A.5 Politique de sécurité de l'information

A.5.1 Orientations 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:	Explications complémentaires
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 salariés et aux tiers concernés	Y	Tout hôpital est tenu de disposer d'une politique publiée et actualisée sur la sécurité de l'information qui a été approuvée par le responsable de la gestion journalière (ou assimilé). Tous les éléments de cette politique dont le collaborateur a besoin pour exécuter correctement ses tâches, doivent être communiqués à l'ensemble des collaborateurs, en ce compris aux collaborateurs occasionnels et aux utilisateurs externes qui utilisent les informations qui sont disponibles dans les systèmes de l'hôpital.

A.5.1.2 Revue des politiques de sécurité de l'information

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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 y a lieu de faire régulièrement rapport à la gestion journalière (ou assimilée) concernant la situation en matière de sécurité de l'information et de protection des données à caractère personnel afin de valider l'applicabilité, l'exhaustivité, l'adéquation et l'effectivité de la sécurité de l'information et de la protection des données à caractère personnel. Les dérogations, problèmes ou incidents constatés feront l'objet d'un suivi en temps utile par des actions/sanctions appropriées en adéquation avec les procédures internes de l'organisation. Les incidents ou infractions majeurs impliquant des données à caractère personnel sont signalés aux instances compétentes.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information	Y	Tout hôpital est tenu de: • organiser un service de sécurité de l'information qui est dirigé par un conseiller en sécurité de l'information ou DPO. • disposer d'un plan de sécurité de l'information qui a été approuvé par le responsable de la gestion journalière de l'hôpital concerné (ou équivalent). • disposer des crédits de fonctionnement nécessaires qui ont été approuvés par le responsable de la gestion journalière de l'hôpital concerné (ou assimilé), afin de pouvoir exécuter le plan de sécurité de l'information et de permettre au service de sécurité de l'information d'exécuter les tâches lui attribuées. • faire participer le conseiller en sécurité de l'information ou DPO aux travaux de l'hôpital au moyen de la mise à la disposition de données et d'une concertation régulière entre les différentes parties concernées.

A.6.1.2 Séparation des tâches

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

A.6.1.3 Relations avec les autorités

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'entretenir des relations appropriées avec les autorités compétentes.	N	Aucun objectif spécifique n'est défini. Cet élément est soutenu au niveau central.

A.6.1.4 Relations avec des groupes de travail spécialisés

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'entretenir des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles.	N	Aucun objectif spécifique n'est défini. Cet élément est soutenu au niveau central.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de traiter la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.	Y	Tout hôpital est tenu de: • pour tout processus et pour tout projet, réaliser une évaluation des risques au niveau de la sécurité de l'information et de la protection des données à caractère personnel, la valider, la communiquer et l'actualiser • au niveau du responsable du traitement, examiner toutes les évaluations de risques à risque résiduel majeur et le cas échéant, conformément au RGPD, consulter l'autorité de contrôle, préalablement au traitement.

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	Explications complémentaires
Il convient d'adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles.	Y	Tout hôpital est tenu de: • prendre les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles ne soient accessibles qu'aux seules personnes autorisées. • prendre les mesures adéquates, en fonction du moyen d'accès, afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'hôpital aux données sensibles, confidentielles et professionnelles de l'organisation. • imposer le respect des conditions qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils privés à des fins professionnelles. • imposer le respect des règles qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils mobiles à des fins professionnelles et à des fins privées. • clairement identifier les appareils mobiles propres, doit les configurer en toute sécurité (et les équiper des logiciels antimalware nécessaires ainsi que des logiciels permettant la suppression à distance de l'ensemble des données sur l'appareil) et doit conserver leur identification dans un registre central. • régulièrement sensibiliser les utilisateurs concernant les bonnes pratiques d'utilisation et leurs responsabilités (en particulier en ce qui concerne la connexion à des réseaux sans fil publics). • s'engager à respecter la protection des données à caractère personnel de l'utilisateur.

A.6.2.2 Télétravail

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de mettre en œuvre une politique et des mesures de sécurité complémentaires pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail	Y	Tout hôpital est tenu de: • prendre les mesures adéquates, en fonction du moyen d'accès, afin de garantir la sécurité de l'accès réalisé en dehors de l'hôpital aux données sensibles, confidentielles et professionnelles de l'hôpital. • clairement définir des règles de bonne conduite ainsi qu'une mise en œuvre appropriée de l'accès à distance, doit les valider, les communiquer et les tenir à jour, et doit aussi préciser quels systèmes peuvent et quels systèmes ne peuvent pas être consultés à distance ou en ayant recours à d'autres appareils. • prendre les mesures appropriées pour autoriser les appareils n'appartenant pas à l'hôpital à accéder aux informations si cela s'avère nécessaire.

