important de souligner qu'il faut déterminer scrupuleusement si les données échangées dans le cadre du commerce électronique et de transactions en ligne constituent des informations personnelles relatives à la santé. Si tel est le cas, il convient de protéger adéquatement

ainsi que la divulgation et la modification non autorisées.		b) les processus d'autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels clés; c) l'assurance que les partenaires engagés dans la communication sont pleinement informés des autorisations qui leur sont accordées pour la fourniture ou l'utilisation du service; d) la détermination et la satisfaction des exigences en matière de confidentialité, d'intégrité, de preuve de la répartition et de la réception des documents-clés et de non-répudiation des contrats, dans le contexte par exemple d'appels d'offres et de contrats; e) le niveau de confiance requis concernant l'intégrité des documents clés; f) les exigences de protection de l'information confidentielle; g) la confidentialité et l'intégrité de toutes transactions de commandes, de détails de paiement, de coordonnées de livraison et de confirmation de réception; h) le degré de vérification adéquat pour contrôler les détails de paiement fournis par le client; i) la sélection du mode de règlement le plus adapté pour se prémunir de la fraude; j) le niveau de protection requis pour maintenir la confidentialité et l'intégrité des éléments du bon de commande; k) le fait d'éviter la perte ou la duplication des détails de la transaction; l) la responsabilité juridique induite par toute transaction frauduleuse; m) les exigences de l'assureur. Une grande partie des considérations ci-dessus peuvent être satisfaites par l'application de mesures de cryptographie (voir l'article 10) tenant compte de la conformité aux exigences légales (voir l'article 18 et plus particulièrement 18.1.5 pour la législation en matière de cryptographie). Il convient qu'un accord documenté, engageant les deux parties conformément aux conditions de service convenues et incluant les détails liés aux autorisations (voir b) ci-dessus) vienne conforter les dispositions des services d'application convenues entre les partenaires. Il convient de tenir compte des exigences de résistance aux attaques, qui peuvent inclure des exigences de protection des serveurs utilisés pour les applications concernées ou de garantie de la disponibilité des interconnexions réseau requises pour délivrer les services.	ces informations. Dans le secteur des soins de santé, il y a lieu d'accorder une attention spéciale aux données concernant les déclarations, les plaintes médicales, les règles de facturation, les créances et aux autres données concernant le commerce électronique dont il est possible de déduire des informations personnelles relatives à la santé.

A.14.1.3 Protection des transactions liées aux services d'application

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger l'information impliquée dans les transactions liées aux services d'application pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.	***N***	Pour la sécurité de l'information des transactions liées aux services d'application, il convient de prendre en compte: a) l'utilisation de signatures électroniques par chacune des parties impliquées dans la transaction; b) l'ensemble des aspects de la transaction, ce qui revient à s'assurer que: 1) les informations secrètes d'authentification utilisateur de toutes les parties sont valables et ont fait l'objet d'une vérification; 2) la transaction demeure confidentielle; 3) la confidentialité des informations personnelles de toutes les parties impliquées est maintenue; c) le canal de communication entre toutes les parties impliquées est chiffré;	

		d) les protocoles utilisés pour la communication entre les parties sont sécurisés; e) la nécessité de veiller à ce que le stockage des détails de la transaction soit situé hors de tout environnement accessible au public, à l'instar d'une plateforme de stockage en place sur l'intranet de l'organisation, et qu'il ne soit pas conservé ou exposé sur un support de stockage directement accessible depuis Internet; f) que lorsqu'une autorité de confiance est utilisée (par exemple dans le but d'émettre et de tenir à jour des signatures ou des certificats électroniques), la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou des signatures.	

A.14.1.3.1 Les informations relatives à la santé accessibles au public

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
		Il convient d'archiver les informations relatives à la santé qui sont accessibles au public (contrairement aux données personnelles relatives à la santé). Il convient de protéger l'intégrité des informations relatives à la santé accessibles au public afin de prévenir des altérations non autorisées. Il convient de mentionner la source (l'auteur) des informations relatives à la santé accessibles au public et d'en protéger l'intégrité.	

A.14.2 Sécurité des processus de développement et d'assistance technique

Objectif: S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.

A.14.2.1 Politique de développement sécurisé

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'établir des règles de développement des logiciels et des systèmes, et de les appliquer aux développements de l'organisation.	Y	Le développement sécurisé est une nécessité pour bâtir un service, une architecture, un logiciel et un système sécurisés. Dans une politique de développement sécurisé, il convient de prendre en compte: a) la sécurité de l'environnement de développement; b) les recommandations liées à la sécurité dans le cycle de vie du développement d'un logiciel: 1) la sécurité de la méthodologie de développement du logiciel; 2) les recommandations relatives à la sécurité du codage pour chaque langage de programmation utilisé; c) les exigences de sécurité dans la phase de conception; d) les points de contrôle de la sécurité aux différentes étapes clés du projet; e) les référentiels sécurisés; f) la sécurité liée au contrôle des versions; g) les connaissances requises en matière de sécurité de l'application; h) les capacités des développeurs à éviter, découvrir et corriger les vulnérabilités. Il convient d'utiliser des techniques de programmation sécurisée pour les nouveaux développements et les scénarios de réutilisation de codes, dans les cas où les normes s'appliquant au développement ne sont pas forcément connues ou lorsqu'elles ne sont pas cohérentes avec les bonnes pratiques en cours. Il convient d'envisager des normes de codage sécurisé et, le cas échéant, rendre leur utilisation obligatoire. Il convient que les	

		développeurs soient formés à leur utilisation et il convient de vérifier leur bonne utilisation en procédant à des tests et des revues de code. Si le développement est externalisé, il convient que l'organisation obtienne l'assurance que les tiers se conforment à ces règles de développement sécurisé (voir 14.2.7).	

A.14.2.2 Procédures de contrôle des changements apportés au système

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de contrôler les changements apportés au système dans le cycle de développement en utilisant des procédures formelles de contrôle des changements.	***N***	Il convient de documenter des procédures formelles de contrôle des changements et d'imposer leur mise en œuvre, afin de garantir l'intégrité des systèmes, des applications et des produits, à partir des toutes premières étapes de la conception et tout au long des opérations de maintenance qui s'ensuivent. Il convient que l'introduction de nouveaux systèmes et les changements de grande ampleur apportés aux systèmes existants suivent une procédure formelle de documentation, de spécification, de phase de tests, de contrôle qualité et de mise en œuvre. Il convient que ce processus intègre une appréciation du risque, une analyse des incidences du changement et une spécification des mesures de sécurité requises. Il convient que ce processus garantisse également que les procédures de sécurité et de contrôle existantes ne sont pas compromises, que les programmeurs chargés de l'assistance n'ont accès qu'aux parties du système nécessaires pour leur permettre d'effectuer leur travail et que tout changement fait l'objet d'un accord formel. Le cas échéant, il convient d'intégrer les procédures de contrôle des changements et des applications (voir 12.1.2). Il convient que les procédures de changement prévoient, sans s'y limiter: a) la tenue à jour d'un enregistrement des niveaux d'autorisation accordés; b) de veiller à ce que les propositions de changements émanent d'utilisateurs autorisés; c) de revoir les commandes et les procédures d'intégrité afin de s'assurer qu'elles ne seront pas compromises par les changements; d) d'identifier tout logiciel, information, élément de base de données et matériel nécessitant un changement; e) d'identifier et de vérifier le code de sécurité critique pour réduire au minimum la probabilité des risques liés aux failles de sécurité connues; f) d'obtenir un accord formel pour les propositions détaillées avant le lancement des travaux; g) de s'assurer que les utilisateurs autorisés acceptent les changements avant leur mise en œuvre; h) de veiller à la mise à jour de la documentation système après chaque changement, et à l'archivage ou la mise au rebut de l'ancienne documentation; i) de tenir à jour un contrôle de version pour toutes les mises à jour logicielles; j) de tenir à jour un système de traçabilité de toutes les demandes de changement; k) de veiller à ce que la documentation du système d'exploitation (voir 12.1.1) et les procédures utilisateurs soient adaptées en fonction des changements; l) de veiller à programmer la mise en œuvre des changements en temps voulu, de manière à ne pas perturber les activités de l'organisation.	

