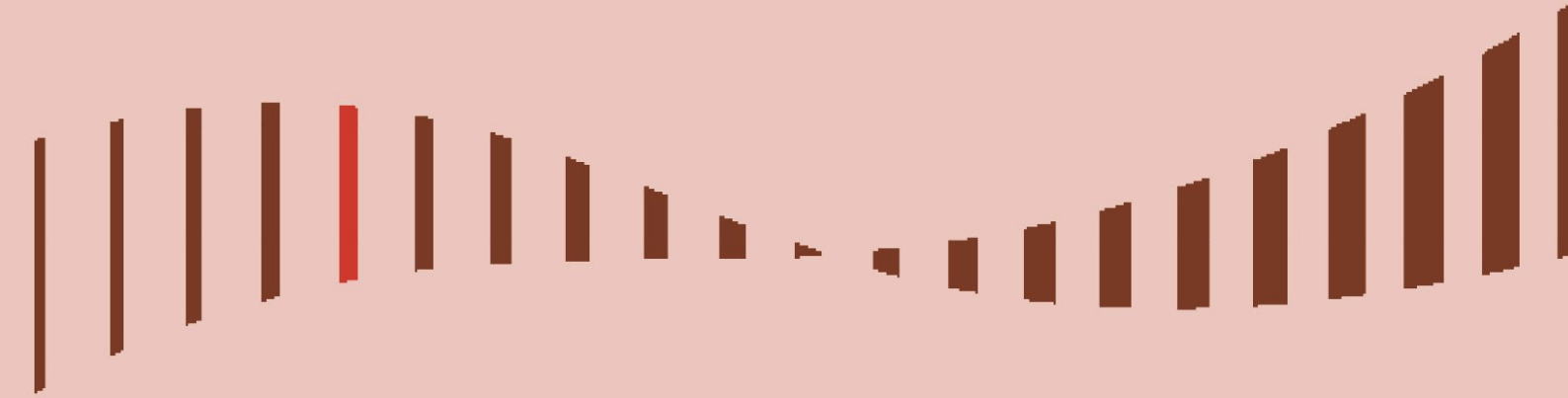
VERSION
0.3.0

Référentiel de certification HDS

Exigences et contrôles

Septembre 2016 - V0.3.0



asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Documents de référence

1. Référence n°1 : ISO/CEI 20000-1:2011
   Technologies de l'information – Gestion des services – Partie 1 : Exigences du système de management des services

2. Référence n°2 : ISO/CEI 27001:2013
   Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences

3. Référence n°3 : ISO/CEI 27002:2013
   Technique de sécurité – Code de bonne pratique pour le management de la sécurité de l'information

4. Référence n°4 : ISO/CEI 27006:2015
   Technologies de l'information – Technique de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

5. Référence n°5 : ISO/CEI 27018:2014
   Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

6. Référence n°6 : Vue d'ensemble du référentiel HDS

7. Référence n°7 : Exigences Référentiel HDS

Sommaire

1.Introduction

1.1. Objet du document

Le présent document constitue le référentiel de certification applicable aux hébergeurs souhaitant obtenir une certification « hébergeur d'infrastructure » ou « hébergeur Infogérant»[1] de données de santé à caractère personnel.

Dans la suite du document, ce référentiel est désigné par le terme référentiel HDS.

1.2. Structure du document

Ce document est composé de cinq chapitres et de deux annexes :

- le chapitre 2 décrit les métiers visés par le référentiel HDS ;
- le chapitre 3 décrit les exigences et les liens entre le référentiel HDS et les normes ISO ;
- le chapitre 4 décrit les modalités de contrôle des exigences et la procédure de certification ;
- le chapitre 5 décrit le cycle de vie de la certification (durée et conditions d'audit, durée de validité de la certification, etc.) ;
- l'annexe A contient la liste exhaustive des exigences du référentiel de certification HDS réparties entre les deux types de certification liée aux métiers « hébergeur d'infrastructure » ou « hébergeur infogérant » ;
- l'annexe B présente un schéma synthétique de la procédure de certification HDS.

[1] Les certifications « hébergeur d'infrastructure » et « hébergeur infogérant » sont décrites dans le document Référence n°6 : Vue d'ensemble du référentiel HDS.
Les dénominations définitives des deux certifications restent à définir.

2.Champ d'application

La définition du périmètre organique des personnes soumises à cette obligation de certification n'est pas traitée dans ce document. Ce périmètre sera défini dans la réglementation.

Le champ d'application présenté dans ce point est relatif aux métiers couverts par la certification HDS.

Deux types de certifications sont définis dans le référentiel :

- une certification « hébergeur d'infrastructure » qui concerne les activités d'hébergement physique, de mise en œuvre de matériels informatiques et de maintenance de matériels informatiques ;
- une certification « hébergeur infogérant » qui concerne les activités d'hébergement physique, de mise en œuvre de matériels informatiques, de maintenance de matériels informatiques et aussi l'activité d'infogérance et de sauvegardes externalisées.

Ces certifications sont délivrées par des organismes de certification (OC) accrédités par le COFRAC en France, ou un homologue européen. Ces organismes de certification ont pour rôle de décider ou non de la conformité de l'hébergeur au référentiel de certification, au vu des résultats d'audits. En fonction des résultats des audits l'OC délivre la certification correspondante (ou attestation de conformité).

Dans la suite du document, le terme certification peut désigner indifféremment l'une ou l'autre de ces certifications.

La certification HDS suppose que le candidat à la certification respecte l'ensemble des exigences du référentiel, dont celles qui sont spécifiques à l'hébergement de données de santé.

Toute exclusion des contrôles prévus en « Annexe A : Exigences du référentiel HDS » doit être formellement justifiée. En cas d'exclusion de contrôles, les affirmations de conformité au référentiel HDS ne sont admises que si ces exclusions n'affectent pas la capacité de l'organisation et/ou sa responsabilité à garantir des niveaux conformes déterminés par une évaluation des risques et les prescriptions légales ou règlementaires.

3.Définition des exigences

Les exigences du référentiel HDS sont définies dans l'Annexe A : Exigences du référentiel HDS. Ces exigences sont :

- des exigences issues de
  - l'ensemble des objectifs et mesures énumérés dans la norme ISO/CEI 27001:2013 ;
  - une partie des objectifs et mesures énumérés dans la norme ISO/CEI 20000-1:2011 ;
  - une partie des objectifs et mesures énumérés dans la norme ISO/CEI 27018:2013 ;
- des exigences spécifiques au domaine de la santé.

Elles sont reparties entre chacun des deux types de certification : « hébergeur d'infrastructure » ou « hébergeur infogérant ». À travers cette segmentation, les hébergeurs peuvent identifier les exigences applicables à leurs activités d'hébergeur de données de santé à caractère personnel et devront mettre en œuvre les moyens organisationnels et techniques permettant d'assurer la sécurité des données de santé. Les hébergeurs peuvent également prendre en compte des exigences additionnelles (par exemple des exigences des normes ISO 20000-1:2011 ou ISO27018 :2015 non obligatoires pour la certification souhaitée).

Les exigences sont regroupées selon 24 domaines d'exigences : 23 domaines sont définis à partir des normes ISO/CEI 27001:2013 (domaines 1 à 21) et ISO/CEI 20000-1:2011 (domaines 22 à 23) et un domaine d'exigences Santé comprend les exigences issues de l'ISO/CEI 270018 :2013 et des exigences spécifiques Santé.

Le tableau suivant énumère les différents domaines d'exigence.

#	Domaine d'exigences	Description
1	Contexte organisationnel	Identification des enjeux externes et internes pertinents qui influent sur la capacité de la direction à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.
2	Leadership	Engagement de la direction en faveur du système de management de la sécurité de l'information.
3	Planification	Implémentation des actions nécessaires afin de maintenir le système de management de la sécurité de l'information.
4	Support	Identification et fourniture des ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.
5	Mise en œuvre du SMSI	Planification, mise en œuvre et contrôle des processus nécessaires à la satisfaction des exigences liées à la sécurité de l'information et à la réalisation des actions déterminées.
6	Évaluation de l'efficacité	Définition d'actions permettant d'évaluer les performances du système de management de la sécurité de l'information dans le but de maintenir le système à jour.
7	Amélioration continue	Amélioration de la pertinence, de l'adéquation et l'efficacité du système de management de la sécurité de l'information.
8	Politique de sécurité	Définition d'une politique de sécurité, adaptée au contexte métier et réglementaire, approuvée par la direction, diffusée et régulièrement revue

#	Domaine d'exigences	Description
9	Organisation	Mise en place d'une organisation interne responsable de la gestion de la sécurité de l'information (organisation, rôles et responsabilités, gouvernance). Gestion du télétravail et des accès en situation de mobilité
10	Ressources humaines	Définition des règles de sécurité pour les employés et les sous-traitants avant leur prise de poste, durant leur emploi et après la résiliation de leur emploi
11	Gestion des actifs	Identification du patrimoine informationnel de l'organisation, classification de l'information et gestion des supports
12	Authentification et contrôle des accès	Gestion des accès (par le personnel de l'hébergeur, le médecin, les utilisateurs, les professionnels de santé, etc.): identification, authentification, autorisation
13	Cryptographie – Chiffrement	Utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.
14	Sécurité physique et environnementale	Protection des infrastructures contre les accès physiques non autorisés, les dommages accidentels. Protection des équipements contre le vol, la perte et toute modification illicite
15	Sécurité liée à l'exploitation	Définition de procédures d'exploitation, protection contre les codes malveillants, sauvegarde, traçabilité des événements, gestion des vulnérabilités et audit des systèmes d'information
16	Acquisition, développement et maintenance des systèmes	Intégration de la sécurité de l'information dans les systèmes d'information tout au long de son cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.
17	Sécurité des communications	Sécurisation des réseaux et des échanges de données entre l'hébergeur et les tiers
18	Gestion des fournisseurs	Protection des actifs de l'hébergeur accessibles par des fournisseurs (éditeur, prestataire, sous-traitant, etc.) et maintien du niveau de sécurité avec les fournisseurs
19	Gestion des incidents	Gestion des incidents de sécurité (rôles et responsabilités, procédures) et notification des parties prenantes
20	Gestion de la continuité d'activité	Gestion de la continuité d'activité, du plan de secours informatique et de la reprise d'activité
21	Conformité	Conformité avec la réglementation (incluant la protection du droit des personnes) et les obligations contractuelles, et audits de la sécurité de l'information
22	Mise en production des services	Évaluation du prestataire de tous les nouveaux services et les changements aux services avec le potentiel d'avoir un impact majeur sur les services ou le client.
23	Fourniture des services	Définition des procédures permettant de fournir et maintenir le service au client.
24	Exigences spécifiques santé	Conformité avec les spécificités du domaine de la santé

4.Modalités de contrôle

4.1. Équivalence

Un candidat souhaitant obtenir une certification devra répondre aux exigences du référentiel et faire une demande de certification auprès d'un organisme de certification accrédité par le COFRAC.