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	Explications complémentaires
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	

A.7.1.2 Termes et conditions d'embauche

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est préalablement à l'entrée en service tenu de: • attirer l'attention du collaborateur futur sur le règlement de travail ou le règlement de service définissant ses responsabilités et celles de l'hôpital en ce qui concerne la sécurité de l'information et la protection de données à caractère personnel. • conclure des accords contractuels avec le fournisseur qui fournit des collaborateurs entrant en contact avec des données à caractère personnel de l'hôpital, par lesquels ce dernier garantit que ces collaborateurs respecteront les règles relatives à la sécurité de l'information et à la protection des données à caractère personnel en vigueur à l'hôpital.

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	Explications complémentaires

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	

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	• La direction est tenue d'exiger de tous les collaborateurs qu'ils appliquent la sécurité de l'information et la protection des données à caractère personnel conformément aux règles relatives à la sécurité de l'information de l'hôpital • Tous les collaborateurs de l'hôpital doivent recevoir une formation appropriée et suivre régulièrement des cours de formation continue concernant les normes minimales et les procédures de l'organisation, pour autant que cela soit pertinent pour leur rôle ou fonction. • Toute organisation doit offrir au moins une fois par an une campagne de sensibilisation ou une session d'information relative à la sécurité de l'information et à la protection des données à caractère personnel.

A.7.2.3 Processus disciplinaire

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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	Explications complémentaires
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 informer le salarié ou le contractant et de veiller à leur application.	Y	

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	Explications complémentaires
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	Les appareils qui appartiennent à l'hôpital ou qui sont gérés par lui et sur lesquels des données à caractère personnel sont traitées, doivent être repris dans un inventaire.

A.8.1.2 Propriété des actifs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les actifs figurant à l'inventaire aient un propriétaire.	Y	

A.8.1.3 Utilisation correcte des actifs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	L'hôpital doit élaborer une directive indiquant que l'utilisateur demeure responsable de la protection des informations en sa possession, quelle que soit la forme sous laquelle ces informations sont enregistrées. L'utilisateur doit donc veiller à la bonne protection de celles-ci en respectant les règles élaborées par l'hôpital, en ce compris la destruction des données lorsque ceci s'avère nécessaire et est autorisé.

A.8.1.4 Restitution des actifs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tous les collaborateurs sont tenus, après la cessation de leur contrat de travail, de rendre tous les informations de santé personnelles sous format non électronique en leur possession et de veiller à ce que toutes les informations de santé personnelles sous format électronique en leur possession soient mises à jour sur les systèmes pertinents et soient ensuite effacées de manière sécurisée sur tous les appareils sur lesquels elles étaient présentes.

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	Explications complémentaires
Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité ou de leur caractère critique pour l'entreprise.	Y	Tout hôpital est tenu de disposer d'une directive relative au schéma de classification. La classification tient compte de la distinction entre des données à caractère personnel et des données à caractère non personnel. La classification des données doit régulièrement être contrôlée en collaboration avec le DPO.

A.8.2.2 Marquage des informations

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de prendre les mesures nécessaires pour clairement informer les utilisateurs des informations sur la classification des données. Ceci peut se faire en labélisant les supports physiques des informations, en mentionnant la classification dans les applications ou au moyen de sessions de sensibilisation organisées par l'hôpital.

A.8.2.3 Manipulation des actifs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'élaborer et de mettre en oeuvre des procédures de traitement des actifs, conformément au plan de classification de l'information adopté par l'organisation.	Y	

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	Explications complémentaires

Il convient de mettre en oeuvre des procédures de gestion des supports amovibles conformément au plan de classification adopté par l'organisation.	Y	Tout hôpital est tenu de prendre les mesures nécessaires afin • d'éviter que les informations conservées sur les médias physiques ne soient divulguées, modifiées, supprimées ou détruites sans autorisation. • de protéger les médias physiques pendant leur transport contre un accès non autorisé. • de détruire en toute sécurité les médias physiques, en ce compris les médias mobiles, lorsque ceux-ci ne sont plus utilisés.

A.8.3.2 Mise au rebut des supports

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de procéder à une mise au rebut sécurisée des supports qui ne servent plus, en suivant des procédures formelles.	Y	

A.8.3.3 Transfert physique des supports

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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	Explications complémentaires
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	

A.9.1.2 Accès aux réseaux et aux services en réseau

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les utilisateurs aient uniquement accès au réseau et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation.	Y	Tout hôpital est tenu de limiter l'accès aux données et aux systèmes d'information au moyen de procédures formelles d'octroi et de retrait de droits d'accès aux systèmes et services d'informations et par la limitation des droits à ce qui est strictement nécessaire pour le prestataire de soins dans le cadre de l'exécution de sa mission. Si le traitement électronique de catégories spécifiques de données à caractère personnel visées à l'article 9, 1., du Règlement général sur la protection des données (RGPD) requiert la vérification de caractéristiques ou relations pertinentes, ces caractéristiques ou relations sont consultées • soit dans les sources authentiques concernées déterminées par le Comité de gestion de la Plate-forme eHealth • soit dans une banque de données de l'organisation ou d'un réseau de santé dont l'organisation fait partie et qui est, là où nécessaire, synchronisée avec les informations de qualité contenues dans les sources authentiques définies par le Comité de gestion de la Plate-forme eHealth.