A.14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Lorsque des changements sont apportés aux plateformes d'exploitation, il convient de revoir et de tester les applications critiques métier afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.	N	Il convient que ce processus prévoie: a) la revue des procédures de contrôle et d'intégrité des applications afin de s'assurer qu'elles n'ont pas été compromises par les changements apportés à la plateforme d'exploitation; b) de veiller à ce que les changements apportés à la plateforme d'exploitation soient notifiés en temps opportun, afin que les tests et revues appropriés soient réalisés avant leur mise en œuvre; c) de veiller à ce que les plans de continuité de l'activité soient modifiés en conséquence (voir 17).	Ceci n'est pas toujours possible, c'est pourquoi ceci a été exclu du champ d'application. À titre d'exemple, un appareil médical dont le fabricant scelle l'accès au système et/ou aux données. Cf. Le serveur d'horodatage dont le fabricant ne garantit plus le bon fonctionnement.

A.14.2.4 Restrictions relatives aux changements apportés aux progiciels

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de ne pas encourager la modification des progiciels et de se limiter aux changements nécessaires. Il convient également d'exercer un contrôle strict sur ces changements.	***N***	Dans la mesure du possible, il convient de ne pas apporter de changements aux progiciels fournis par l'éditeur. Lorsqu'une modification du progiciel est nécessaire, il convient de tenir compte des points suivants: a) le risque de compromettre les commandes intégrées et le processus de vérification de l'intégrité; b) le fait qu'il convienne ou non d'obtenir le consentement de l'éditeur; c) la possibilité d'obtenir les changements souhaités auprès de l'éditeur, sous la forme de mises à jour de programme classiques; d) les conséquences si l'organisation devenait responsable de la maintenance du logiciel suite à des changements; e) la compatibilité avec les autres logiciels en service. Lorsque des changements s'avèrent nécessaires, il convient de conserver le logiciel original et d'appliquer ces changements à une copie clairement identifiée. Il convient d'appliquer une politique de gestion des mises à jour afin que tous les logiciels autorisés bénéficient des versions et des correctifs logiciels les plus récents (voir 12.6.1). Il convient de tester avec soin et de documenter tous les changements apportés afin de pouvoir les réappliquer aux versions ultérieures, le cas échéant. Si nécessaire, il convient que les changements apportés soient testés et validés par un organisme indépendant.	

A.14.2.5 Principes d'ingénierie de la sécurité des systèmes

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'établir, de documenter, de tenir à jour et d'appliquer des principes d'ingénierie de la sécurité des systèmes à tous les travaux de mise en oeuvre de systèmes d'information.	Y	Il convient d'établir, de documenter et d'appliquer des procédures d'ingénierie de la sécurité des systèmes d'information, reposant sur les principes d'ingénierie de la sécurité, aux activités internes d'ingénierie des systèmes d'information. Il convient de concevoir la sécurité à tous les niveaux de l'architecture (activité, données, applications et technologie) en préservant l'équilibre entre la nécessité d'une sécurité de l'information et la nécessité de	

.		son accessibilité. Il convient d'analyser les nouvelles technologies au regard des risques de sécurité et il convient de revoir la conception par rapport aux modèles d'attaques connus. Il convient de revoir régulièrement ces principes et les procédures d'ingénierie établies pour s'assurer qu'ils contribuent de manière efficace à l'amélioration des normes de sécurité liées au processus d'ingénierie. Il convient également de les revoir régulièrement pour s'assurer qu'ils restent d'actualité pour combattre toute nouvelle menace potentielle et continuent de s'appliquer aux avancées réalisées dans les technologies et les solutions appliquées. S'il y a lieu, il convient d'appliquer les principes d'ingénierie de la sécurité aux systèmes d'information externalisés par le biais de contrats et autres accords exécutoires passés entre l'organisation et le prestataire auprès duquel l'organisation externalise ses systèmes. Il convient que l'organisation confirme que les principes d'ingénierie de la sécurité du prestataire ont la même rigueur que ses propres principes.	

A.14.2.6 Environnement de développement sécurisé

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les organisations établissent un environnement de développement sécurisé pour les tâches de développement et d'intégration du système, , qui englobe l'intégralité du cycle de développement du système, et qu'ils en assurent la protection de manière appropriée.	Y	Un environnement de développement sécurisé englobera les personnes, les processus et la technologie associés au développement et à l'intégration du système. Il convient que les organisations apprécient les risques liés aux tâches individuelles de développement du système et établissent des environnements de développement sécurisés pour des tâches spécifiques de développement du système en tenant compte: a) de la sensibilité des données à traiter, stocker et transférer par le système; b) des exigences internes et externes applicables, découlant par exemple de règlements ou de politiques; c) des mesures de sécurité déjà mises en œuvre par l'organisation qui appuieront la tâche de développement du système; d) du niveau de fiabilité du personnel travaillant dans l'environnement (voir 7.1.1); e) du degré d'externalisation associé à la tâche de développement du système; f) de la nécessité d'opérer un cloisonnement entre différents environnements de développement: g) du contrôle de l'accès à l'environnement de développement; h) de la surveillance des changements apportés à l'environnement et au code qu'il renferme; i) du stockage des sauvegardes à des emplacements sécurisés hors site; j) du contrôle des déplacements de données à partir de l'environnement et vers l'environnement. Une fois le niveau de protection déterminé pour un environnement de développement spécifique, il convient que les organisations documentent les processus correspondants dans des procédures de développement sécurisé et les fournissent à toutes les personnes en ayant besoin.	

A.14.2.7 Développement externalisé

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins

Il convient que l'organisation supervise et contrôle l'activité de développement du système externalisé.	Y	Lorsqu'un développement de système est externalisé, il convient de considérer les aspects suivants au sein de la chaîne d'approvisionnement de l'organisation: a) accords de licence, propriété du code et droits de propriété intellectuelle relatifs au contenu externalisé (voir 18.1.2); b) exigences contractuelles relatives à la conception sécurisée, au codage et aux pratiques de tests (voir 14.2.1); c) tests d'acceptation pour vérifier la qualité et la précision des fournitures; d) communication des preuves montrant que les seuils de sécurité ont été utilisés pour établir les niveaux minimums acceptables en matière de qualité de la sécurité et de la confidentialité des données personnelles; e) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de contenus volontairement ou involontairement malveillants à la livraison; f) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de vulnérabilités connues; g) accords de séquestre, par exemple si le code source n'est plus disponible; h) droit contractuel de procéder à un audit des processus et des contrôles de développement; i) documentation efficace sur l'environnement servant à créer les livrables; j) l'organisation demeure responsable de la conformité aux lois en vigueur et de la vérification de l'efficacité des mesures.	