Pour obtenir une certification, un hébergeur devra :

- exploiter un système de gestion de la sécurité des informations conforme à la norme ISO/CEI 27001:2013 ;
    - l'hébergeur pourra obtenir sa certification ISO 27001 :2013 dans le cadre de la certification HDS ou faire valoir une certification ISO 27001 :2013 déjà obtenue ;
- de plus, l'hébergeur sera évalué pour la conformité vis-à-vis des exigences des domaines 22 à 24 (exigences issues des normes ISO 20000 -1 :2011, ISO 27018 :2014 et exigences spécifiques santé).

Le chapitre Annexe A : Exigences du référentiel HDS précise les exigences applicables pour chacun des types de certification (certification « hébergeur d'infrastructure », certification « hébergeur infogérant »).

La certification ISO 20000-1:2011 n'est pas exigée, seules des exigences extraites de cette certifications doivent être respectées par l'hébergeur. Un hébergeur disposant déjà de cette certification ne sera évalué que sur le périmètre des exigences éventuellement non couvertes par sa certification. La certification déjà obtenue fera l'objet d'une vérification selon les modalités définies dans le chapitre 4.2.1.1. Dans ce cas, l'hébergeur devra réaliser un audit limité des exigences couvertes par les certifications existantes.

Cet audit limité aura pour objectif de réaliser un examen de niveau modéré, sur la base de diligences ne mettant toutefois pas en œuvre toutes les procédures requises pour un audit. Cet audit limité est décrit dans le chapitre 4.2.1.1.

La norme ISO 27018:2014, n'est pas prévue pour la délivrance d'une certification mais uniquement comme guide d'implémentation. Les certifications ISO 27018:2014 sont par conséquent émises hors accréditation. Pour cette raison, la notion d'équivalence ne s'applique pas à la norme.

Tout organisme possédant un certificat ISO 27018:2014 et souhaitant être certifié hébergeur de données de santé à caractère personnel, sera évalué par l'organisme de certification sur l'implémentation des contrôles de la norme ISO 27018:2014.

Source des exigences	Cas 1 – le candidat possède les certifications ISO 27001 et 20000	Cas 2 - le candidat possède la certification ISO 27001	Cas 3 - le candidat ne possède aucune certification
ISO 27001			
ISO 20000			
ISO 27018			
Exigences spécifiques			

Pour ce périmètre, les certifications existantes valent respect des exigences et ne font l'objet que d'une vérification.

Pour ce périmètre, les exigences seront auditées par l'organisme de certification

Un candidat n'ayant pas la certification ISO 27001 devra l'obtenir, soit auprès d'un organisme de certification de son choix, soit auprès de l'organisme de certification HDS.

4.2. Procédure de certification

4.2.1. Audit de certification

Le processus de certification HDS est représenté en Annexe B. Il se base sur le processus standard de type système de management (cf. ISO/CEI 17021).

Les chapitres suivants rappellent les points principaux du processus de certification.

4.2.1.1. Vérification des certifications

Si un hébergeur dispose déjà d'une certification sur un ou plusieurs normes sur lesquelles s'appuie le référentiel HDS les contrôles correspondant aux exigences issues de ces normes font l'objet d'un contrôle limité portant sur les points suivants :

- le périmètre de la certification dont dispose l'hébergeur doit inclure toutes les activités de ses opérations liées à l'hébergement de données de santé à caractère personnel, notamment tous les systèmes liés ; toute exclusion du périmètre devra être justifiée en détail ;
- pour un candidat disposant d'une certification ISO 27001, la Déclaration d'applicabilité du système de gestion de la sécurité des informations de l'organisation doit expressément inclure tous les contrôles prévus en Annexe A : Exigences du référentiel HDS, toutes les activités de leurs opérations liées à l'hébergement de données de santé et notamment tous les systèmes liés ; toute exclusion des contrôles ISO/IEC 27001 devra être justifiée en détail ; tout contrôle non applicable sera justifié en détail ;
- la certification doit
  - être en cours de validité
  - ne pas faire l'objet d'une procédure de suspension ou de recertification ;

- ne pas faire l'objet d'une demande de transfert.

4.2.1.2. Préparation de l'audit

Une fois la demande de certification formalisée et communiquée à l'organisme de certification, ce dernier réalise un plan d'audit dans lequel il définit :

- les objectifs en termes de degré de conformité de tout ou partie du système d'information hébergeant les données de santé à caractère personnel ;
- l'évaluation du système d'information à assurer la conformité aux exigences du référentiel HDS ;
- l'évaluation de l'efficacité du système d'information à satisfaire ces objectifs d'hébergement de données de santé à caractère personnel.

4.2.1.3. 1ère étape de l'audit de certification

Avant d'intervenir sur le(s) site(s) où les données de santé seront hébergées, l'organisme de certification réalise une revue documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel HDS. La documentation peut comprendre des documents définissant les différentes procédures de gestion du système d'information ainsi que des rapports d'audit précédents.

4.2.1.4. 2ème étape de l'audit de certification

La 2ème étape de l'audit de certification consiste aux activités d'audit sur site. Avant d'intervenir sur site, l'organisme de certification doit formaliser un plan d'audit spécifiant les modalités de l'intervention de l'audit entre le candidat, l'organisme de certification et l'équipe d'audit.

Le plan d'audit doit notamment contenir :

- les objectifs d'audit ;
- les documents de référence ;
- le périmètre d'intervention ;
- l'identification des lieux d'audit ;
- les rôles et responsabilités de chaque personne ;
- les durées et les dates d'intervention.

L'organisme de certification exécute l'audit de certification en recueillant et vérifiant des informations.

Les preuves d'audit peuvent être recueillies par différentes manières définies dans l'ISO/CEI 27006:2015.

Elles sont évaluées par rapport aux objectifs de l'audit et de telle manière qu'elles soient en accord avec les exigences du référentiel HDS.

Il convient d'enregistrer et de conserver les preuves associées aux non-conformités.

L'organisme de certification formalise et communique un rapport d'audit dans lequel sont définis différents éléments tels que :

- les objectifs de l'audit ;
- le périmètre de l'audit ;
- les dates et lieux d'intervention ;
- les constats d'audits ;
- les conclusions d'audits.

Dans le cas où l'organisme de certification détecte des non-conformités, des actions correctives, préventives ou d'amélioration devront être entreprises par l'audité.

L'ensemble des actions doit être réalisé et audité dans un délai maximum de 3 mois après la date de fin de la 2ème étape de l'audit.

4.2.2. Délivrance du certificat

La délivrance du certificat d'hébergeur de données de santé à caractère personnel résulte de l'examen positif du processus de certification par l'organisme de certification.

Si des non-conformités avaient été constatées à la fin de la 2ème étape de l'audit, le certificat ne pourra être délivré qu'après leur correction, c'est-à-dire lorsque les actions correctives auront été vérifiées et/ou admises par l'organisme de certification.

4.2.3. Audit de surveillance

Une fois l'hébergeur de données de santé certifié pour une période de 3 ans, ce dernier doit effectuer un audit de surveillance auprès de l'organisme de certification une fois par an et cela 1 an après la date de certification initiale (au plus tôt 3 mois avant la date d'anniversaire du certificat).

Tout organisme certifié hébergeur de données de santé devra réaliser un audit de surveillance chaque année avant la date limite qui ne peut pas être fixée plus tard que 12 mois après le dernier jour de la 2ème étape de l'audit.

5.Cycle de vie de la certification

5.1. Durée des audits

La détermination de la durée d'audit doit être réalisée en appliquant la méthode et les tableaux de l'Annexe C de la norme ISO/CEI 27006:2015.

La durée d'audit d'un service d'hébergement dépend notamment de différents critères afférents à l'hébergeur de données de santé, tels que :

- le nombre d'employés ;
- la taille du service d'hébergement : par exemple le nombre de serveurs et/ou machines virtuelles utilisés, le nombre de systèmes d'information utilisés, le volume d'informations traitées, le nombre de clients, le nombre d'utilisateurs intervenant sur le système d'information, la complexité du réseau ;
- les caractéristiques du candidat : par exemple le nombre de pôles ou départements de l'organisation du candidat faisant partie du périmètre de la certification ;
- la complexité du service d'hébergement : par exemple la criticité du ou des systèmes d'information hébergés, la criticité des risques identifiés, le volume d'informations sensibles manipulé, le nombre et les types de transactions électroniques réalisés au sein du service d'hébergement, le nombre de sites impliqués dans le service d'hébergement et la distance les séparant, l'étendue de la documentation formalisée par le candidat, l'étendue et diversité des technologies mises en œuvre au sein du service d'hébergement : les dispositifs de contrôle permettant d'assurer la confidentialité et l'intégrité des données de santé, les mesures correctives ou préventives permettant de limiter les risques, l'étendue et la complexité des réseaux (mobiles, interne, externe, etc.).

5.2. Durée de validité de la certification

La certification est délivrée pour une durée de 3 ans. Les hébergeurs certifiés doivent déposer auprès de l'organisme de certification une demande de recertification au plus tard 3 mois avant la date de fin de la validité de la certification.

5.3. Recertification

Le processus de recertification HDS se base sur le processus standard de type système de management (cf. ISO/CEI 17021).

Un audit de recertification doit être planifié et effectué pour évaluer le maintien de la conformité à toutes les exigences du référentiel HDS. Le but de l'audit de recertification est de confirmer le maintien de la conformité et de l'efficacité du système de management dans son ensemble ainsi que sa pertinence et son applicabilité en permanence au regard du service d'hébergement proposé.