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	Explications complémentaires
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	

A.9.2.2 Maîtrise de la gestion des accès utilisateur

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

A.9.2.3 Gestion des privilèges d'accès

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges d'accès.	Y	Tout hôpital est tenu de limiter l'octroi de droits d'accès privilégiés aux gestionnaires d'information à ce qui est strictement nécessaire pour la gestion des informations et des systèmes qui leur ont été confiés. L'hôpital attirera l'attention du gestionnaire d'information sur le fait qu'un accès supplémentaire entraîne aussi des responsabilités supplémentaires. L'hôpital contrôle l'utilisation de ces accès privilégiés.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires

Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.	Y	L'organisation authentifie l'identité de la personne physique qui traite les catégories spécifiques de données à caractère personnel (« l'utilisateur ») visées à l'article 9, 1, du Règlement général sur la protection des données (RGPD).
		Cette authentification intervient soit
		• par un moyen intégré dans le Federal Authentication Service (FAS) d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth;
		• par un système d'authentification propre à l'organisation
		  ○ à condition que l'enregistrement de l'identité soit effectué au moyen d'un usage unique d'un moyen d'authentification intégré dans le FAS d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth et
		  ○ à condition que le système d'authentification du prestataire satisfasse aux conditions d'un niveau de garantie « substantiel », telles que précisées aux points 2.1., 2.2.1., élément 2, 2.2.3., 2.2.4., 2.3.1. (à l'exception de l'élément 1) et 2.4. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS
		  ○ à condition que le moyen d'authentification utilisé dans le système d'authentification propre au prestataire et son processus d'activation satisfassent aux conditions d'un niveau de garantie « faible » précisées au point 2.2.1, élément 1, et au point 2.2.2. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et qu'il ait été conçu de

		la sorte que l'on suppose qu'il sera uniquement utilisé par la personne à laquelle il a appartient. Le niveau minimal dans le FAS fixé par le Comité de gestion de la Plate-forme eHealth est le niveau est 400.

A.9.2.5 Revue des droits d'accès utilisateurs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers.	Y	

A.9.2.6 Suppression ou adaptation des droits d'accès

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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	Explications complémentaires
Il convient d'exiger des utilisateurs des informations secrètes d'authentification qu'ils appliquent les pratiques de l'organisation en la matière.	Y	Tout hôpital doit veiller à ce que l'utilisateur prenne suffisamment de mesures pour protéger ses informations d'authentification (nom d'utilisateur et mot de passe).

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	Explications complémentaires
Il convient de restreindre l'accès à l'information et aux fonctions d'application système conformément à la politique de contrôle d'accès.	Y	

A.9.4.2 Sécuriser les procédures de connexion

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	L'organisation authentifie l'identité de la personne physique qui traite les catégories spécifiques de données à caractère personnel (« l'utilisateur ») visées à l'article 9, 1, du Règlement général sur la protection des données (RGPD). Cette authentification intervient soit • par un moyen intégré dans le Federal Authentication Service (FAS) d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth; • par un système d'authentification propre à l'organisation ○ à condition que l'enregistrement de l'identité soit effectué au moyen d'un usage unique d'un moyen d'authentification intégré dans le FAS d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth et

		○ à condition que le système d'authentification du prestataire satisfasse aux conditions d'un niveau de garantie « substantiel », telles que précisées aux points 2.1., 2.2.1., élément 2, 2.2.3., 2.2.4., 2.3.1. (à l'exception de l'élément 1) et 2.4. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS ○ [3]. Le niveau minimal dans le FAS fixé par le Comité de gestion de la Plate-forme eHealth est le niveau 400.

A.9.4.3 Système de gestion des mots de passe

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.	Y	Tout hôpital doit veiller à ce que l'utilisateur prenne suffisamment de mesures pour protéger ses informations d'authentification (nom d'utilisateur et mot de passe). Le système assurant l'authentification doit, en fonction du risque et des possibilités techniques, prévoir une ou plusieurs mesures suivantes: • prévoir des moyens techniques pour une authentification multifacteur • imposer l'utilisation d'identifiants et de mots de passe individuels à des fins de responsabilisation; • autoriser les utilisateurs à sélectionner et à modifier leurs propres mots de passe et à prévoir une procédure de confirmation • maintenir un choix de mots de passe de qualité • obliger les utilisateurs à modifier leur mot de passe lors de la première connexion; • imposer des modifications de mots de passe réguliers et lorsque nécessaire; • tenir un registre des mots de passe déjà utilisés et prévenir une réutilisation; Pour l'utilisation de systèmes de mots de passe, il y a lieu de respecter les mesures suivantes: • ne pas afficher les mots de passe à l'écran au moment de leur introduction; • conserver les fichiers de mots de passe dans un endroit séparé des données système de l'application; conserver et envoyer les mots de passe sous forme sécurisée.

A.9.4.4 Utilisation de programmes utilitaires à privilèges

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de restreindre l'accès au code source des programmes.	N	

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	Explications complémentaires
Il convient d'élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.	N	Ces mesures sont déjà reprises comme contrôle possible pour la protection des informations.