A.14.2.8 Phase de test de la sécurité du système

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de réaliser les tests de fonctionnalité de la sécurité pendant le développement.	Y	Les systèmes, nouveaux et mis à jour, nécessitent d'être soumis à des tests et à des vérifications rigoureux pendant les processus de développement, requérant la mise en place d'un programme détaillé des tâches et des données de test d'entrée, avec les résultats attendus en sortie sous un certain nombre de conditions. En ce qui concerne les développements in situ, il convient que ces tests soient réalisés dès le début par l'équipe de développement. Ensuite, il convient de procéder à des tests de conformité indépendants (à la fois pour les développements in situ et externalisés) pour garantir que le système fonctionne comme prévu et uniquement comme prévu (voir 14.1.1 et 14.2.9). Il convient que l'étendue du programme de test soit cohérent avec l'importance et la nature du système.	

A.14.2.9 Test de conformité du système

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de déterminer des programmes de test de conformité et des critères associés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.	Y	Il convient que les tests de conformité du système testent les exigences liées à la sécurité de l'information (voir 14.1.1 et 14.1.2) et le respect des pratiques de développement sécurisé des systèmes (voir 14.2.1). Il convient que des tests soient également menés sur les systèmes intégrés et les composants reçus. Les organisations peuvent recourir à des outils automatiques, tels que des outils d'analyse de code ou des scanneurs de vulnérabilités: il convient qu'elles vérifient les actions correctives apportées aux défauts liés à la sécurité.	Il convient de classer l'ampleur et la précision de ces tests à un niveau correspondant aux risques identifiés du changement. Voir 12.1.2.

		Il convient de réaliser les tests dans un environnement réaliste pour garantir que le système n'introduira pas de vulnérabilités dans l'environnement de l'organisation et que les tests sont fiables.	

A.14.3 Données de test

Objectif: Garantir la protection des données utilisées pour les tests

A.14.3.1 Protection des données de test

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les données de test soient sélectionnées avec soin, protégées et contrôlées.	Y	Dans le cadre de tests, il convient d'éviter d'utiliser des données d'exploitation contenant de l'information personnelle ou toute autre information confidentielle. Si une information personnelle ou toute autre information confidentielle est utilisée dans le cadre de tests, il convient de supprimer tous les détails et contenus sensibles ou de les modifier (voir ISO/CEI 29101[26]). Lorsque des données d'exploitation sont utilisées pour les besoins d'un test, il convient d'appliquer les lignes directrices suivantes afin de les protéger: a) il convient que les procédures de contrôle d'accès, qui s'appliquent aux systèmes d'applications en exploitation, s'appliquent également aux systèmes d'applications de test; b) il convient d'obtenir une nouvelle autorisation chaque fois qu'une information d'exploitation est copiée dans un environnement de test; c) il convient d'effacer les informations d'exploitation d'un environnement de test immédiatement après la fin des tests; d) il convient de journaliser toute reproduction et utilisation de l'information d'exploitation, afin de créer un système de traçabilité.	Il convient que les organisations qui traitent des informations personnelles relatives à la santé n'utilisent pas des données personnelles relatives à la santé réelles en tant que données de test. La norme ISO/TS 14441 contient des directives détaillées pour tester la conformité des systèmes EHR, dont l'utilisation de données de test.

A.15 Relations avec les fournisseurs

A.15.1 Sécurité de l'information dans les relations avec les fournisseurs

Objectif: Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.

A.15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de convenir avec le fournisseur les exigences de sécurité de l'information pour limiter les risques résultant de l'accès du fournisseur aux actifs de l'organisation et de les documenter.	Y	Il convient que les organisations établissent une politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs à l'information de l'organisation. Il convient que ces mesures tiennent compte des processus et des procédures mis en œuvre par l'organisation, ainsi que des processus et des procédures qu'il convient que l'organisation demande au fournisseur de mettre en œuvre, notamment: a) l'identification et la documentation du type de fournisseurs, par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique, auxquels l'organisation accordera un accès à son information; b) un processus et un cycle normalisés de gestion des relations avec les fournisseurs;	L'évaluation des risques est essentielle pour une gestion efficace des accès par des tiers aux systèmes contenant des informations relatives à la santé, à savoir des données personnelles relatives à la santé. Il convient de protéger les droits des patients, même si une partie externe ayant un accès potentiel à des informations relatives à la santé relève d'une autre juridiction que celle compétente pour le patient ou l'organisation de soins.

		c) une définition des types d'accès à l'information que les différents types de fournisseurs se verront accorder, ainsi qu'une surveillance et un contrôle de ces accès; d) les exigences minimales de sécurité de l'information pour chaque type d'information et chaque type d'accès servant de fondement aux accords conclus avec chaque fournisseur, qui reposeront sur les besoins et les exigences de l'organisation et son profil de risque; e) les processus et les procédures permettant de surveiller la conformité aux exigences de sécurité de l'information établies pour chaque type de fournisseur et chaque type d'accès, incluant une revue et une validation des produits par une tierce partie; f) des contrôles de précision et d'exhaustivité pour garantir l'intégrité de l'information ou du traitement de l'information assurés par l'une ou l'autre partie; g) les types d'obligations applicables aux fournisseurs pour protéger l'information de l'organisation; h) le traitement des incidents et des impondérables associés aux accès fournisseurs, incluant les responsabilités de l'organisation et celles des fournisseurs; i) les dispositions de résistance et, si nécessaire, de récupération et de secours pour garantir la disponibilité de l'information ou du traitement de l'information assurés par l'une ou l'autre partie; j) une formation à la sensibilisation aux politiques, aux processus et aux procédures applicables pour le personnel de l'organisation impliqué dans les achats; k) une formation à la sensibilisation du personnel de l'organisation en interaction avec le personnel du fournisseur, sur les règles appropriées d'engagement et de comportement en fonction du type de fournisseur et du niveau d'accès du fournisseur aux systèmes et à l'information de l'organisation; l) les conditions dans lesquelles les exigences et les mesures de sécurité de l'information seront documentées dans un accord signé par les deux parties; m) la gestion des transitions nécessaires de l'information, des moyens de traitement de l'information et tout ce qui transite en général, et l'assurance que la sécurité de l'information est maintenue tout au long de la période de transition.	

A.15.1.2 La sécurité dans les accords conclus avec les fournisseurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les exigences applicables liées à la sécurité de l'information soient établies et convenues avec chaque fournisseur pouvant avoir accès, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.	Y	Il convient de rédiger et de documenter les accords de fournisseur de sorte à s'assurer qu'il n'y ait aucun malentendu entre l'organisation et le fournisseur concernant les devoirs des deux parties à répondre aux exigences de sécurité de l'information applicables. Pour répondre aux exigences de sécurité de l'information identifiées, il convient d'envisager d'inclure les conditions suivantes dans l'accord: a) description de l'information à fournir ou à laquelle l'accès doit être rendu possible et des méthodes utilisées pour fournir ces informations ou y accéder; b) la classification de l'information selon le plan de classification de l'organisation (voir 8.2): si nécessaire, en outre, la mise en correspondance du plan de classification de l'organisation et du plan de classification du fournisseur; c) les exigences légales et réglementaires, y compris la protection des données, les droits de propriété intellectuelle et les droits d'auteur, et la description de la méthode servant à garantir qu'elles sont respectées;	La gestion de la prestation de services par des tiers peut être fortement simplifiée par la conclusion d'un contrat formel précisant les mesures de gestion minimales à mettre en place.