Durant cet audit de recertification, l'organisme de certification réalise :

- un examen de la documentation du système d'information de l'hébergeur de données de santé sur la période de certification ;
- un audit sur site afin de s'assurer que toutes les exigences du référentiel HDS sont vérifiées ;
- une évaluation des résultats des audits de surveillance réalisés sur la période de validité de la certification.

Lorsque des cas de non-conformité ou d'absence de preuves de conformité sont identifiés au cours d'un audit de recertification, l'organisme de certification doit fixer des délais pour la mise en œuvre de corrections et d'actions correctives avant l'expiration de la certification.

L'audit de recertification doit être réalisé et achevé avant l'expiration de la durée de validité du certificat délivré à l'hébergeur de données de santé à caractère personnel. La recertification doit être considérée comme la prolongation de la certification obtenue lors de l'audit initial.

5.4. Sanctions

[Chapitre à compléter avec un renvoi vers les sanctions.

Les normes ISO prévoient que des sanctions soient définies et laissées à la discrétion des autorités compétentes.]

5.5. Transfert de certification

Le transfert d'une certification est défini comme la reconnaissance d'une certification existante et valide, au cours d'un cycle de certification, qui est accordé par un organisme de certification couvert par une accréditation en cours de validité par un autre organisme de certification, également couvert par une accréditation en cours de validité afin d'émettre sa propre certification.

Un hébergeur certifié peut demander le transfert de sa certification, pour la durée de la validité restante à courir à condition que :

- la certification objet de la demande de transfert ne soit pas suspendue ;
- la certification objet de la demande de transfert ne doit pas faire l'objet d'une procédure de recertification.

Annexe A : Exigences du référentiel HDS

Le tableau présenté dans cette annexe énumère la liste des exigences du référentiel HDS.

Chaque ligne comporte :

- un identifiant d'exigence ;
- le point de contrôle ;
- la norme sur laquelle cette exigence s'appuie ;
- une indication précisant si cette exigence doit faire partie de la DdA de la certification « hébergeur d'infrastructure » ou « hébergeur infogérant » ;
- le libellé de l'exigence
- les tests des points de contrôle.

Identifiant	Contrôles	Normes	Types de certification		Exigences certification HDS	Référence
			Hébergeur d'infrastructure	Hébergeur Infogérant		
1 - Contexte organisationnel						
1.1 - Compréhension du contexte						
1.1.1	Objectifs du SMSI	ISO 27001	X	X	Le candidat doit identifier les objectifs du SMSI et les difficultés pouvant porter atteinte à l'efficacité de son système de management de la sécurité de l'information (SMSI).	**cf. ISO/CEI 27001:2013 partie 4.1**
1.2 - Compréhension des attentes des parties prenantes						
1.2.1	Parties prenantes du SMSI	ISO 27001	X	X	Le candidat doit identifier les parties prenantes concernées par le SMSI.	**cf. ISO/CEI 27001:2013 partie 4.2 (a)**
1.2.2	Exigences de sécurité et responsabilités des parties prenantes	ISO 27001	X	X	Le candidat doit communiquer les exigences de sécurité sous responsabilité des parties prenantes.	**cf. ISO/CEI 27001:2013 partie 4.2 (b)**
1.3 - Définition du périmètre du SMSI						
1.3.1	Périmètre du SMSI	ISO 27001	X	X	Le candidat doit formaliser et présenter le périmètre de son SMSI.	**cf. ISO/CEI 27001:2013 partie 4.3**

1.4 - Définition du SMSI						
1.4.1	Conformité du SMSI	ISO 27001	X	X	Le candidat doit être capable de démontrer qu'il a défini, mis en œuvre, maintenu et amélioré son SMSI conformément à la norme ISO 27001.	**cf. ISO/CEI 27001:2013 partie 4.4**
2 - Leadership						
2.1 - Engagement du management						
2.1.1	Orientations stratégiques	ISO 27001	X	X	La politique de sécurité des systèmes d'information doit être en ligne avec les orientations stratégiques.	**cf. ISO/CEI 27001:2013 partie 5.1 (a)**
2.1.2	Intégration du SMSI dans les processus	ISO 27001	X	X	Les processus métier liés à l'activité d'hébergement de données de santé doivent comprendre les exigences liées au SMSI.	**cf. ISO/CEI 27001:2013 partie 5.1 (b)**
2.1.3	Ressources du SMSI	ISO 27001	X	X	La direction doit s'assurer que les ressources nécessaires au bon fonctionnement du SMSI sont disponibles.	**cf. ISO/CEI 27001:2013 partie 5.1 (c)**
2.1.4	Communication du management	ISO 27001	X	X	La direction doit communiquer sur l'importance d'un SMSI efficace et opérationnel au sein des activités d'hébergement de données de santé.	**cf. ISO/CEI 27001:2013 partie 5.1 (d)**
2.1.5	Objectifs du SMSI	ISO 27001	X	X	La direction doit s'assurer que le SMSI atteint les objectifs définis.	**cf. ISO/CEI 27001:2013 partie 5.1 (e)**
2.1.6	Management	ISO 27001	X	X	La direction doit encourager ses équipes à contribuer à l'amélioration et au maintien du SMSI.	**cf. ISO/CEI 27001:2013 partie 5.1 (f)**
2.1.7	Amélioration du SMSI	ISO 27001	X	X	La direction doit promouvoir l'amélioration continue du SMSI.	**cf. ISO/CEI 27001:2013 partie 5.1 (g)**
2.1.8	Leadership	ISO 27001	X	X	La direction encourage les autres membres du management impliqués à faire preuve de leadership sur leur domaine de responsabilité.	**cf. ISO/CEI 27001:2013 partie 5.1 (h)**

2.2 - Politique de Sécurité du SI (PSSI)						
2.2.1.1	Contexte	ISO 27001	X	X	La PSSI doit être adaptée au contexte de l'entreprise, notamment l'hébergement de données de santé.	**cf. ISO/CEI 27001:2013 partie 5.2 (a)**
2.2.1.2	Objectifs du SMSI	ISO 27001	X	X	Les objectifs du SMSI doivent être clairement mentionnés dans la PSSI.	**cf. ISO/CEI 27001:2013 partie 5.2 (b)**
2.2.1.3	Exigences de sécurité	ISO 27001	X	X	Un engagement à respecter les exigences de sécurité doit être formalisé dans la PSSI.	**cf. ISO/CEI 27001:2013 partie 5.2 (c)**
2.2.1.4	Un engagement d'amélioration continue du SMSI est présent dans la PSSI	ISO 27001	X	X	La PSSI doit faire mention de l'amélioration continue du SMSI.	**cf. ISO/CEI 27001:2013 partie 5.2 (d)**
2.2.1.5	La PSSI est documentée	ISO 27001	X	X	La PSSI doit être formalisée.	**cf. ISO/CEI 27001:2013 partie 5.2 (e)**
2.2.1.6	La PSSI est communiquée aux parties concernées	ISO 27001	X	X	La PSSI doit être diffusée au sein de l'organisation.	**cf. ISO/CEI 27001:2013 partie 5.2 (f)**
2.2.1.7	La PSSI est disponible aux parties concernées	ISO 27001	X	X	La PSSI doit être disponible pour les parties concernées.	**cf. ISO/CEI 27001:2013 partie 5.2 (g)**
2.3 - Définition des rôles et responsabilités						
2.3.1	Supervision du niveau de conformité du SMSI	ISO 27001	X	X	La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.	**cf. ISO/CEI 27001:2013 partie 5.3 (a)**
2.3.2	Supervision de la performance du SMSI	ISO 27001	X	X	La direction doit désigner le responsable et lui conférer l'autorité pour s'assurer que le SMSI est conforme aux exigences de la norme ISO/CEI 27001 et rendre compte de la performance du SMSI.	**cf. ISO/CEI 27001:2013 partie 5.3 (b)**

3 - Planification						
3.1 - Actions de traitement des risques						
3.1.1 - Planification générale						
3.1.1.1	Planification du traitement des risques	ISO 27001	X	X	L'organisation doit identifier ses risques et s'assurer que leur traitement est en accord avec les objectifs du SMSI.	**cf. ISO/CEI 27001:2013 partie 6.1.1 (a)**
3.1.1.2	Prévention ou réduction des effets indésirables	ISO 27001	X	X	L'organisation doit s'assurer que le traitement des risques sélectionnés permet la prévention ou la réduction des effets indésirables.	**cf. ISO/CEI 27001:2013 partie 6.1.1 (b)**
3.1.1.3	Amélioration continue du SMSI	ISO 27001	X	X	L'organisation doit appliquer une démarche d'amélioration continue du SMSI.	**cf. ISO/CEI 27001:2013 partie 6.1.1 (c)**
3.1.1.4	Plan d'action	ISO 27001	X	X	Formaliser et mettre en œuvre les actions définies dans le plan d'action permettant de traiter les risques qui ont été identifiés dans l'analyse de risque.	**cf. ISO/CEI 27001:2013 partie 6.1.1 (d)**
3.1.1.5	Intégration des actions correctives aux processus du SMSI	ISO 27001	X	X	S'assurer que la mise en œuvre du plan d'action prévoit les modalités d'intégration aux processus du SMSI ainsi que l'évaluation de leur efficacité.	**cf. ISO/CEI 27001:2013 partie 6.1.1 (e)**
3.1.2 - Évaluation des risques						
3.1.2.1	Méthodologie	ISO 27001	X	X	Le candidat doit fournir une méthodologie d'analyse de risques décrivant notamment les critères d'acceptation des risques.	**cf. ISO/CEI 27001:2013 partie 6.1.2 (a)**
3.1.2.2	Résultats quantifiables et comparables	ISO 27001	X	X	La méthodologie d'analyse de risques doit permettre la production de résultats cohérents, valides et comparables.	**cf. ISO/CEI 27001:2013 partie 6.1.2 (b)**