A.10.1.2 Gestion des clés

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital prévoit des mesures pour la protection des clés de chiffrement. Ces mesures ont trait à la gestion des certificats du côté des utilisateurs et les clés doivent être protégées contre tout usage non autorisé et la distribution non souhaitée.

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	Explications complémentaires
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	

A.11.1.2 Contrôles physiques des accès

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de prévoir des contrôles d'accès afin de protéger les espaces contenant des données critiques ou sensibles ainsi que le matériel informatique, de sorte que seul le personnel compétent y ait accès.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de concevoir et d'appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements.	Y	Voir A.11.1.2

A.11.1.4 Protection contre les menaces extérieures et environnementales

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de concevoir et d'appliquer des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents.	Y	Tout hôpital est tenu de réaliser une protection physique contre les dégâts causés par un incendie, une inondation, une intrusion et toute autre forme de calamités physiques ou humaines ainsi que contre les dégâts occasionnés par une attaque ciblée.

A.11.1.5 Travail dans les zones sécurisées

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de concevoir et d'appliquer des procédures pour le travail en zone sécurisée.	N	N'est pas repris comme point spécifique mais tombe sous: Tout hôpital est tenu de prévoir des contrôles d'accès afin de protéger les espaces contenant des données critiques ou sensibles ainsi que le matériel informatique, de sorte que seul le personnel compétent y ait accès.

A.11.1.6 Zones de livraison et de chargement

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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 traitement de l'information, de façon à éviter les accès non autorisés.	Y	Tout hôpital est tenu de prévoir des contrôles d'accès afin de protéger les espaces contenant des données critiques ou sensibles ainsi que le matériel informatique, de sorte que seul le personnel compétent y ait accès.

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	Explications complémentaires
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	Les appareils destinés au traitement d'informations personnelles ou qui assurent un rôle critique dans la prestation de service d'un hôpital doivent être placés et protégés de la sorte à réduire les menaces et dangers provenant de l'extérieur ainsi que le risque d'accès par des personnes non autorisées.

A.11.2.2 Services généraux

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.	Y	

A.11.2.3 Sécurité du câblage

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Cette matière est déjà traitée dans la protection réseau.

A.11.2.4 Maintenance du matériel

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité.	N	Constitue déjà un élément de la disponibilité

A.11.2.5 Sortie des actifs

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires

Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisation sans autorisation préalable.	N	Cette mesure ne s'applique pas aux hôpitaux où les médecins emporteront régulièrement des informations et des appareils. Des mesures supplémentaires de protection des informations, en ce compris le transport des informations, sont déjà comprises dans le chapitre concerné Transport des informations

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.	N	Couvert par la gestion par une tierce partie en ce qui concerne la gestion d'informations off-site et pendant le télétravail

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de prendre les mesures utiles pour que l'ensemble des données soient supprimées ou rendues inaccessibles sur les médias avant leur mise au rebut ou leur réutilisation. À cet égard, il y a également lieu d'accorder l'attention utile aux appareils sur lesquels le stockage d'informations ne constitue pas la fonction primaire (telles que les photocopieuses) Il en va de même pour les supports d'information qui ne sont pas la propriété de l'hôpital. Ceci sera fixé dans un contrat avec le(s) fournisseur(s).

A.11.2.8 Matériel utilisateur laissé sans surveillance

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les utilisateurs s'assurent que le matériel non surveillé est doté d'une protection appropriée.	Y	Tout hôpital est tenu de prendre les mesures nécessaires afin • d'éviter que les informations conservées sur les médias physiques ne soient divulguées, modifiées, supprimées ou détruites sans autorisation. • de protéger les médias physiques pendant leur transport contre un accès non autorisé.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de prendre les mesures nécessaires afin • d'éviter que les informations conservées sur les médias physiques et numérique soient accessible pour des personnes non autorisées

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	Explications complémentaires
Il convient de documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés.	Y	Tout hôpital est tenu d'au moins prévoir la documentation relative au backup, au démarrage et à la réparation de systèmes, à la gestion de logs et au monitoring d'activités.

A.12.1.2 Gestion des changements

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de: • disposer de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes • éviter qu'une seule et même personne n'assure le contrôle complet de ce processus.

A.12.1.3 Dimensionnement

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Vu l'éventail des différents appareils utilisés, il s'agit d'un point opérationnel plutôt que d'un contrôle de sécurité.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Le cas échéant, l'hôpital est tenu de prendre les mesures appropriées de sorte que • l'environnement de production soit séparé et distinct des autres environnements tels les environnements de développement, d'acceptation, de test, … • veiller à ce que tout développement ou test soit exclu au sein de l'environnement de production. Dans certains cas exceptionnels, il est possible de déroger à cette règle moyennant la mise en place de mesures adéquates. • doit veiller à ce que les informations présentes sur chacun des systèmes soient traitées conformément à l'ensemble des réglementations. Ainsi, les plateformes de test, de développement et d'acceptation prévoiront l'encadrement utile de sorte que les informations soient traitées conformément au RGPD et aux autres règlements.