		d) obligation pour chaque partie au contrat de mettre en œuvre un ensemble convenu de contrôles, incluant le contrôle d'accès, la revue des performances, la surveillance, la rédaction de rapport et l'audit; e) les règles d'utilisation acceptable de l'information, y compris, si nécessaire, les conditions d'utilisation inacceptables; f) soit une liste explicite des salariés du fournisseur autorisés à recevoir ou à accéder à l'information de l'organisation, soit des procédures ou conditions liées à l'octroi et au retrait d'autorisations pour l'accès à l'information de l'organisation ou la réception d'information de l'organisation à destination des salariés du fournisseur; g) les politiques de sécurité de l'information pertinentes pour le contrat spécifique; h) les exigences et les procédures de gestion des incidents (notamment la notification et la collaboration lors de l'action corrective); i) les exigences de formation et de sensibilisation aux procédures spécifiques et aux exigences de sécurité de l'information, par exemple la réponse aux incidents, les procédures d'autorisation; j) les règlementations à prendre en compte concernant la sous-traitance, y compris les mesures qu'il est nécessaire de mettre en œuvre; k) les partenaires signataires de l'accord, avec une personne de contact pour les questions de sécurité liées à l'information; l) les exigences de sélection, le cas échéant, des salariés du fournisseur, incluant les responsabilités liées aux procédures de sélection et de notification si la sélection n'a pas abouti ou si les résultats sont source d'inquiétude ou de doute; m) le droit d'auditer les processus et les mesures de sécurité du fournisseur en rapport avec le contrat; n) les processus de résolution des défauts et de résolution des conflits; o) l'obligation du fournisseur à communiquer périodiquement un rapport indépendant sur l'efficacité des mesures et son accord pour apporter en temps opportun les actions correctives aux problèmes soulevés dans le rapport; p) l'obligation du fournisseur à se conformer aux exigences de sécurité de l'organisation.	

A.15.1.3 Chaine d'approvisionnement informatique

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les accords conclus avec les fournisseurs incluent des exigences sur le traitement des risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et des services informatiques.	Y	Il convient d'étudier l'intégration aux accords des fournisseurs des aspects suivants relatifs à la sécurité de la chaîne d'approvisionnement: a) la définition des exigences de sécurité de l'information à appliquer à l'achat de produits ou de services informatiques, en plus des exigences de sécurité de l'information générales applicables aux relations avec les fournisseurs; b) en ce qui concerne les services informatiques, l'obligation pour les fournisseurs de diffuser les exigences de sécurité de l'organisation jusqu'au dernier maillon de la chaîne d'approvisionnement si le fournisseur sous-traite des parties des services informatiques qu'il fournit à l'organisation; c) en ce qui concerne les produits informatiques, l'obligation pour les fournisseurs de diffuser les pratiques de sécurité appropriées jusqu'au dernier maillon de la chaîne d'approvisionnement si ces produits comportent des composants achetés chez d'autres fournisseurs;	

		d) la mise en œuvre d'un processus de surveillance et de méthodes acceptables permettant de confirmer que les produits et les services informatiques livrés respectent les exigences de sécurité stipulées; e) la mise en œuvre d'un processus d'identification des composants d'un produit ou d'un service critiques pour le maintien des fonctionnalités et qui nécessitent, par conséquent, plus d'attention et de soins lorsqu'ils sont élaborés en dehors de l'organisation, notamment si le fournisseur principal sous-traite certains aspects des composants du produit ou du service à d'autres fournisseurs; f) la garantie que les composants critiques et leur origine peuvent être tracés tout au long de la chaîne d'approvisionnement; g) la garantie que les produits informatiques livrés fonctionnent comme prévu et ne présentent aucune fonctionnalité inattendue ou indésirable; h) la définition de règles de partage de l'information concernant la chaîne d'approvisionnement et tous les problèmes et compromis possibles entre l'organisation et les fournisseurs; i) la mise en œuvre de processus spécifiques de gestion du cycle de vie des composants informatiques et de leur disponibilité, ainsi que les risques associés liés à la sécurité. Cela inclut la gestion des risques présentés par la rupture de stock de composants, les fournisseurs ayant cessé leur activité ou ayant arrêté de produire ces composants en raison des avancées technologiques.	

A.15.2 Gestion de la prestation du service

Objectif: Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.

A.15.2.1 Surveillance et revue des services des fournisseurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les organisations surveillent, revoient et auditent à intervalles réguliers la prestation des services assurés par les fournisseurs.	Y	Il convient que la surveillance et la revue des services des fournisseurs garantissent que les conditions générales sur la sécurité de l'information prévues dans les accords sont respectées et que les incidents et les problèmes liés à la sécurité de l'information sont gérés correctement. Il convient qu'il existe, à cet effet, un processus relationnel de gestion des services entre l'organisation et le fournisseur en vue de: a) surveiller les niveaux de performance des services et vérifier ainsi qu'ils sont conformes aux accords; b) revoir les rapports de service produits par le fournisseur et organiser des réunions régulières sur l'avancement comme l'exigent les accords; c) mener des audits des fournisseurs conjointement à la revue de rapports d'audits indépendants, s'ils existent, et assurer un suivi des problèmes identifiés; d) fournir l'information relative aux incidents liés à la sécurité de l'information et assurer une revue de cette information comme l'exigent les accords et toutes les lignes directrices et procédures d'accompagnement; e) revoir les systèmes de traçabilité et les enregistrements du fournisseur concernant les événements liés à la sécurité de l'information, les problèmes d'exploitation, les défaillances et le suivi des pannes et des interruptions liées au service fourni; f) résoudre et gérer tout problème identifié;	Voir aussi la directive de mise en œuvre spécifique aux soins mentionnée au point 15.1.2.

		g) revoir les aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs; h) s'assurer que le fournisseur maintient une capacité de service suffisante ainsi que des plans exploitables conçus pour garantir le maintien du niveau de continuité de service convenu en cas de défaillance majeure du service ou de sinistre (voir l'article 17). Il convient d'attribuer la responsabilité de la gestion des relations avec les fournisseurs à une personne désignée ou à une équipe de gestion des services. En outre, il convient que l'organisation s'assure que les fournisseurs nomment les personnes chargées de contrôler le respect et l'application des exigences stipulées dans les accords. Il convient de prévoir les compétences et ressources techniques suffisantes pour veiller à ce que les exigences du contrat, et en particulier celles qui traitent de la sécurité de l'information, sont respectées. Il convient de prendre les mesures adéquates lorsque des insuffisances sont observées dans la prestation du service. Il convient que l'organisation conserve une visibilité et un contrôle global suffisants sur tous les aspects de la sécurité ayant trait à l'information ou aux moyens de traitement de l'information sensible ou critique auxquels le fournisseur a accès, qu'il traite ou qu'il gère. Il convient que l'organisation veille à conserver, par un processus de signalement défini, une visibilité sur les activités liées à la sécurité, telles que la gestion des changements, l'identification des vulnérabilités et le signalement des incidents liés à la sécurité de l'information et les réponses qui y sont apportées.	