3.1.2.3	Critères d'analyse de risque	ISO 27001	X	X	La méthodologie d'analyse de risques doit permettre une identification précise des risques suivant les critères de sécurité (disponibilité, intégrité et confidentialité) ainsi que le propriétaire de ces risques.	**cf. ISO/CEI 27001:2013 partie 6.1.2 (c)**
3.1.2.4	Impacts et criticité	ISO 27001	X	X	Le candidat doit s'assurer que la méthodologie d'analyse de risques permet l'identification des impacts, probabilités et niveaux de criticité associée à chacun des risques.	**cf. ISO/CEI 27001:2013 partie 6.1.2 (d)**
3.1.2.5	Priorisation des risques	ISO 27001	X	X	Le candidat doit mettre en œuvre une priorisation des risques en vue d'un traitement et d'une comparaison des risques.	**cf. ISO/CEI 27001:2013 partie 6.1.2 (e)**
3.1.3 - Plan de traitement des risques						
3.1.3.1	Processus de traitement des risques	ISO 27001	X	X	Le processus de traitement des risques doit prendre en compte les résultats de l'analyse de risques, notamment concernant le choix des options de traitement des risques et leur priorisation.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (a)**
3.1.3.2	Traitement des non-conformités	ISO 27001	X	X	Le processus de traitement des risques doit permettre de déterminer toutes les mesures de traitement des risques conformément au choix des options de traitement.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (b)**
3.1.3.3	Rapprochement	ISO 27001	X	X	Le candidat doit s'assurer qu'un rapprochement avec l'Annexe A de l'ISO 27001 de la norme est réalisé afin de s'assurer qu'aucun point de contrôle n'a été omis.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (c)**
3.1.3.4	Déclaration d'applicabilité	ISO 27001	X	X	Présenter une déclaration d'applicabilité, justifiant la sélection et l'exclusion de contrôles de sécurité définie en Annexe A de l'ISO 27001.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (d)**
3.1.3.5	Plan de traitement des risques	ISO 27001	X	X	Présenter un plan de traitement des risques.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (e)**

3.1.3.6	Risques résiduels	ISO 27001	X	X	Faire approuver le plan de traitement des risques par les responsables et obtenir leur acception des risques résiduels.	**cf. ISO/CEI 27001:2013 partie 6.1.3 (f)**
3.2 - Objectifs relatifs à la sécurité de l'information						
3.2.1	Définition	ISO 27001	X	X	Définir les objectifs de sécurité qui doivent être en ligne avec les objectifs de la PSSI.	**cf. ISO/CEI 27001:2013 partie 6.2 (a)**
3.2.2	Indicateur	ISO 27001	X	X	Établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information mesurables.	**cf. ISO/CEI 27001:2013 partie 6.2 (b)**
3.2.3	Analyse de risque	ISO 27001	X	X	Établir des objectifs de sécurité qui prennent en compte l'analyse de risques et les exigences applicables à la sécurité de l'information.	**cf. ISO/CEI 27001:2013 partie 6.2 (c)**
3.2.4	Communication	ISO 27001	X	X	Les objectifs de sécurité doivent être communiqués.	**cf. ISO/CEI 27001:2013 partie 6.2 (d)**
3.2.5	Revue	ISO 27001	X	X	Les objectifs de sécurité doivent être régulièrement contrôlés et mis à jour afin, notamment de s'assurer qu'ils répondent toujours au cadre réglementaire et législatif et que les mesures de sécurité sont toujours en adéquation avec ces objectifs.	**cf. ISO/CEI 27001:2013 partie 6.2 (e)**
3.2.6	Actions	ISO 27001	X	X	Définir les actions permettant d'atteindre les objectifs de sécurité.	**cf. ISO/CEI 27001:2013 partie 6.2 (f)**
3.2.7	Ressources	ISO 27001	X	X	Identifier les ressources mises en œuvre pour réaliser les actions permettant d'atteindre les objectifs de sécurité.	**cf. ISO/CEI 27001:2013 partie 6.2 (g)**
3.2.8	Responsables	ISO 27001	X	X	Identifier les responsables des actions permettant d'atteindre les objectifs de sécurité.	**cf. ISO/CEI 27001:2013 partie 6.2 (h)**
3.2.9	Délais	ISO 27001	X	X	Définir les délais imposés pour la mise en œuvre de chacune des actions.	**cf. ISO/CEI 27001:2013 partie 6.2 (i)**
3.2.10	Évaluation des actions	ISO 27001	X	X	Définir les modalités d'évaluation des résultats des actions.	**cf. ISO/CEI 27001:2013 partie 6.2 (j)**

4 - Support						
4.1 - Ressources						
4.1.1	Ressources	ISO 27001	X	X	Identifier et communiquer les ressources nécessaires à la définition, l'implémentation, la maintenance et l'amélioration continue du SMSI.	**cf. ISO/CEI 27001:2013 partie 7.1**
4.2 - Compétences						
4.2.1	Compétences	ISO 27001	X	X	Identifier les compétences nécessaires aux personnes intervenant sur le périmètre de la sécurité de l'information.	**cf. ISO/CEI 27001:2013 partie 7.2 (a)**
4.2.2	Qualification	ISO 27001	X	X	S'assurer de la compétence de ces personnes.	**cf. ISO/CEI 27001:2013 partie 7.2 (b)**
4.2.3	Adaptation des compétences	ISO 27001	X	X	Si nécessaire, mettre en œuvre les mesures pour acquérir ces compétences et évaluer l'efficacité de ces mesures.	**cf. ISO/CEI 27001:2013 partie 7.2 (c)**
4.2.4	Conservation	ISO 27001	X	X	Conserver les preuves formelles des compétences des ressources.	**cf. ISO/CEI 27001:2013 partie 7.2 (d)**
4.3 - Sensibilisation						
4.3.1	Diffusion	ISO 27001	X	X	Présenter la liste de diffusion permettant de s'assurer que tous les intervenants de l'hébergeur ont pris connaissance de la PSSI.	**cf. ISO/CEI 27001:2013 partie 7.3 (a)**
4.3.2	Rôles et responsabilités des intervenants	ISO 27001	X	X	Les intervenants doivent avoir conscience de leur contribution au SMSI.	**cf. ISO/CEI 27001:2013 partie 7.3 (b)**
4.3.3	Conséquences	ISO 27001	X	X	Les intervenants doivent avoir conscience des conséquences en cas de non-application des exigences du SMSI.	**cf. ISO/CEI 27001:2013 partie 7.3 (c)**
4.4 - Communication						

4.4.1	Plan de communication	ISO 27001	X	X	Présenter le plan ou les principes de communication visant à informer l'ensemble des partenaires et plus particulièrement les personnes physiques ou morales à l'origine du dépôt des données de santé.	**cf. ISO/CEI 27001:2013 partie 7.4 (a)**
4.4.2	La fréquence des communications est définie	ISO 27001	X	X	Identifier à quels moments communiquer.	**cf. ISO/CEI 27001:2013 partie 7.4 (b)**
4.4.3	Les destinataires des communications sont identifiés	ISO 27001	X	X	Identifier les personnes avec qui communiquer.	**cf. ISO/CEI 27001:2013 partie 7.4 (c)**
4.4.4	Les responsables des communications sont identifiés	ISO 27001	X	X	Identifier les personnes responsables de la communication.	**cf. ISO/CEI 27001:2013 partie 7.4 (d)**
4.4.5	Les modalités et moyens de communication sont définis	ISO 27001	X	X	Formaliser les modalités et moyens de communication.	**cf. ISO/CEI 27001:2013 partie 7.4 (e)**
4.5 - Documentation de l'information						
4.5.1 - Documentation générale						
4.5.1.1	Documentation	ISO 27001	X	X	Formaliser et fournir les documents imposés par la norme ISO 27001.	**cf. ISO/CEI 27001:2013 partie 7.5.1 (a)**
4.5.1.2	Documents	ISO 27001	X	X	Formaliser et fournir les documents considérés comme nécessaires au bon fonctionnement du SMSI.	**cf. ISO/CEI 27001:2013 partie 7.5.1 (b)**
4.5.2 - Création et mise à jour de documents						
4.5.2.1	Identification	ISO 27001	X	X	Le candidat doit s'assurer que les documents sont clairement identifiés (exemple : titre, date, auteur et référence).	**cf. ISO/CEI 27001:2013 partie 7.5.2 (a)**
4.5.2.2	Format	ISO 27001	X	X	Le candidat doit s'assurer que les documents produits sont au format approprié.	**cf. ISO/CEI 27001:2013 partie 7.5.2 (b)**

4.5.2.3	Revue et validation	ISO 27001	X	X	Les documents doivent être revus et validés périodiquement afin de garantir la pertinence des informations.	**cf. ISO/CEI 27001:2013 partie 7.5.2 (c)**
4.5.3 - Contrôle de la documentation						
4.5.3.1	Disponibilité de la documentation	ISO 27001	X	X	Définir les contrôles mis en œuvre permettant de s'assurer que la documentation est disponible à tout moment.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (a)**
4.5.3.2	Protection de la documentation	ISO 27001	X	X	Définir les contrôles et les moyens de sécurité mis en œuvre permettant de s'assurer que la documentation est correctement protégée.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (b)**
4.5.3.3	Moyens d'accès	ISO 27001	X	X	Définir les modalités de distribution, d'accès et d'utilisation de la documentation.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (c)**
4.5.3.4	Conservation et archivage	ISO 27001	X	X	Définir les modalités de stockage et conservation de la documentation.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (d)**
4.5.3.5	Système de gestion des versions	ISO 27001	X	X	Présenter un système de gestion des versions documentaires.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (e)**
4.5.3.6	Durées de conservation	ISO 27001	X	X	Définir les durées de rétention et modalités de destruction de la documentation.	**cf. ISO/CEI 27001:2013 partie 7.5.3 (f)**
5 - Mise en œuvre du SMSI						
5.1 - Prérequis globaux						
5.1.1	Objectifs de sécurité	ISO 27001	X	X	Planifier, mettre en œuvre et contrôler les processus permettant d'atteindre les objectifs de sécurité.	**cf. ISO/CEI 27001:2013 partie 8.1**
5.1.2	Processus (1/2)	ISO 27001	X	X	Conserver les preuves du suivi de ces processus.	**cf. ISO/CEI 27001:2013 partie 8.1**
5.1.3	Processus (2/2)	ISO 27001	X	X	Définir un processus de contrôle des modifications prévues ou imprévues de ces processus qui prévoit a minima l'analyse des conséquences des modifications et la définition d'actions limitant les effets négatifs.	**cf. ISO/CEI 27001:2013 partie 8.1**