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	Explications complémentaires
Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération, conjuguées à une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants.	Y	Toute hôpital est tenu de disposer de systèmes actualisés de protection (prévention, détection et rétablissement) contre des codes nocifs. Par ailleurs, des procédures adéquates doivent être instaurées afin de renforcer la prise de conscience des utilisateurs.

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	Explications complémentaires
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	Afin d'éviter la perte irréparable de données, tout hôpital convient de: • prendre des copies de sauvegarde des informations et des programmes. • contrôler régulièrement les copies de sauvegarde prises quant à leur exhaustivité et exploitabilité

		• protéger les copies de sauvegarde prises contre un accès non autorisé et contre leur destruction.

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	Explications complémentaires
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	Tout hôpital est tenu d'enregistrer les activités réalisées par les utilisateurs sur les données à caractère personnel et de déterminer les exceptions et les événements dans des fichiers journaux (logs). Ces fichiers journaux doivent être conservés pendant une période convenue (communiquée aux parties concernées) pour les besoins d'une étude et d'un contrôle d'accès futurs, compte tenu des réglementations relatives à la protection de données à caractère personnel. La conservation de logs permet notamment de répondre aux fonctions suivantes: • permettre de déterminer rapidement et de manière aisée quelle personne physique a eu accès à quelles données à caractère personnel relatives à quelle personne, à quel moment et de quelle manière; • pouvoir identifier de manière univoque la personne qui a traité des données à caractère personnel et la personne concernant laquelle les données à caractère personnel ont été traitées; • mettre les outils nécessaires à la disposition afin de permettre une exploitation des logs par des personnes autorisées.

A.12.4.2 Protection de l'information journalisée

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de protéger les moyens de journalisation et l'information journalisée contre les risques de falsification ou d'accès non autorisé.	Y	

A.12.4.3 Journaux administrateur et opérateur

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

A.12.4.4 Synchronisation des horloges

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de synchroniser les horloges de ses différents systèmes informatiques en fonction d'une source temporelle de référence. Cette synchronisation est nécessaire pour relier entre eux les événements sur différents systèmes et pour des raisons d'horodatage de certaines actions.

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	Explications complémentaires
Il convient de mettre en œuvre des procédures pour contrôler l'installation de logiciels sur des systèmes en exploitation.	Y	Tout hôpital est tenu de: • disposer de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes

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	Explications complémentaires
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 mesures appropriées pour traiter le risque associé.	Y	Tout hôpital est tenu de recueillir, en temps utile, des informations sur les vulnérabilités techniques des systèmes d'information utilisés ou de se faire informer par le fournisseur. Il y a lieu d'évaluer la mesure dans laquelle l'hôpital est exposé à ce type de vulnérabilités et il y a lieu de prendre les mesures appropriées pour faire face aux risques y liés.

A.12.6.2 Restrictions liées à l'installation de logiciels

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient d'établir et de mettre en oeuvre des règles régissant l'installation de logiciels par les utilisateurs.	Y	Ce qui suit s'applique aux appareils en gestion propre: Tout hôpital est tenu de: • disposer de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes

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	Explications complémentaires
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	

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	Explications complémentaires

Il convient de gérer et de contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications.	Y	Tout hôpital est tenu de vérifier que l'ensemble des réseaux (y compris ceux sans fil) sont gérés et contrôlés de sorte qu'ils soient protégés contre les menaces. Par ailleurs, il doit garantir, de manière adéquate, la protection des systèmes et applications utilisant le réseau. Si le réseau ne permet pas d'offrir les garanties de protection utiles, il y a lieu d'envisager d'autres techniques telles que le chiffrement.

A.13.1.2 Sécurité des services de réseau

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	• Tout hôpital est tenu de vérifier que l'ensemble des réseaux (y compris ceux sans fil) sont gérés et contrôlés de sorte qu'ils soient protégés contre les menaces. Par ailleurs, il doit garantir, de manière adéquate, la protection des systèmes et applications utilisant le réseau. • Tout hôpital est tenu de mettre en place les mesures techniques utiles afin de garantir le plus haut niveau de disponibilité de ses services et connexions externes. Ceci est nécessaire pour assurer une accessibilité maximale des données de santé rendues disponibles et consultées.

A.13.1.3 Cloisonnement des réseaux

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés sur les réseaux.	N	Est couvert par la minimalisation des accès aux applications et Tout hôpital est tenu de vérifier que l'ensemble des réseaux (y compris ceux sans fil) sont gérés et contrôlés de sorte qu'ils soient protégés contre les menaces. Par ailleurs, il doit garantir, de manière adéquate, la protection des systèmes et applications utilisant le réseau.

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	Explications complémentaires
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	Tout hôpital est tenu de prendre les mesures nécessaires afin • de protéger les médias physiques pendant leur transport contre un accès non autorisé. • Le transport d'informations à travers des réseaux doit être protégé de manière adéquate et suffisante.