A.15.2.2 Gestion des changements apportés dans les services des fournisseurs

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de gérer les changements effectués dans les prestations de service des fournisseurs, y compris le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation du risque.	Y	Il convient de tenir compte des facteurs suivants: a) les changements apportés aux accords passés avec les fournisseurs; b) les changements effectués par l'organisation pour mettre en œuvre: 1) des améliorations aux services offerts; 2) le développement d'applications et de systèmes nouveaux; 3) des changements ou des mises à jour des politiques et des procédures de l'organisation; 4) des mesures nouvelles ou modifiées permettant de résoudre les incidents liés à la sécurité de l'information et d'améliorer la sécurité; c) les changements dans les services assurés par les fournisseurs pour mettre en œuvre: 1) des changements et des améliorations apportées aux réseaux; 2) l'utilisation de nouvelles technologies; 3) l'adoption de nouveaux produits ou des versions/des éditions plus récentes; 4) des outils et des environnements de développement nouveaux; 5) des changements apportés à l'emplacement physique des équipements de dépannage; 6) des changements de fournisseurs; 7) la sous-traitance à un autre fournisseur.	Voir aussi la directive de mise en œuvre spécifique aux soins définie au point 15.1.2.

A.16 Gestion des incidents liés à la sécurité de l'information

A.16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Objectif: Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.

A.16.1 Responsabilités et procédures

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.	Y	Il convient d'examiner les recommandations suivantes en matière de responsabilités et de procédures de gestion des incidents liés à la sécurité de l'information: a) il convient d'établir des responsabilités de gestion pour garantir que les procédures suivantes sont développées et communiquées de manière adéquate au sein de l'organisation: 1) procédures de planification et de préparation des réponses aux incidents; 2) procédures de surveillance, de détection, d'analyse et de signalement des événements et des incidents liés à la sécurité de l'information; 3) procédures de journalisation des activités de gestion des incidents; 4) procédures de traitement des preuves scientifiques; 5) procédures d'appréciation et de prise de décision relatives aux événements liés à la sécurité de l'information et d'appréciation des failles liées à la sécurité de l'information; 6) procédures de réponse, incluant les procédures de remontée d'information, de récupération contrôlée de l'incident et de communication aux organisations ou aux personnes internes ou extérieures à l'organisation; b) il convient que les procédures établies garantissent: 1) qu'un personnel compétent au sein de l'organisation traite les questions relatives aux incidents liés à la sécurité de l'information; 2) qu'un point de contact pour la détection et le signalement des incidents liés à la sécurité existe; 3) que des contacts appropriés sont entretenus avec les autorités, les groupes d'intérêts externes ou les forums qui traitent des questions relatives aux incidents liés à la sécurité de l'information. c) il convient que les procédures de signalement prévoient: 1) des formulaires spécifiques destinés à faciliter le signalement, récapitulant toutes les actions à mettre en œuvre lorsqu'un événement lié à la sécurité de l'information est détecté; 2) la procédure à engager lorsqu'un événement lié à la sécurité de l'information se produit, à savoir: noter immédiatement tous les détails (par exemple le type de non-conformité ou de défaillance, le dysfonctionnement constaté, les messages apparaissant à l'écran) et en informer immédiatement le responsable servant de point de contact et n'exécuter que des actions concertées; 3) une référence à un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité;	

		4) des processus de retour d'information adéquats, afin de communiquer les détails de la résolution du problème aux personnes ayant signalé un événement, une fois que le problème a été réglé et clôturé. Il convient que les objectifs de la gestion des incidents liés à la sécurité de l'information fassent l'objet d'un accord avec la direction. Il convient également de s'assurer que les personnes responsables de la gestion des incidents liés à la sécurité de l'information connaissent les priorités de l'organisation dans ce domaine.	

A.16.1.2 Signalement des événements liés à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées.	Y	Il convient d'informer tous les salariés et contractants de leur obligation de signaler les événements liés à la sécurité de l'information dans les meilleurs délais. Il convient de les informer de l'existence d'une procédure de signalement des événements liés à la sécurité de l'information et d'un responsable servant de point de contact auprès duquel effectuer le signalement. Exemples de situations dans lesquelles envisager le signalement d'un événement: a) une mesure de sécurité inefficace; b) une violation de l'intégrité de l'information, de sa confidentialité ou de sa disponibilité; c) une erreur humaine; d) le non-respect des politiques ou des recommandations; e) une violation des dispositions relatives à la sécurité physique; f) un changement non contrôlé apporté au système; g) un dysfonctionnement logiciel ou matériel; h) une violation d'accès.	Les organisations de la santé ont tendance à opérer une distinction artificielle entre les incidents liés à la sécurité de l'information et les autres types d'incidents, tant en ce qui concerne leur traitement que leur rapportage. Étant donné qu'une intrusion pourrait donner lieu au vol de matériel IT (ce qui donne lieu à une violation de la confidentialité) ou qu'un incendie pourrait être causé pour cacher l'abus de matériel IT, ou que l'abus identifié ou l'usage erroné du système pourrait avoir eu un impact clinique, il y a lieu de réaliser une évaluation de la sécurité de l'information de tous ces types d'incidents ou d'un incident représentatif afin de poursuivre l'évaluation de l'efficacité des mesures de gestion mises en place et de l'analyse des risques qui a donné lieu à leur mise en place.

A.16.1.3 Signalement des failles liées à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'enjoindre tous les salariés et contractants utilisant les systèmes et services d'information de l'organisation à noter et à signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	Y	Il convient que tous les salariés et contractants signalent ce type de problème au responsable servant de point de contact dans les meilleurs délais, afin d'éviter des incidents liés à la sécurité de l'information. Il convient que le mécanisme de signalement soit aussi simple, accessible et disponible que possible.	

A.16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient d'apprécier les événements liés à la sécurité de l'information et de décider s'ils doivent être classés comme incidents liés à la sécurité de l'information.	Y	Il convient que le responsable servant de point de contact apprécie chaque événement lié à la sécurité de l'information en utilisant l'échelle de classification des incidents et des événements liés à la sécurité de l'information convenue et qu'il décide s'il convient de classer l'événement comme tel. La classification et la hiérarchisation des incidents peuvent permettre d'identifier les conséquences et l'étendue d'un incident.	Les organisations qui traitent des données personnelles relatives à la santé doivent évaluer si l'événement lié à la sécurité de l'information concernait une donnée personnelle relative à la santé.

		Au cas où l'organisation dispose d'une équipe chargée de la réponse aux incidents liés à la sécurité de l'information, l'appréciation et la décision peuvent être transmises à cette équipe en vue de leur confirmation ou d'une nouvelle appréciation. Il convient d'enregistrer les conclusions de l'appréciation et la décision de manière détaillée en vue de contrôles ou de références ultérieurs.	

A.16.1.5 Réponse aux incidents liés à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de répondre aux incidents liés à la sécurité de l'information conformément aux procédures documentées.	Y	Il convient que ce soit le responsable servant de point de contact et les autres personnes concernées de l'organisation, ou relevant des tiers, qui répondent aux incidents liés à la sécurité de l'information (voir le point 16.1.1). Il convient que la réponse comporte: a) le recueil de preuves aussitôt que possible après l'incident; b) une analyse scientifique de la sécurité de l'information, le cas échéant (voir 16.1.7); c) une remontée d'informations, le cas échéant; d) l'assurance que toutes les tâches concernant la réponse sont correctement journalisées en vue d'une analyse ultérieure; e) la communication de l'existence d'un incident lié à la sécurité de l'information ou de tout détail pertinent qui s'y rapporte aux autres personnes internes et externes à l'organisation ou aux organisations ayant besoin d'en connaître; f) le traitement de la ou des failles constatées dans la sécurité de l'information causant ou contribuant à l'incident; g) une fois que l'incident a été résolu avec succès, la clôture formelle de l'incident et son enregistrement. Il convient de procéder à une analyse postérieure à l'incident, le cas échéant, pour identifier la source de l'incident.	