5.1.4	Processus externalisés	ISO 27001	X	X	Identifier et contrôler les processus externalisés	**cf. ISO/CEI 27001:2013 partie 8.1**
5.2 - Analyses de risques						
5.2.1	Fréquence	ISO 27001	X	X	Mettre à jour l'analyse de risque à intervalles planifiés ou en cas de changement significatif.	**cf. ISO/CEI 27001:2013 partie 8.2**
5.2.2	Résultats	ISO 27001	X	X	Documenter et conserver les résultats des analyses de risques.	**cf. ISO/CEI 27001:2013 partie 8.2**
5.3 - Traitement des risques						
5.3.1	Plan de traitement des risques	ISO 27001	X	X	Définir et mettre en œuvre un plan de traitement des risques	**cf. ISO/CEI 27001:2013 partie 8.3**
5.3.2	Conservation	ISO 27001	X	X	Documenter et conserver les résultats du plan de traitement des risques	**cf. ISO/CEI 27001:2013 partie 8.3**
6 - Évaluation de l'efficacité						
6.1 - Supervision, évaluation et analyse de l'efficacité du SMSI						
6.1.1	Périmètre de supervision	ISO 27001	X	X	Définir le périmètre de supervision du SMSI notamment des processus et des mesures définies dans le SMSI.	**cf. ISO/CEI 27001:2013 partie 9.1 (a)**
6.1.2	Moyens de surveillance	ISO 27001	X	X	Présenter les moyens de surveillance mis en œuvre.	**cf. ISO/CEI 27001:2013 partie 9.1 (b)**
6.1.3	Indicateurs de supervision	ISO 27001	X	X	Planifier la surveillance du SMSI.	**cf. ISO/CEI 27001:2013 partie 9.1 (c)**
6.1.4	Responsables de la génération des indicateurs	ISO 27001	X	X	Identifier le(s) responsable(s) de la surveillance	**cf. ISO/CEI 27001:2013 partie 9.1 (d)**
6.1.5	Analyse des indicateurs	ISO 27001	X	X	Définir une fréquence d'analyse des résultats de la surveillance.	**cf. ISO/CEI 27001:2013 partie 9.1 (e)**
6.1.6	Responsables de l'analyse	ISO 27001	X	X	Identifier le(s) responsable(s) de cette analyse.	**cf. ISO/CEI 27001:2013 partie 9.1 (f)**
6.2 - Audit interne						
6.2.1	Rapports d'audit	ISO 27001	X	X	Communiquer les rapports d'audit réalisés par le candidat permettant de s'assurer de la conformité du SMSI aux exigences de l'entreprise ainsi qu'aux exigences de la norme ISO 27001	**cf. ISO/CEI 27001:2013 partie 9.2 (a)**

6.2.2	Contrôles	ISO 27001	X	X	Présenter les principes de contrôles périodiques visant à assurer que les mesures de protection sont efficacement mises en œuvre.	**cf. ISO/CEI 27001:2013 partie 9.2 (b)**
6.2.3	Plan d'audit	ISO 27001	X	X	Un plan d'audit interne est défini (fréquence, méthodologie responsabilités, planning), prenant en compte les résultats des précédents audits	**cf. ISO/CEI 27001:2013 partie 9.2 (c)**
6.2.4	Périmètre	ISO 27001	X	X	Le plan d'audit doit définir le périmètre et les critères de chacun des audits réalisés.	**cf. ISO/CEI 27001:2013 partie 9.2 (d)**
6.2.5	Objectivité	ISO 27001	X	X	Le candidat doit s'assurer de l'objectivité et de l'impartialité des résultats d'audit.	**cf. ISO/CEI 27001:2013 partie 9.2 (e)**
6.2.6	Communication	ISO 27001	X	X	S'assurer de la communication des résultats d'audit à la direction concernée.	**cf. ISO/CEI 27001:2013 partie 9.2 (f)**
6.2.7	Documentation	ISO 27001	X	X	Le plan d'audit et les résultats d'audit doivent être documentés et conservés comme preuve de la mise en œuvre des audits.	**cf. ISO/CEI 27001:2013 partie 9.2 (g)**
6.3 - Revue périodique du management						
6.3.1	Revues périodiques	ISO 27001	X	X	Le management doit réaliser des revues périodiques du SMSI de manière à s'assurer de sa pertinence et de son efficacité.	**cf. ISO/CEI 27001:2013 partie 9.3**
6.3.2	Revues antérieurs	ISO 27001	X	X	Les revues périodiques du SMSI par le management doivent prendre en compte les actions relatives aux précédentes revues.	**cf. ISO/CEI 27001:2013 partie 9.3 (a)**
6.3.3	Changement impactant le SMSI	ISO 27001	X	X	Les revues doivent prendre en compte les changements affectant le SMSI.	**cf. ISO/CEI 27001:2013 partie 9.3 (b)**

6.3.4	Retours relatifs à l'efficacité du SMSI	ISO 27001	X	X	Les revues doivent prendre en compte les retours relatifs à l'efficacité du SMSI (non-conformités, indicateurs de supervision, résultats d'audit, évaluation de l'atteinte des objectifs de sécurité).	**cf. ISO/CEI 27001:2013 partie 9.3 (c)**
6.3.5	Retours des parties concernées	ISO 27001	X	X	Les revues doivent prendre en compte les retours, remarques et points d'attention des parties concernées.	**cf. ISO/CEI 27001:2013 partie 9.3 (d)**
6.3.6	Analyse de risque	ISO 27001	X	X	Les revues doivent prendre en compte les résultats de l'analyse de risques et le statut des actions du plan de traitement des risques.	**cf. ISO/CEI 27001:2013 partie 9.3 (e)**
6.3.7	Amélioration continue du SMSI	ISO 27001	X	X	Les revues doivent prendre en compte les opportunités d'amélioration continue.	**cf. ISO/CEI 27001:2013 partie 9.3 (f)**
6.3.8	Revues périodiques (1/2)	ISO 27001	X	X	Les conclusions de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et aux éventuellement changements.	**cf. ISO/CEI 27001:2013 partie 9.3**
6.3.9	Revues périodiques (2/2)	ISO 27001	X	X	Les conclusions de la revue de direction doivent être formalisées et conservées à titre de preuve.	**cf. ISO/CEI 27001:2013 partie 9.3**
7 - Amélioration continue						
7.1 - Gestion des non-conformités						
7.1.1	Mesures	ISO 27001	X	X	En cas de détection de non-conformité, corriger et maîtriser les mesures prises permettant de traiter les conséquences dues à la non-conformité.	**cf. ISO/CEI 27001:2013 partie 10.1 (a)**

7.1.2	Origines	ISO 27001	X	X	Mettre en œuvre une action permettant d'éliminer les causes des non-conformités, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs. Pour cela, l'hébergeur doit examiner et déterminer les causes des non-conformités.	**cf. ISO/CEI 27001:2013 partie 10.1 (b)**
7.1.3	Actions correctives	ISO 27001	X	X	Dans le cas de détection de non-conformité, mettre en œuvre des actions correctives permettant de limiter les risques.	**cf. ISO/CEI 27001:2013 partie 10.1 (c)**
7.1.4	Évaluation	ISO 27001	X	X	Les actions correctives doivent faire l'objet d'une évaluation afin de s'assurer de leurs efficacités.	**cf. ISO/CEI 27001:2013 partie 10.1 (d)**
7.1.5	Modification du SMSI	ISO 27001	X	X	Documenter toutes les modifications apportées au système de management de sécurité de l'information dans le cas du déploiement d'actions correctives.	**cf. ISO/CEI 27001:2013 partie 10.1 (e)**
7.1.6	Association des non-conformités	ISO 27001	X	X	Conserver des informations documentées comme preuve de la nature des non-conformités et de toute action subséquente.	**cf. ISO/CEI 27001:2013 partie 10.1 (f)**
7.1.7	Documentation des actions correctives	ISO 27001	X	X	Conserver des informations documentées comme preuves des résultats de toute action corrective.	**cf. ISO/CEI 27001:2013 partie 10.1 (g)**
7.2 - Processus d'amélioration continue						
7.2.1	SMSI	ISO 27001	X	X	Formaliser, appliquer et mettre à jour régulièrement une procédure permettant d'améliorer la pertinence, l'adéquation et l'efficacité du système de management de la sécurité de l'information.	**cf. ISO/CEI 27001:2013 partie 10.2**

8 - Politique de sécurité du SI						
8.1 -Gestion de la sécurité de l'information						
8.1.1	Politiques de sécurité du SI	ISO 27001	X	X	Un ensemble de politique de sécurité de l'information doit être défini, approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	**cf. ISO/CEI 27001:2013 Annexe A. 5.1.1**
8.1.2	Revue des politiques de sécurité du SI	ISO 27001	X	X	Pour garantir la pertinence, l'adéquation et l'effectivité dans le temps des politiques de sécurité de l'information, ces dernières doivent être réexaminées à intervalles fixés préalablement ou en cas de changements majeurs.	**cf. ISO/CEI 27001:2013 Annexe A. 5.1.2**
9- Organisation de la sécurité						
9.1 - Organisation interne						
9.1.1	Rôles et responsabilités relatifs à la sécurité	ISO 27001	X	X	Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement et attribuées.	**cf. ISO/CEI 27001:2013 Annexe A. 6.1.1**
9.1.2	Séparation des tâches	ISO 27001	X	X	Définir une matrice de séparation des tâches définissant les domaines de responsabilité incompatibles dans la gestion des données de santé. De plus, présenter les contrôles mis en œuvre afin de s'assurer que les modifications non autorisées ou involontaires des actifs des personnes concernées fassent l'objet d'alerte.	**cf. ISO/CEI 27001:2013 Annexe A. 6.1.2**
9.1.3	Contact avec les autorités compétentes	ISO 27001	X	X	Des relations appropriées doivent être mises en place avec les autorités compétentes.	**cf. ISO/CEI 27001:2013 Annexe A. 6.1.3**