A.13.2.2 Accords en matière de transfert d'information

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que les accords traitent du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.	N	Ce contrôle traite de contrats mais il doit s'agir d'une mesure technique. Par ailleurs, des contrats ne sont pas toujours conclus pour transporter des données.

A.13.2.3 Messagerie électronique

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de protéger de manière appropriée l'information transitant par la messagerie électronique.	Y	Les aspects liés à la sécurité de l'information pour les messages électroniques doivent comprendre ce qui suit:

		• protéger les messages contre l'accès ou la modification non autorisé ou l'attaque de service (*denial of service*) proportionnelle en fonction du schéma de classification défini par l'organisation; • veiller à un adressage et un transport corrects du message;

A.13.2.4 Engagements de confidentialité ou de non-divulgation

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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	Explications complémentaires
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	Toute organisation est tenue de mettre au point une communication efficace et constructive entre les différentes parties concernées par le projet (en ce compris avec les clients et les fournisseurs), en particulier avec le conseiller en sécurité de l'information ou DPO. Ceci doit offrir un niveau de sécurité de l'information et de protection des données à caractère personnel adéquat connu de tous et est nécessaire à l'application du Data Protection by Design

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de protéger l'information liée aux services d'application transmise sur les réseaux publics contre les activités frauduleuses, les différends contractuels, ainsi que la divulgation et la modification non autorisées.	N	Déjà repris dans la protection réseau.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	

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	Explications complémentaires
Il convient d'établir des règles de développement des logiciels et des systèmes, et de les appliquer aux développements de l'organisation.	Y	Si d'application, l'organisation doit appliquer le « secure project lifecycle » tel que décrit dans la politique « Achat, conception, développement et maintenance d'applications ».

A.14.2.2 Procédures de contrôle des changements apportés au système

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de contrôler les changements apportés au système dans le cycle de développement en utilisant des procédures formelles de contrôle des changements.	N	Déjà repris au point 12.5.1

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Bien qu'il soit fortement recommandé de réaliser ces tests, il n'est dans la réalité pas toujours possible de les faire avoir lieu. Le responsable doit toutefois prendre les mesures utiles afin de tester au maximum l'intégrité des informations et leur traitement, avant qu'une application critique ne puisse être mise en service après une mise à jour.

A.14.2.4 Restrictions relatives aux changements apportés aux progiciels

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Déjà repris au point 12.5.1

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Toute organisation est tenue de mettre au point une communication efficace et constructive entre les différentes parties concernées par le projet (en ce compris avec les clients et les fournisseurs), en particulier avec le conseiller en sécurité de l'information ou DPO. Ceci doit offrir un niveau de sécurité de l'information et de protection des données à caractère personnel adéquat connu de tous et est nécessaire à l'application du Data Protection by Design

A.14.2.6 Environnement de développement sécurisé

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Si d'application, l'hôpital est tenu de: • prendre les mesures adéquates pour que l'environnement de production soit séparé et distinct des autres environnements tels les environnements de développement, de test, d'acceptation, de préproduction, … • veiller à ce que tout développement ou test soit exclu au sein de l'environnement de production. Dans certains cas exceptionnels, il est possible de déroger à cette règle moyennant la mise en place de mesures adéquates.

A.14.2.7 Développement externalisé

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que l'organisation supervise et contrôle l'activité de développement du système externalisé.	Y	Voir 14.2.1. Lors de la mise à la disposition de données pour la partie qui développe, les parties doivent conclure un contrat de sous-traitance.

A.14.2.8 Phase de test de la sécurité du système

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires

Il convient de réaliser les tests de fonctionnalité de la sécurité pendant le développement.	Y	Si d'application, l'hôpital est tenu d'y veiller.

A.14.2.9 Test de conformité du système

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Toute organisation est tenue de s'assurer par l'entremise du responsable du suivi, le chef de projet, et lors de la mise en production du projet, que les conditions relatives à la sécurité de l'information et à la protection des données à caractère personnel qui ont été fixées au début du projet sont effectivement mises en œuvre.

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	Explications complémentaires
Il convient que les données de test soient sélectionnées avec soin, protégées et contrôlées.	Y	Tout hôpital est tenu de veiller à ce que les informations présentes sur chacun des systèmes soient traitées conformément à l'ensemble de la réglementation. Ainsi, les plateformes de test, de développement et d'acceptation prévoiront l'encadrement utile de sorte que les informations soient traitées conformément au RGPD et aux autres règlements. Cela signifie notamment qu'aucune donnée à caractère personnel ne peut être utilisée dans des environnements autres que les environnements de production.