A.16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de tirer parti des connaissances recueillies suite à l'analyse et la résolution des incidents liés à la sécurité de l'information pour réduire la probabilité ou les conséquences d'incidents ultérieurs.	Y	Il convient de mettre en place des mécanismes permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information, ainsi que leur volume et les coûts associés. Il convient de se servir de l'information recueillie lors de cette évaluation pour identifier les incidents récurrents ou ayant des conséquences graves.	

A.16.1.7 Recueil de preuves

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'organisation définisse et applique des procédures d'identification, de recueil, d'acquisition et de protection	Y	Il convient de mettre au point et d'appliquer des procédures internes de traitement des preuves dans le cadre d'une action judiciaire et disciplinaire. Il convient, en général, que les procédures relatives aux preuves prévoient des processus d'identification, de recueil, d'acquisition et de protection selon les différents types de	Les organisations qui traitent des données personnelles relatives à la santé doivent éventuellement accorder une attention particulière aux implications de la collecte de preuves permettant de prouver des erreurs médicales et aux

de l'information pouvant servir de preuve.		supports, de dispositifs et d'état des dispositifs, par exemple allumé ou éteint. Il convient que les procédures prennent en compte: a) la chaîne de traçabilité; b) la sécurité des preuves; c) la sécurité du personnel; d) les fonctions et les responsabilités du personnel impliqué; e) les aptitudes du personnel; f) la documentation; g) les séances d'information. S'il en existe, il convient de rechercher les certifications et autres justificatifs de la qualification du personnel et des outils, de sorte à renforcer la valeur des preuves protégées. Les preuves scientifiques peuvent dépasser les limites de l'organisation ou les frontières juridictionnelles. Dans ce cas, il convient de s'assurer que l'organisation est habilitée à recueillir les informations devant servir de preuve scientifique. Il convient de tenir compte des exigences des diverses juridictions afin d'optimiser l'admissibilité de la preuve auprès des juridictions compétentes.	exigences interjuridictionnelles lorsque les systèmes d'information de la santé sont accessibles au-delà des frontières de leur propre juridiction.

A.17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

A.17.1 Continuité de la sécurité de l'information

Objectif: Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité.

A.17.1.1 Organisation de la continuité de la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'organisation détermine ses exigences en matière de sécurité de l'information et de continuité du management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre.	Y	Il convient que l'organisation détermine si la continuité de la sécurité de l'information est intégrée au processus de gestion de la continuité de l'activité ou au processus de gestion de la récupération après sinistre. Il convient de déterminer les exigences de sécurité de l'information lors de l'élaboration du programme de récupération en cas de sinistre et de continuité de l'activité. En l'absence de programme formel de récupération en cas de sinistre et de continuité de l'activité, il convient que le management de la sécurité de l'information parte du principe que les exigences de sécurité de l'information restent les mêmes tant dans des situations défavorables que dans des conditions d'exploitation normales. Il est également possible qu'une organisation réalise une analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information pour déterminer les exigences de sécurité de l'information applicables aux situations défavorables.	Les considérations suivantes sont importantes dans les environnements de soins. La gestion de la continuité des activités qui comprend également la récupération après sinistre, est de plus en souvent reconnue comme une exigence pour les organisations de la santé et fait l'objet d'une priorité de plus en plus élevée. Compte tenu des exigences strictes en matière de disponibilité des soins de santé, il convient d'investir de manière significative dans des dispositifs de résilience et de redondance, non seulement en ce qui concerne la technologie en tant que telle, mais aussi en ce qui concerne la formation plus large du personnel de santé. La planification de la continuité des activités dans le secteur des soins de santé est un défi particulier pour le professionnel de la sécurité de l'information, étant donné que tous les plans doivent être intégrés de manière appropriée dans les plans de l'organisation pour faire face aux pannes de courant, mettre en œuvre le contrôle des

			infections et traiter d'autres urgences cliniques. Si l'on fait appel à l'un de ces plans, il est également probable que cela donne directement lieu à un recours au plan de gestion de la continuité des activités, ne fusse que pour fournir un soutien supplémentaire au-delà de celui normalement disponible. Toutefois, des incidents récents, tels que l'épidémie de SRAS, ont montré que des incidents majeurs peuvent entraîner des pénuries de personnel qui peuvent alors limiter fortement la capacité à mettre en œuvre avec succès des plans de gestion de la continuité des activités. Les établissements de soins doivent veiller à ce que leur plan de gestion de la continuité des activités comprenne un plan de gestion des crises sanitaires. En effet, la vie de patients peut dépendre de l'accès aux données du patient. Il est essentiel d'en tenir compte dans le planning. Les catastrophes et les crises de force majeure qui mettent hors service les systèmes informatiques dans d'autres secteurs d'activités sont précisément les événements qui peuvent conduire à une crise de santé publique. L'accès à temps aux informations relatives à la santé constitue en effet un élément crucial. Les organisations actives dans le secteur des soins de santé doivent aussi garantir que les plans qu'ils développent, soient régulièrement testés en termes de programmes. Les tests inclus dans ce programme devraient se compléter les uns les autres, à partir de tests de bureau jusqu'à des tests modulaires, une synthèse des temps de réparation probables et enfin des exercices complets. Ce type de programme constitue un risque peu élevé et donne lieu à une véritable amélioration du niveau de conscience général de la population des utilisateurs. Enfin, il convient que l'organisation reste au courant du rôle joué par les systèmes d'information de la santé dans la continuité des soins assurés aux patients. Il convient que ces organisations soient prêtes lorsque les systèmes informatiques ne fonctionnent pas correctement.

A.17.1.2 Mise en œuvre de la continuité de la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'organisation établisse, documente, mette en oeuvre et maintienne à jour des processus, des procédures et des mesures permettant de garantir le niveau requis de	Y	Il convient que l'organisation s'assure: a) qu'il existe une structure de gestion adéquate pour se préparer, atténuer et réagir à un événement perturbant en mobilisant du personnel possédant l'autorité, l'expérience et les compétences nécessaires; b) que les membres du personnel chargés de la réponse à apporter aux incidents, et qui possèdent les responsabilités, l'autorité et les compétences nécessaires pour gérer les incidents et maintenir la sécurité de l'information, sont nommées;	Il convient que les organisations qui traitent des données personnelles relatives à la santé identifient les processus, les systèmes et autres équipements pertinents vitaux pour la prestation des soins. Afin de parer aux dysfonctionnements des processus, systèmes et autres équipements pertinents vitaux pour la

continuité de la sécurité de l'information au cours d'une situation défavorable.		c) qu'il existe des plans documentés, des procédures de réponse et de récupération approuvés, détaillant la manière dont l'organisation gère un événement perturbant et maintient la sécurité de son information à un niveau prédéterminé, reposant sur des objectifs de continuité de la sécurité de l'information approuvés par la direction (voir 17.1.1). Conformément aux exigences de continuité de la sécurité de l'information, il convient que l'organisation établisse, documente, mette en œuvre et tienne à jour: a) des mesures de sécurité de l'information intégrées aux processus de continuité de l'activité ou de récupération après un sinistre, aux procédures et aux outils et systèmes associés; b) des processus, des procédures et des changements à mettre en œuvre pour maintenir les mesures de sécurité de l'information existantes lors d'une situation défavorable; c) des mesures destinées à contrebalancer les mesures de sécurité de l'information qu'il est impossible de maintenir dans une situation défavorable.	prestation des soins, il convient de qualifier les procédures d'urgence de procédures nécessaires.