9.1.4	Contact avec les groupes d'intérêts communs	ISO 27001	X	X	Des relations appropriées doivent être entretenues avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.	**cf. ISO/CEI 27001:2013 Annexe A. 6.1.4**
9.1.5	Intégration de la sécurité dans les projets	ISO 27001	X	X	Considérer la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.	**cf. ISO/CEI 27001:2013 Annexe A. 6.1.5**
9.2 - Terminaux mobiles et télétravail						
9.2.1	Sécurité des terminaux mobiles	ISO 27001	X	X	Une politique formelle et des mesures de sécurité appropriées doivent être mises en place pour assurer une protection contre le risque lié à l'utilisation d'appareils mobiles.	**cf. ISO/CEI 27001:2013 Annexe A. 6.2.1**
9.2.2	Télétravail	ISO 27001	X	X	Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.	**cf. ISO/CEI 27001:2013 Annexe A. 6.2.2**
10 - Gestion des ressources humaines						
10.1 - Avant contractualisation						
10.1.1	Screening	ISO 27001	X	X	Des contrôles de vérification de fond sur tous les candidats à l'embauche doivent être effectués en conformité avec les lois, les règlements pertinents et l'éthique et doivent être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	**cf. ISO/CEI 27001:2013 Annexe A. 7.1.1**
10.1.2	Définition des conditions d'emploi	ISO 27001	X	X	Les conditions contractuelles signées avec les employés et les sous-traitants indiquent les rôles et responsabilités de chaque partie en matière de sécurité de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 7.1.2**

10.2 - Pendant la contractualisation						
10.2.1	Responsabilités du management	ISO 27001	X	X	La direction demande aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.	**cf. ISO/CEI 27001:2013 Annexe A. 7.2.1**
10.2.2	Formation et sensibilisation à la sécurité	ISO 27001	X	X	Les plans de formation et des plans de sensibilisation aux mesures de sécurité sont mis en place à l'attention du personnel et, quand cela est pertinent, des sous-traitants. De plus, le personnel et les sous-traitants reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.	**cf. ISO/CEI 27001:2013 Annexe A. 7.2.2**
10.2.3	Processus disciplinaire	ISO 27001	X	X	Mettre en œuvre et maintenir à jour une procédure disciplinaire en place permettant de prendre des mesures contre les employés ayant commis des infractions liées à la confidentialité et l'intégrité des données de santé.	**cf. ISO/CEI 27001:2013 Annexe A. 7.2.3**
10.3 - Résiliation du contrat						
10.3.1	Résiliation ou modification du contrat	ISO 27001	X	X	Les informations traitant des devoirs et responsabilités des employés en matière de sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, doivent être définies et communiquées à l'employé.	**cf. ISO/CEI 27001:2013 Annexe A. 7.3.1**

11- Gestion des actifs						
11.1 - Affectation des responsabilités						
11.1.1	Inventaire des actifs	ISO 27001	X	X	Les actifs liés à l'information et aux moyens de traitement de l'information doivent être clairement identifiés au sein du système d'information (DMZ, etc.) et un inventaire de ces actifs doit être réalisé a minima une fois par an.	**cf. ISO/CEI 27001:2013 Annexe A. 8.1.1**
11.1.2	Propriétaires des actifs	ISO 27001	X	X	La propriété de chaque information et des moyens de traitement de l'information doit être attribuée à une partie définie de l'organisme.	**cf. ISO/CEI 27001:2013 Annexe A. 8.1.2**
11.1.3	Conditions d'utilisation des actifs	ISO 27001	X	X	Des règles permettant l'utilisation correcte des données à caractère personnel et des actifs associés et les moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.	**cf. ISO/CEI 27001:2013 Annexe A. 8.1.3**
11.1.4	Retour des actifs	ISO 27001	X	X	Tous les salariés et utilisateurs tiers doivent restituer l'ensemble des actifs de l'organisation qu'ils ont en leur possession au terme de leur contrat ou accord.	**cf. ISO/CEI 27001:2013 Annexe A. 8.1.4**
11.2 - Classification de l'information						
11.2.1	Classification de l'information	ISO 27001	X	X	Présenter une classification des données faisant apparaitre une catégorie "donnée de santé" définissant la criticité et sensibilité de chaque actif. De plus, la classification doit faire apparaitre le risque d'exposition à l'altération ou divulgation des données de santé.	**cf. ISO/CEI 27001:2013 Annexe A. 8.2.1**
11.2.2	Marquage de l'information	ISO 27001	X	X	Fournir une procédure de marquage des données de santé en conformité avec le système de classification de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 8.2.2**

11.2.3	Gestion des actifs	ISO 27001	X	X	Élaborer et mettre en œuvre des procédures de traitement de l'information conformément au plan de classification de l'information adopté par l'organisation.	**cf. ISO/CEI 27001:2013 Annexe A. 8.2.3**
11.3 - Manipulation des supports						
11.3.1	Gestion des supports amovibles	ISO 27001	X	X	Des procédures doivent être implémentées pour la gestion des supports amovibles en adéquation avec le modèle de classification retenu par l'organisation.	**cf. ISO/CEI 27001:2013 Annexe A. 8.3.1**
11.3.2	Mise au rebut	ISO 27001	X	X	Tout matériel équipé des supports de stockage doit être contrôlé en cas de mise au rebut afin que toutes les données de santé soient supprimées de manière sécurisée. Si ce matériel contient des données à caractère personnel sensibles, des mesures spécifiques doivent être prises pour détruire physiquement ce matériel ou supprimer les informations au moyen de techniques qui rendent impossible toute récupération.	**cf. ISO/CEI 27001:2013 Annexe A. 8.3.2**

11.3.3	Transfert sur support physique	ISO 27001	X	X	Tout support contenant des données de santé doit être protégé contre tout accès non autorisé, abus ou corruption durant le transfert. Pour cela, appliquer des mesures de protection relatives aux dispositifs de stockage contenant des données à caractère personnel ainsi que des dispositifs de sécurité sur les réseaux • Encodage (à travers un module) des supports physiques; • Chiffrement des canaux de communication; • Protection par code checksum; • etc. Certains aspects des solutions mises en œuvre seront laissés à la discrétion des hébergeurs en tant que décision relative à la gestion des risques.	**cf. ISO/CEI 27001:2013 Annexe A. 8.3.3**
12 - Contrôle d'accès						
12.1 - Besoins Métier relatifs au contrôle d'accès						
12.1.1	Politique de contrôle d'accès	ISO 27001	X	X	Fournir une politique de contrôle d'accès établie, documentée et examinée sur la base des exigences métier et de sécurité de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 9.1.1**
12.1.2	Accès au réseau et aux services réseau	ISO 27001	X	X	Des méthodes d'authentification appropriées doivent être utilisées pour contrôler l'accès des utilisateurs distant.	**cf. ISO/CEI 27001:2013 Annexe A. 9.1.2**

12.2 - Gestion des accès utilisateurs						
12.2.1	Création et suppression d'accès	ISO 27001	X	X	Une procédure formelle d'inscription et désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie et mise en œuvre.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.1**
12.2.2	Provisionnement des droits	ISO 27001	X	X	Un processus doit être implémenté pour l'attribution et le retrait des droits à tous types d'utilisateurs sur l'ensemble des systèmes et services.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.2**
12.2.3	Gestion des droits étendus	ISO 27001	X	X	L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.3**
12.2.4	Gestion des identifiants	ISO 27001	X	X	Présenter une procédure de gestion des identifiants décrivant l'attribution des informations secrètes d'authentification.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.4**
12.2.5	Revue des habilitations	ISO 27001	X	X	Les propriétaires d'actifs doivent réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.5**
12.2.6	Retrait ou ajustement de droits	ISO 27001	X	X	Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.	**cf. ISO/CEI 27001:2013 Annexe A. 9.2.6**
12.3 - Responsabilités des utilisateurs						
12.3.1	Utilisation et protection des identifiants	ISO 27001	X	X	Les utilisateurs internes de l'organisation doivent respecter les pratiques définies quant à l'utilisation des informations secrètes d'authentification	**cf. ISO/CEI 27001:2013 Annexe A. 9.3.1**

12.4 Contrôle d'accès aux systèmes et applications						
12.4.1	Restriction des accès	ISO 27001	X	X	Pour les utilisateurs et le personnel chargé de l'assistance technique, l'accès aux informations et aux fonctions applicatives doit être restreint conformément à la politique de contrôle d'accès.	**cf. ISO/CEI 27001:2013 Annexe A. 9.4.1**
12.4.2	Mécanismes de contrôle d'accès	ISO 27001	X	X	L'accès aux systèmes et aux applications doit être contrôlés par une procédure de connexion sécurisée qui impose l'utilisation d'un identifiant unique et exclusif pour chaque utilisateur et une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur.	**cf. ISO/CEI 27001:2013 Annexe A. 9.4.2**
12.4.3	Système de gestion des mots de passe	ISO 27001	X	X	Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité.	**cf. ISO/CEI 27001:2013 Annexe A. 9.4.3**
12.4.4	Utilisation de systèmes à droits étendus	ISO 27001	X	X	L'accès aux fonctions IT étendues est limité aux utilisateurs appropriés et étroitement contrôlé.	**cf. ISO/CEI 27001:2013 Annexe A. 9.4.4**
12.4.5	Contrôle d'accès au code source	ISO 27001	X	X	L'accès au code source des programmes doit être restreint aux personnes autorisées.	**cf. ISO/CEI 27001:2013 Annexe A. 9.4.5**
13- Cryptographie - Chiffrement						
13.1 - Contrôles cryptographiques						
13.1.1	Politique de chiffrement et d'utilisation des contrôles cryptographiques	ISO 27001	X	X	Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.	**cf. ISO/CEI 27001:2013 Annexe A. 10.1.1**
13.1.2	Gestion des clés	ISO 27001	X	X	Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie.	**cf. ISO/CEI 27001:2013 Annexe A. 10.1.2**

14 - Sécurité physique et environnementale						
14.1 - Zones sécurisées						
14.1.1	Périmètre de sécurité physique	ISO 27001	X	X	Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.1**
14.1.2	Contrôle des accès physiques	ISO 27001	X	X	Les zones sécurisées doivent être protégées par des contrôles à l'entrée, adéquats pour s'assurer que seul le personnel habilité est admis.	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.2**
14.1.3	Sécurisation des salles et bureaux	ISO 27001	X	X	Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements.	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.3**
14.1.4	Protection contre les menaces externes et environnementales	ISO 27001	X	X	Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.4**
14.1.5	Travail dans les zones sécurisées	ISO 27001	X	X	Des mesures de protection physique et des directives pour le travail en zone sécurisée doivent être conçues et appliquées.	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.5**
14.1.6	Zones de livraison	ISO 27001	X	X	Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés. Les points d'accès doivent également, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.	**cf. ISO/CEI 27001:2013 Annexe A. 11.1.6**