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	Explications complémentaires
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	En cas de sous-traitance à des tiers (en ce compris les solutions de cloud computing), tout hôpital est tenu de s'assurer que: • les obligations en matière de traitement de données à caractère personnel sont fixées dans un contrat. • les conditions relatives à la sécurité de l'information et à la protection des données à caractère personnel font l'objet d'un accord avec les tiers et sont documentées afin de réduire les risques relatifs à l'accès des tiers aux moyens d'information • les « directives relatives à la sécurité de la sous-traitance à des tiers » telles que décrites dans la politique « sécurité de la sous-traitance à des tiers » sont respectées. • Un contrat de sous-traitance est conclu avec le fournisseur selon les dispositions du RGPD. • Il est fixé dans un contrat ce qu'il faut faire avec les données lorsque la collaboration prend fin.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires

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	En cas de sous-traitance à des tiers (en ce compris les solutions de cloud computing), tout hôpital est tenu de s'assurer que: • toutes les conditions pertinentes relatives à la sécurité de l'information et à la protection des données à caractère personnel font l'objet d'un accord avec chacun de ces tiers qui lisent, traitent, enregistrent, communiquent les informations de l'hôpital ou fournissent des éléments d'infrastructure TIC • les contrats conclus avec les tiers comprennent toutes les conditions permettant de traiter les risques liés à la sécurité de l'information et à la protection des données à caractère personnel qui sont afférents aux services TIC • Un contrat de sous-traitance est conclu avec le fournisseur selon les dispositions du RGPD.

A.15.1.3 Chaine d'approvisionnement informatique

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Voir 15.1.2

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	Explications complémentaires
Il convient que les organisations surveillent, revoient et auditent à intervalles réguliers la prestation des services assurés par les fournisseurs.	Y	En cas de sous-traitance à des tiers (en ce compris les solutions de cloud computing), tout hôpital est tenu de s'assurer que la prestation de services par des tierces parties fait l'objet d'un monitoring, d'une évaluation et d'un audit réguliers.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	En cas de sous-traitance à des tiers (en ce compris les solutions de cloud computing), tout hôpital est tenu de s'assurer que les modifications dans la prestation de service par des tiers sont gérées, notamment par la tenue à jour et l'amélioration des lignes directrices, procédures et mesures existantes relatives à la sécurité de l'information et à la protection des données à caractère personnel. Lors de la gestion, il y a lieu de tenir compte du caractère critique des systèmes et processus en question et de la réévaluation des risques.

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	Explications complémentaires
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	Tout hôpital doit disposer de procédures pour la détermination et la gestion d'incidents relatifs à la sécurité de l'information ou à la protection des données à caractère personnel et des responsabilités y afférentes. Ces procédures doivent être connues par tous les collaborateurs qui sont concernés par le traitement des incidents en matière de sécurité de l'information

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées.	Y	Toute organisation est tenue de : • fixer dans un règlement de travail ou un règlement de service que tout collaborateur (fixe ou temporaire, interne ou externe) est obligé de signaler tout accès, utilisation, modification, publication, perte ou destruction non autorisé d'informations et de systèmes d'information. • prévoir que les collaborateurs doivent communiquer les événements et failles relatifs à la sécurité de l'information ou à la protection des données à caractère personnel en lien avec les informations et les systèmes d'information, de sorte que l'hôpital puisse prendre, en temps utile, des mesures correctrices adéquates. • prévoir que les collaborateurs rapportent les incidents relatifs à la sécurité de l'information et à la protection des données à caractère personnel, dans les meilleurs délais, à l'intervention du supérieur hiérarchique, du helpdesk, du conseiller en sécurité de l'information ou du délégué à la protection des données (DPO).

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	L'hôpital développe la police qui prévoit que les collaborateurs doivent communiquer les événements et failles relatifs à la sécurité de l'information ou à la protection des données à caractère personnel en lien avec les informations et les systèmes d'information, de sorte que l'hôpital puisse prendre, en temps utile, des mesures correctrices adéquates

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de: • évaluer tout incident relatif à la sécurité de l'information ou à la protection des données à caractère personnel de manière formelle, de sorte que les procédures et mesures de contrôle puissent être améliorées. Les leçons tirées d'un incident doivent être communiquées à la direction de l'hôpital, en vue de la validation et de l'approbation d'actions futures.

		• être en possession d'une procédure d'évaluation d'un incident dans laquelle il est précisé comment un incident doit être signalé à l'autorité de protection des données et/ou au point de contact central et comment les personnes concernées doivent être informées

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de répondre aux incidents liés à la sécurité de l'information conformément aux procédures documentées.	Y	Voir A.16.1.4

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Toute organisation est tenu d'évaluer formellement tout incident relatif à la sécurité de l'information ou à la protection des données à caractère personnel, de sorte que les procédures et mesures de contrôle puissent être améliorées. Les leçons tirées d'un incident doivent être communiquées à la direction de l'hôpital, en vue de la validation et de l'approbation d'actions futures.

A.16.1.7 Recueil de preuves

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient que l'organisation définisse et applique des procédures d'identification, de recueil, d'acquisition et de protection de l'information pouvant servir de preuve.	Y	L'hôpital est tenu, en cas d'incidents relatifs à la sécurité de l'information ou à la protection des données à caractère personnel, de collecter correctement les preuves conformément aux prescriptions réglementaires et légales.