A.17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que l'organisation vérifie à intervalles réguliers les mesures de continuité de la sécurité de l'information déterminées et mises en œuvre, afin de s'assurer qu'elles restent valables et efficaces dans des situations défavorables.	Y	Les changements organisationnels, techniques, liés aux procédures et aux processus, que ce soit dans le contexte habituel d'exploitation ou dans un contexte de continuité, peuvent entraîner des changements dans les exigences de continuité de la sécurité de l'information. Dans ce cas, il convient de revoir la continuité des processus, des procédures et des mesures de la sécurité de l'information en tenant compte des changements apportés aux exigences. Il convient que les organisations vérifient la continuité de management de la sécurité de l'information: a) en exerçant et en testant les fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de l'information pour s'assurer qu'elles sont cohérentes avec les objectifs de continuité de la sécurité de l'information; b) en exerçant et en testant les connaissances et les tâches de routine pour appliquer les processus, les procédures et les mesures de continuité de la sécurité de l'information afin de s'assurer que leurs performances sont cohérentes avec les objectifs de continuité de la sécurité de l'information; c) en revoyant la validité et l'efficacité des mesures de continuité de la sécurité de l'information lorsque les systèmes d'information, les processus, les procédures et les mesures de sécurité de l'information ou les solutions et les processus de gestion de la continuité de l'activité/gestion de la récupération après sinistre connaissent des changements.	

A.17.2 Redondances

Objectif: Garantir la disponibilité des moyens de traitement de l'information.

A.17.2.1 Disponibilité des moyens de traitement de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en oeuvre des moyens de traitement de l'information	***N***	Il convient que les organisations identifient les exigences de l'activité en matière de disponibilité des systèmes d'information. Lorsqu'il n'est pas possible de garantir la disponibilité en utilisant l'architecture	

avec suffisamment de redondances pour répondre aux exigences de disponibilité.		existante du système, il convient d'envisager des composants ou des architectures redondants. Le cas échéant, il convient de tester les systèmes d'information redondants pour s'assurer que le basculement d'un composant à un autre fonctionne comme prévu.	

A.18 Conformité

A.18.1 Conformité aux obligations légales et réglementaires

Objectif: Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

A.18.1.1 Identification de la législation et des exigences contractuelles applicables

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient, pour chaque système d'information et pour l'organisation elle-même, de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences.	Y	De la même façon, il convient de définir et de documenter les mesures spécifiques et les responsabilités individuelles mises en place pour répondre à ces exigences. Il convient que les responsables identifient toutes les législations applicables à l'organisation afin de répondre aux exigences liées à leur type d'activité. Si l'organisation mène des activités dans d'autres pays, il convient que les responsables étudient la conformité aux règles des pays concernés.	Il convient que les établissements de soins établissent un programme d'audit de conformité qui porte sur l'ensemble du cycle de vie des activités, c'est-à-dire non seulement les processus qui identifient les problèmes, mais aussi ceux qui évaluent les résultats et décident des mises à jour du système de gestion de la sécurité de l'information (SGSI). Il convient que les programmes d'audit des organisations de la santé soient formellement structurés de sorte qu'ils incluent tous les éléments de la présente norme internationale, tous les domaines à risque et toutes les mesures de gestion mises en œuvre dans un cycle de 12 à 18 mois. Dans l'environnement hautement réglementé et contrôlé de nombreux établissements de soins, l'ISMF (forum de gestion de la sécurité de l'information) devrait se fixer pour objectif d'établir un cadre de contrôle de conformité graduel, dont la couche inférieure serait l'auto-vérification par ceux qui mettent en œuvre les processus et les gestionnaires. Par la suite, les audits du SGSI pour les besoins de l'ISMF, les audits internes, les évaluations en vue de garantir les mesures de contrôle et les audits externes doivent être définis de manière à ce que chaque niveau puisse bénéficier de la confiance de tous les niveaux inférieurs.

A.18.1.2 Droits de propriété intellectuelle

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de mettre en œuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles	***N***	Il convient de prendre en compte les directives suivantes en vue de protéger tout matériel pouvant être soumis à des droits de propriété intellectuelle:	

relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires.		a) publier une politique de conformité relative aux droits de propriété intellectuelle définissant l'utilisation légale des logiciels et des produits liés à l'information; b) acquérir des logiciels uniquement à partir de sources connues et réputées afin de s'assurer du respect des droits d'auteur; c) maintenir la sensibilisation aux politiques appliquées en matière de protection des droits de propriété intellectuelle et prévenir le personnel de l'intention de prendre des mesures disciplinaires à l'encontre des personnes enfreignant cette politique; d) tenir à jour des registres des actifs appropriés et identifier tous les actifs soumis à des exigences de protection des droits de propriété intellectuelle; e) conserver les preuves tangibles de la propriété des licences, des disques maîtres, des manuels, etc.; f) mettre en œuvre des contrôles permettant de s'assurer que le nombre maximal d'utilisateurs autorisé par la licence n'est pas dépassé; g) effectuer des revues permettant de s'assurer que seuls des logiciels autorisés et sous licence sont installés; h) mettre en œuvre une politique de gestion des conditions de licence appropriées; i) mettre en œuvre une politique permettant de céder des logiciels ou de les transmettre à des tiers; j) se conformer aux conditions générales régissant les logiciels et l'information obtenus à partir des réseaux publics; k) ne pas reproduire, convertir dans un autre format ou extraire de l'information à partir d'enregistrements du commerce (film, enregistrement audio) en dehors de ce qui est permis par la législation sur les droits d'auteur; l) ne pas copier, intégralement ou en partie, des livres, articles, rapports ou autres documents en dehors de ce qui est permis par la législation sur les droits d'auteur.	

A.18.1.3 Protection des enregistrements

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de protéger les enregistrements de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.	***N***	Au moment de décider de la protection spécifique des enregistrements de l'organisation, il convient de tenir compte de leur classification, proposée par le plan de classification de l'organisation. Il convient de classer les enregistrements par types, tels que documents comptables, enregistrements de base de données, journaux de transactions, journaux d'audit et procédures d'exploitation; chaque type comporte des détails sur les périodes de conservation et le type de support de stockage permis, par exemple papier, microfiche, support magnétique, support optique. Il convient également de stocker les clés cryptographiques qui s'y rapportent et les programmes associés à des archives ou des signatures électroniques chiffrées (voir l'article 10), afin de permettre le déchiffrement des enregistrements pendant leur durée de conservation. Il convient d'envisager l'éventualité d'une dégradation du support utilisé pour le stockage des enregistrements. Il convient de mettre en œuvre les procédures de stockage et de manipulation conformément aux recommandations du fabricant. Si le choix se porte sur des supports de stockage électroniques, il convient d'établir des procédures visant à garantir l'accès aux données (lisibilité du support et du format) tout au	

		long de la période de conservation afin de protéger les données contre toute perte due à l'évolution de la technologie. Il convient de choisir les systèmes de stockage des données de sorte qu'ils permettent la récupération des données requises dans un délai raisonnable et sous un format lisible selon les exigences à respecter. Il convient que le système de stockage et de manipulation garantisse l'identification des enregistrements et de leur durée de conservation telles que définies par la législation nationale ou régionale ou par les réglementations, le cas échéant. Il convient que ce système permette la destruction appropriée des enregistrements à l'issue de cette période si l'organisation n'en a plus besoin. Pour remplir ces objectifs de sauvegarde des enregistrements, il convient que l'organisation suive les étapes suivantes: a) il convient d'établir des directives relatives à la conservation, au stockage, à la manipulation et à l'élimination des enregistrements et de l'information; b) il convient d'établir un programme de conservation identifiant les enregistrements et leur durée de conservation; c) il convient de tenir à jour un inventaire des sources de l'information clé.	