14.2 - Équipements						
14.2.1	Localisation et protection des équipements	ISO 27001	X	X	Les matériels doivent être situés et protégés de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.1**
14.2.2	Protection contre les pannes de courant	ISO 27001	X	X	Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.2**
14.2.3	Sécurité du câblage	ISO 27001	X	X	Les câbles électriques ou de télécommunications transportant des données ou supportant les services d'information doivent être protégés contre toute interception d'information ou dommage.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.3**
14.2.4	Maintenance des équipements	ISO 27001	X	X	Les matériels doivent être entretenus correctement pour garantir sa disponibilité permanente et son intégrité.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.4**
14.2.5	Retrait des équipements	ISO 27001	X	X	Les matériels, les informations ou les logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.5**
14.2.6	Sécurité des équipements non présents sur site	ISO 27001	X	X	Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.6**
14.2.7	Mise au rebut des équipements sécurisés	ISO 27001	X	X	Tous les composants matériel contenant des supports de stockage doivent être vérifiés 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 leur réutilisation.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.7**

14.2.8	Protection des équipements non surveillés	ISO 27001	X	X	Les utilisateurs doivent s'assurer que tout matériel laissé sans surveillance est doté d'une protection appropriée.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.8**
14.2.9	Application de la politique du bureau vide	ISO 27001	X	X	Une politique du bureau propre doit être adoptée pour les documents papier et les supports de stockage amovibles, et une politique de l'écran verrouillé doit également être adoptée pour les moyens de traitement de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 11.2.9**
15 - Sécurité opérationnelle						
15.1 - Procédures et responsabilités opérationnelles						
15.1.1	Formalisation et disponibilité des procédures opérationnelles	ISO 27001	X	X	Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	**cf. ISO/CEI 27001:2013 Annexe A. 12.1.1**
15.1.2	Gestion des changements	ISO 27001	X	X	Les changements apportés aux systèmes, processus métier et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.	**cf. ISO/CEI 27001:2013 Annexe A. 12.1.2**
15.1.3	Dimensionnement	ISO 27001	X	X	L'Utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.	**cf. ISO/CEI 27001:2013 Annexe A. 12.1.3**
15.1.4	Séparation des environnements (développement, test, production)	ISO 27001	X	X	Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.	**cf. ISO/CEI 27001:2013 Annexe A. 12.1.4**

15.2 - Protection contre les logiciels malveillants						
15.2.1	Contrôles contre les logiciels malveillants	ISO 27001	X	X	Des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre.	**cf. ISO/CEI 27001:2013 Annexe A. 12.2.1**
15.3 - Sauvegarde						
15.3.1	Sauvegarde des informations	ISO 27001	X	X	Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.	**cf. ISO/CEI 27001:2013 Annexe A. 12.3.1**
15.4 - Journalisation et supervision						
15.4.1	Journalisation des événements	ISO 27001 et ISO 27018	X	X	Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être crées, tenus à jour et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.	**cf. ISO/CEI 27018:2014 Partie 12.4**
15.4.2	Protection des journaux	ISO 27001 et ISO 27018	X	X	Les équipements de journalisation et les informations journalisées doivent être protégés contre les risques de falsification ou d'accès non autorisés.	**cf. ISO/CEI 27018:2014 Partie 12.4**
15.4.3	Journaux des administrateurs	ISO 27001 et ISO 27018	X	X	Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.	**cf. ISO/CEI 27018:2014 Partie 12.4**

15.4.4	Synchronisation horaire	ISO 27001	X	X	Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de référence temporelle unique.	**cf. ISO/CEI 27001:2013 Annexe A. 12.4.4**
15.5 - Contrôle des logiciels opérationnels						
15.5.1	Installation de logiciels sur les environnements de production	ISO 27001	X	X	Des procédures doivent être mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.	**cf. ISO/CEI 27001:2013 Annexe A. 12.5.1**
15.6 - Gestion des vulnérabilités techniques						
15.6.1	Gestion des vulnérabilités techniques	ISO 27001	X	X	Toutes informations concernant toutes vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues à temps, l'exposition de l'organisme aux dites vulnérabilités doit être évaluée et les mesures appropriées doivent être entreprises pour traiter le risque associé.	**cf. ISO/CEI 27001:2013 Annexe A. 12.6.1**
15.6.2	Restrictions concernant l'installation de logiciels	ISO 27001	X	X	Des procédures doivent être mises en place pour contrôler l'installation de logiciels par les utilisateurs sur les systèmes en exploitation.	**cf. ISO/CEI 27001:2013 Annexe A. 12.6.2**
15.7 - Considérations d'audit des SI						
15.7.1	Réalisation d'audits de contrôle	ISO 27001	X	X	Les exigences d'audit et les activités impliquant des vérifications sur des systèmes en exploitation doivent être planifiées de manière précise et doivent être le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.	**cf. ISO/CEI 27001:2013 Annexe A. 12.7.1**

16- Sécurité des communications						
16.1 - Gestion de la sécurité réseau						
16.1.1	Contrôles réseau	ISO 27001	X	X	Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.	**cf. ISO/CEI 27001:2013 Annexe A. 13.1.1**
16.1.2	Sécurité des services réseau	ISO 27001	X	X	Pour tous les services réseau, les mécanismes de sécurité, les fonctions réseau, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	**cf. ISO/CEI 27001:2013 Annexe A. 13.1.2**
16.1.3	Cloisonnement des réseaux	ISO 27001	X	X	Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés sur les réseaux.	**cf. ISO/CEI 27001:2013 Annexe A. 13.1.3**
16.2 - Transferts d'informations						
16.2.1	Politiques et procédures de transfert d'informations	ISO 27001	X	X	Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tout type d'équipement de télécommunication.	**cf. ISO/CEI 27001:2013 Annexe A. 13.2.1**
16.2.2	Contractualisation relative aux échanges d'informations (avec les entités externes)	ISO 27001	X	X	Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.	**cf. ISO/CEI 27001:2013 Annexe A. 13.2.2**
16.2.3	Messagerie électronique	ISO 27001	X	X	Les informations échangées par la messagerie électronique doivent être protégées de façon appropriée	**cf. ISO/CEI 27001:2013 Annexe A. 13.2.3**
16.2.4	Engagements de confidentialité	ISO 27001	X	X	Les exigences en matière d'engagements de confidentialité ou de non-divulgation doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.	**cf. ISO/CEI 27001:2013 Annexe A. 13.2.4**

17 - Acquisition, développement et maintenance des systèmes						
17.1 - Exigences de sécurité						
17.1.1	Analyse et formalisation des exigences de sécurité	ISO 27001	X	X	Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.	**cf. ISO/CEI 27001:2013 Annexe A. 14.1.1**
17.1.2	Sécurisation des services applicatifs sur les réseaux publics	ISO 27001	X	X	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, la capacité de connexion réseau des utilisateurs doit être restreinte, conformément à la politique de contrôle d'accès et aux exigences relatives aux applications métier. De plus, les informations transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, la divulgation et la modification non autorisées.	**cf. ISO/CEI 27001:2013 Annexe A. 14.1.2**
17.1.3	Protection des transactions applicatives	ISO 27001	X	X	Les transactions entre services applicatifs doivent être protégées contre les interruptions de transmission, les erreurs de routage, les altérations illicites, les pertes de confidentialité, et les duplications ou rejeux non autorisés	**cf. ISO/CEI 27001:2013 Annexe A. 14.1.3**
17.2 - Sécurité des processus support et de développement						
17.2.1	Politique de développement sécurisé	ISO 27001	X	X	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.1**

17.2.2	Gestion des évolutions (contrôle, formalisation)	ISO 27001	X	X	Les demandes de changements (mise à niveau, modifications de programme, correctifs, nouvelles applications, changements de configuration) des applications et des systèmes dans le cadre du cycle de développement doivent être documentées et contrôlées dans le respect des procédures de gestion des évolutions informatiques.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.2**
17.2.3	Revue technique des applications suite à des modifications	ISO 27001	X	X	Lorsque des modifications sont apportées aux systèmes d'exploitation, les applications critiques métier doivent être réexaminées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.3**
17.2.4	Restrictions sur les modifications des progiciels	ISO 27001	X	X	Les modifications des progiciels ne doivent pas être encouragées, et être limitées aux changements nécessaires. Un contrôle strict doit également être exercé sur ces modifications.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.4**
17.2.5	Principe de sécurisation des systèmes	ISO 27001	X	X	Les principes de conception de systèmes sécurisés doivent être définis, documentés, maintenus et appliqués à toute activité d'implémentation de système	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.5**
17.2.6	Environnement de développement sécurisé	ISO 27001	X	X	Des dispositifs de sécurité doivent être mis en œuvre sur les environnements de développements pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.6**

17.2.7	Développements externalisés	ISO 27001	X	X	Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.7**
17.2.8	Tests sur la sécurité des systèmes	ISO 27001	X	X	Pendant le développement, la sécurité des systèmes doit être réexaminée et testée afin de vérifier la conformité des dispositifs mis en œuvre sur le système d'information.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.8**
17.2.9	Tests d'acceptation	ISO 27001	X	X	Des critères d'acceptation doivent être fixés pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.	**cf. ISO/CEI 27001:2013 Annexe A. 14.2.9**
17.3 - Données de test						
17.3.1	Protection des données de test	ISO 27001	X	X	Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.	**cf. ISO/CEI 27001:2013 Annexe A. 14.3.1**
18- Relation client/fournisseur						
18.1 - Sécurité de l'information dans les relations client/fournisseur						
18.1.1	Politique de sécurité pour les relations client/fournisseur	ISO 27001	X	X	Les mesures de sécurité de l'information, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers doivent être mises en œuvre, appliquées et tenues à jour par le tiers.	**cf. ISO/CEI 27001:2013 Annexe A. 15.1.1**