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	Explications complémentaires
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	Tout hôpital est tenu de disposer d'un plan de continuité propre qui accorde au moins une attention aux aspects suivants: • L'identification et la documentation des processus essentiels et des systèmes d'information y afférents de l'organisation; • L'évaluation des risques dans laquelle le risque, l'impact et les mesures de contrôle actuelles sont définies; • Les connaissances et compétences des collaborateurs leur permettant de faire tourner les processus essentiels et systèmes d'information y afférents de l'hôpital ou de les redémarrer; • En cas d'incident grave ou de sinistre, qui peut activer le plan de continuité, quand et comment? • Pour toute application critique, déterminer la durée maximale que l'application peut être indisponible (return to operational) et décider qu'en cas d'incident, la perte de données pendant une courte période déterminée au préalable est acceptable. Ce qui a été introduit au cours de cette période devra être introduit à nouveau.

		• Priorités et ordre de restauration; • Communication pendant et après un incident grave ou un sinistre; • Comment le plan de continuité exécuté est-il formellement clôturé après un incident grave ou un sinistre, par qui et à quel moment?

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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 continuité de la sécurité de l'information au cours d'une situation défavorable.	Y	Tout hôpital est tenu de: • rédiger un plan de continuité pour tous les processus critiques et systèmes d'information essentiels. Ce plan décrit l'ensemble des activités, mesures et données essentielles des processus de l'hôpital, et a pour but de limiter le temps d'interruption à un niveau acceptable. • élaborer la sécurité de l'information et la protection des données à caractère personnel en tant qu'élément faisant partie intégrante de la gestion de la continuité (voir la directive 'Gestion de la continuité')

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Tout hôpital est tenu de régulièrement tester et corriger le plan de continuité là où nécessaire. Les résultats des tests doivent être évalués et communiqués au responsable désigné de l'hôpital en vue de la validation et de l'approbation d'actions futures.

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	Explications complémentaires
Il convient de mettre en oeuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité.	N	Pas de norme spécifique. DRP comme demandé ici peut être repris dans la norme suivante *Rédiger un plan de continuité pour tous les processus critiques et systèmes d'information essentiels. Ce plan décrit l'ensemble des activités, mesures et données essentielles des processus de l'hôpital, et a pour but de limiter le temps d'interruption à un niveau acceptable.*

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	Explications complémentaires
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	Toute organisation est tenue de : • réaliser périodiquement une étude de conformité de la situation relative à la sécurité de l'information et à la protection des données à caractère personnel telle que décrite dans les politiques.

		• éviter toute violation de la législation et des obligations contractuelles, statutaires, réglementaires ou légales relatives à la sécurité de l'information et à la protection des données à caractère personnel. • garantir que la sécurité de l'information et la protection des données ont été mises en œuvre et sont opérationnelles conformément aux attentes de la direction. • disposer d'un processus disciplinaire formel pour les travailleurs ayant commis une infraction à la sécurité de l'information ou à la protection des données à caractère personnel.

A.18.1.2 Droits de propriété intellectuelle

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de mettre en oeuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires.	N	N'est pas applicable aux hôpitaux (à l'exception de licences)

A.18.1.3 Protection des enregistrements

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Protection d'enregistrements. Aucun contrôle spécifique en la matière n'est nécessaire.

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Toute organisation est tenue de : • régulièrement établir la cartographie des risques concernant la conformité au Règlement européen. Les actions planifiées suite à un risque « résiduel » majeur de non-conformité doivent être intégrées dans le plan relatif à la sécurité de l'information de l'hôpital et doivent, le cas échéant, être rapportées aux autorités compétentes conformément au RGPD. • au moins réaliser les actions suivantes, en fonction du rôle (sous-traitant ou responsable du traitement) pour un traitement spécifique (ou groupe de traitements spécifiques): • inscrire le traitement dans le registre central des responsables de traitement ou des sous-traitants; • une justification formelle de la non-réalisation des mesures de contrôle axées sur le respect du Règlement européen.

A.18.1.5 Réglementation relative aux mesures cryptographiques

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.	N	Domaine en Belgique. Peut constituer un point supplémentaire lorsque les données sont hébergées à l'étranger.

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	Explications complémentaires
Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisation pour gérer et mettre en oeuvre la sécurité de	N	Le respect des normes sera contrôlé sur base régulière par l'autorité compétente. Pour ce faire, les méthodes suivantes peuvent envisagées.

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.		- Audit par des entreprises externes: une entreprise externe sera désignée pour contrôler le respect des normes au sein des hôpitaux - Peer review: les hôpitaux désignent des personnes compétentes qui peuvent participer à l'exécution de contrôles quant au respect des normes au sein des autres hôpitaux - Audits de qualité: le respect des normes minimales est vérifié lors de l'audit de qualité des hôpitaux (NIAS, JCI)

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

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	L'hôpital doit pouvoir prouver de manière suffisante qu'une révision interne a eu lieu.

A.18.2.3 Examen de la conformité technique

Mesure de gestion (ISO 27001)	SOA	Explications complémentaires
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	Voir A.18.2.2