A.18.1.4 Protection de la vie privée et protection des données à caractère personnel

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de garantir la protection de la vie privée et la protection des données à caractère personnel telles que l'exigent la législation et les réglementations applicables, le cas échéant.	Y	Il convient de développer et de mettre en œuvre une politique des données de l'organisation pour assurer la protection de la vie privée et la protection des données à caractère personnel. Il convient de communiquer cette politique à toutes les personnes impliquées dans le traitement des données à caractère personnel. La conformité à cette politique et à toutes les législations et réglementations pertinentes en matière de protection de la vie privée des personnes et de protection des données à caractère personnel exige une structure et des mesures de gestion appropriées. La meilleure façon de mettre en place une telle structure est de désigner un responsable, par exemple un administrateur de la protection de la vie privée. Il convient que cet administrateur conseille les responsables, les utilisateurs et les prestataires de services sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de respecter. Il convient que la responsabilité afférente au traitement des données à caractère personnel et à la sensibilisation aux principes de protection de la vie privée prenne en compte la législation et les réglementations applicables. Il convient de mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel.	Un exemple d'une loi ou d'une réglementation requérant le consentement éclairé des patients est la recommandation R (97)5 du Conseil de l'Europe sur la protection des données médicales, Conseil de l'Europe, Strasbourg, 12 février 1997: Avant de procéder à un test génétique, la personne concernée doit être informée de l'objectif du test et de la possibilité de découvertes inattendues. Il convient d'informer la personne soumise à un test génétique sur les découvertes inattendues si les conditions suivantes sont remplies: a. ce type d'informations n'est pas interdit en vertu du droit interne; b. la personne concernée a explicitement demandé les informations; c. les informations ne causeront pas de dommages majeurs: i. à la santé de la personne concernée; ou ii. à un parent par le sang de la personne concernée du côté du père ou de la mère, à une personne de son entourage immédiat ou à une personne directement liée à la même lignée génétique que la personne concernée. Un exemple d'une directive professionnelle éthique requérant le consentement du patient est la Déclaration

			d'Helsinki de l'Organisation mondiale de la santé relative aux recherches médicales sur les êtres humains. Davantage d'informations sur la gestion du consentement éclairé dans le secteur des soins de santé sont disponibles dans la norme ISO/TS 17975.

A.18.1.5 Réglementation relative aux mesures cryptographiques

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.	***N***	En vue de se conformer aux accords, lois et réglementations applicables, il convient de prendre en compte les éléments suivants: a) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels destinés à l'exécution de fonctions cryptographiques; b) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels intégrant des fonctions cryptographiques; c) les restrictions en matière d'utilisation du chiffrement; d) les méthodes non discrétionnaires ou non dont disposent les autorités nationales pour accéder aux informations chiffrées par des moyens matériels ou logiciels dans le but de préserver la confidentialité du contenu. Il convient de demander un avis juridique afin de s'assurer de la conformité aux lois et réglementations nationales. Il convient également de solliciter un avis juridique avant de transmettre de l'information chiffrée ou des mesures cryptographiques au-delà des limites juridictionnelles.	

A.18.2 Revue de la sécurité de l'information

Objectif: Garantir que la sécurité de l'information est mise en oeuvre et appliquée conformément aux politiques et procédures organisationnelles.

A.18.2.1 Revue indépendante de la sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) à intervalles définis ou lorsque des changements importants sont intervenus.	***N***	Il convient que la direction instaure une revue indépendante. Des revues indépendantes sont nécessaires pour veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche de l'organisation en matière de management de la sécurité de l'information. Il convient que la revue permette d'analyser les opportunités d'amélioration et les changements éventuels à apporter à l'approche adoptée en matière de sécurité, en particulier à la politique et aux objectifs. Il convient qu'une telle revue soit réalisée par des personnes indépendantes du domaine concerné, par exemple par des intervenants de la fonction d'audit interne, par un responsable indépendant ou une organisation tiers spécialisée dans de telles revues. Il convient que les personnes chargées de ces revues possèdent les compétences et l'expérience nécessaires. Il convient d'enregistrer et de communiquer les résultats de la revue indépendante à la direction à l'origine de la demande. Il convient de conserver ces enregistrements. Si la revue indépendante détermine que l'approche de l'organisation et sa mise en œuvre du management de la sécurité de l'information sont inadaptés, à savoir que les objectifs et les exigences documentés ne sont pas respectés ou ne sont pas conformes aux directives	

		énoncées dans les politiques de sécurité de l'information (voir 5.1.1), il convient que la direction envisage des actions correctives.	

A.18.2.2 Conformité avec les politiques et les normes de sécurité

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les responsables revoient régulièrement la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.	Y	Il convient que les responsables déterminent la manière de vérifier que les exigences de sécurité de l'information définies dans les politiques, les normes et autres règlementations applicables, sont respectées. Il convient d'envisager l'utilisation d'outils de mesure et d'enregistrement automatisés pour procéder à des revues régulières efficaces. Si la revue détecte une non-conformité, il convient que les responsables: a) déterminent les causes de la non-conformité; b) évaluent la nécessité d'engager des actions pour établir la conformité; c) mettent en œuvre l'action corrective appropriée; d) revoient l'action corrective entreprise pour vérifier son efficacité et identifier toute insuffisance ou faille. Il convient que les résultats des revues et des actions correctives réalisées par les responsables soient enregistrés et que ces enregistrements soient tenus à jour. Il convient que ces résultats soient communiqués aux personnes réalisant des revues indépendantes (voir 18.2.1) par le responsable concerné lorsqu'une revue indépendante est menée dans son domaine de responsabilité.	

A.18.2.3 Examen de la conformité technique

Mesure de gestion (ISO 27001)	SOA	Directive de mise en œuvre	Directive de mise en œuvre spécifique aux soins
Il convient que les systèmes d'information soient régulièrement revus pour vérifier leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.	Y	Il convient que la revue de conformité technique soit réalisée de préférence à l'aide d'outils automatiques, générant des rapports techniques à soumettre à l'interprétation d'un spécialiste. Il est également possible de faire procéder à une revue manuelle (avec l'appui, si nécessaire d'outils logiciels appropriés) par un ingénieur systèmes expérimenté. Lors de tests d'intrusion ou d'appréciations des vulnérabilités, il convient de procéder avec la plus grande prudence, car de telles activités peuvent compromettre la sécurité du système. Il convient de planifier et de documenter ces tests qui doivent pouvoir être répétés. Il convient que toute revue de conformité technique soit effectuée par des personnes compétentes, autorisées ou sous la supervision de telles personnes.	Il y a lieu d'accorder une attention particulière au respect de l'interopérabilité technique, étant donné que les systèmes d'information de la santé de grande envergure se composent généralement d'un grand nombre de systèmes qui collaborent entre eux.