18.1.2	Mentions relatives à la sécurité de l'information lors de la contractualisation	ISO 27001	X	X	Les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services au moyen de traitement de l'information, doivent couvrir l'ensemble des exigences applicables en matière de sécurité de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 15.1.2**
18.1.3	Chaîne d'approvisionnement des produits et des services informatiques	ISO 27001	X	X	Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associée à la chaîne d'approvisionnement des produits et des services informatiques.	**cf. ISO/CEI 27001:2013 Annexe A. 15.1.3**
18.2 - Gestion des services des fournisseurs						
18.2.1	Supervision et revue des services des fournisseurs	ISO 27001	X	X	Surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.	**cf. ISO/CEI 27001:2013 Annexe A. 15.2.1**
18.2.2	Gestion des changements contractuels	ISO 27001	X	X	Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.	**cf. ISO/CEI 27001:2013 Annexe A. 15.2.2**

19 - Gestion des incidents						
19.1 - Gestion des incidents de sécurité						
19.1.1	Procédures et responsabilités	ISO 27001	X	X	Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.1**
19.1.2	Reporting sur les événements de sécurité	ISO 27001	X	X	Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.2**
19.1.3	Reporting sur les vulnérabilités de la part des parties internes et externes	ISO 27001	X	X	Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.3**
19.1.4	Évaluation et décision relatives aux événements de sécurité	ISO 27001	X	X	Des mécanismes doivent être mis en place, 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.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.4**
19.1.5	Réponse aux incidents	ISO 27001	X	X	Présenter les moyens mis en œuvre en matière de surveillance des systèmes visant à être alertés de toute atteinte à la sécurité du système d'information.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.5**
19.1.6	Capitalisation des incidents de sécurité	ISO 27001	X	X	Conserver les preuves de correction des incidents afin de constituer une base de connaissance et capitaliser sur les incidents résolus.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.6**

19.1.7	Collecte de preuves	ISO 27001	X	X	Définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.	**cf. ISO/CEI 27001:2013 Annexe A. 16.1.7**
20 - Aspects sécurité relatifs à la gestion de la continuité d'activité						
20.1 - Continuité de la sécurité de l'information						
20.1.1	Planification de la continuité d'activité	ISO 27001	X	X	Déterminer les exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre .	**cf. ISO/CEI 27001:2013 Annexe A. 17.1.1**
20.1.2	Implémentation du plan de continuité d'activité	ISO 27001	X	X	Établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.	**cf. ISO/CEI 27001:2013 Annexe A. 17.1.2**
20.1.3	Vérification, revue et évaluation du plan de continuité d'activité	ISO 27001	X	X	Les plans de continuité de la sécurité de l'information doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.	**cf. ISO/CEI 27001:2013 Annexe A. 17.1.3**
20.2 - Gestion de redondances						
20.2.1	Disponibilité des équipements	ISO 27001	X	X	Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.	**cf. ISO/CEI 27001:2013 Annexe A. 17.2.1**

21 - Conformité						
21.1 - Conformité aux exigences légales et contractuelles						
21.1.1	Identification des exigences contractuelles et réglementaires	ISO 27001	X	X	Pour chaque système d'information, toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, doivent être définies, documentées et mises à jour, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.	**cf. ISO/CEI 27001:2013 Annexe A. 18.1.1**
21.1.2	Propriété intellectuelle	ISO 27001	X	X	Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.	**cf. ISO/CEI 27001:2013 Annexe A. 18.1.2**
21.1.3	Protection des données stockées	ISO 27001	X	X	Les enregistrements importants doivent être protégés 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.	**cf. ISO/CEI 27001:2013 Annexe A. 18.1.3**
21.1.4	Vie privée et protection des données à caractère personnel	ISO 27001	X	X	La protection et la confidentialité de la vie privée et la protection des données à caractère personnel doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.	**cf. ISO/CEI 27001:2013 Annexe A. 18.1.4**

21.1.5	Contrôles cryptographiques réglementaires	ISO 27001	X	X	Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.	**cf. ISO/CEI 27001:2013 Annexe A. 18.1.5**
21.2 - Revues de sécurité						
21.2.1	Revue de sécurité indépendante	ISO 27001	X	X	Des réexamens réguliers et indépendants de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectués; de tels réexamens sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité.	**cf. ISO/CEI 27001:2013 Annexe A. 18.2.1**
21.2.2	Conformité à la Politique de sécurité interne et aux standards appliqués	ISO 27001	X	X	Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et s'assurer de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques, les normes de sécurité applicables et autres exigences de sécurité.	**cf. ISO/CEI 27001:2013 Annexe A. 18.2.2**
21.2.3	Revue de conformité technique	ISO 27001	X	X	Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.	**cf. ISO/CEI 27001:2013 Annexe A. 18.2.3**

22 - Mise en production des services						
22.1 - Planification de nouveaux services ou de services modifiés						
22.1.1	Définition des responsabilités pour la conception, le développement et les activités de transition	ISO 20000	X	X	Les autorités et les responsabilités liées à la conception, le développement et les activités de transition doivent être définies.	**cf. ISO/CEI 20000:2011 partie 5.2 (a)**
22.1.2	Présentation des activités exécutées par les fournisseurs de services et autres parties prenantes	ISO 20000	X	X	La planification des services doit inclure une référence aux activités devant être exécutées par le fournisseur de services et d'autres parties, y compris les activités à travers les interfaces du fournisseur de services.	**cf. ISO/CEI 20000:2011 partie 5.2 (b)**
22.1.3	Communication aux parties intéressées	ISO 20000	X	X	Présenter le plan ou les principes de communication visant à informer les personnes intéressées.	**cf. ISO/CEI 20000:2011 partie 5.2 (c)**
22.1.4	Ressources humaines, techniques, informationnelles et financières	ISO 20000	X	X	Décrire les ressources humaines, techniques, informationnelles et financières affectées à la prestation de service d'hébergeur de données de santé	**cf. ISO/CEI 20000:2011 partie 5.2 (d)**
22.1.5	Délais de mise en œuvre pour les activités planifiées	ISO 20000	X	X	Présenter les délais de mises en œuvre de la prestation de service.	**cf. ISO/CEI 20000:2011 partie 5.2 (e)**
22.1.6	Identification, évaluation et gestion des risques	ISO 20000	X	X	Le candidat doit démontrer que le processus de traitement des risques permet une identification, une évaluation et une gestion des risques.	**cf. ISO/CEI 20000:2011 partie 5.2 (f)**
22.1.7	Dépendances avec les autres services	ISO 20000			Présenter les liens et dépendances entre services.	**cf. ISO/CEI 20000:2011 partie 5.2 (g)**

22.1.8	Tests	ISO 20000		X	Les tests doivent être fixés et décrits pour les nouveaux services ou services modifiés et doivent être réalisés au moment du développement et préalablement à la mise en œuvre du service d'hébergement.	**cf. ISO/CEI 20000:2011 partie 5.2 (h)**
22.1.9	Critères d'acceptation du service	ISO 20000		X	Des critères d'acceptation du service doivent être fixés pour les nouveaux services ou services modifiés, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.	**cf. ISO/CEI 20000:2011 partie 5.2 (i)**
22.1.10	Information mesurable	ISO 20000			La fourniture de nouveaux services ou de services modifiés doit permettre la production de résultats mesurables et comparables entre eux.	**cf. ISO/CEI 20000:2011 partie 5.2 (j)**
22.2 - Conception et implémentation des nouveaux services ou des services modifiés						
22.2.1	Définition des responsabilités pour la fourniture de nouveaux services ou de services modifiés	ISO 20000			Les autorités et les responsabilités pour la fourniture de nouveaux services ou de services modifiés doivent être définies.	**cf. ISO/CEI 20000:2011 partie 5.3 (a)**
22.2.2	Présentation des activités exécutées par les fournisseurs de services, clients et autres parties	ISO 20000	X	X	La planification des services doit inclure une référence aux activités devant être exécutées par les fournisseurs de services et clients.	**cf. ISO/CEI 20000:2011 partie 5.3 (b)**
22.2.3	Ressources humaines	ISO 20000			Définir des exigences relatives à la gestion des ressources humaines, y compris les exigences concernant les formations, les compétences et l'expérience.	**cf. ISO/CEI 20000:2011 partie 5.3 (c)**
22.2.4	Exigences financières	ISO 20000			Définir les besoins en ressources financières pour la fourniture des nouveaux services ou services modifiés.	**cf. ISO/CEI 20000:2011 partie 5.3 (d)**

22.2.5	Nouvelles technologies	ISO 20000			Présenter les technologies permettant de fournir la prestation du service d'hébergeur de données de santé.	**cf. ISO/CEI 20000:2011 partie 5.3 (f)**
22.2.6	Accords contractuels	ISO 20000			Formaliser et documenter des nouveaux contrats ou contrats modifiés afin d'aligner les accords avec l'évolution des besoins de services.	**cf. ISO/CEI 20000:2011 partie 5.3 (g)**
22.2.7	Changements	ISO 20000			Identifier les changements sur le système de management des services.	**cf. ISO/CEI 20000:2011 partie 5.3 (h)**
22.2.8	SLA	ISO 20000			Définir et mettre en œuvre une nouvelle SLA ou modifier la SLA en place lors d'une modification de la prestation de service.	**cf. ISO/CEI 20000:2011 partie 5.3 (i)**
22.2.9	Catalogue de services	ISO 20000			Mettre à jour le catalogue de services lors de modifications de la prestation.	**cf. ISO/CEI 20000:2011 partie 5.3 (j)**
22.2.10	Informations et procédures mesurables	ISO 20000			Définir et mettre en place des procédures, mesures et informations utilisées lors de la fourniture des services.	**cf. ISO/CEI 20000:2011 partie 5.3 (k)**
23 - Fourniture des services						
23.1 - Gestion des niveaux de service						
23.1.1	Accords entre fournisseurs et clients	ISO 20000			Des accords entre fournisseurs et clients concernant les services et les niveaux de SLA à fournir doivent être définis.	**cf. ISO/CEI 20000:2011 partie 6.1**
23.2 - Description de services						
23.2.1	La performance du service	ISO 20000			Mettre en œuvre une mesure de la performance du service par rapport aux objectifs initialement prévus.	**cf. ISO/CEI 20000:2011 partie 6.2 (a)**

23.2.2	Informations pertinentes	ISO 20000			Des rapports de service doivent comporter des informations pertinentes sur les événements importants (incidents majeurs, déploiement de services, etc.) permettant d'assurer une exploitation optimale du service.	**cf. ISO/CEI 20000:2011 partie 6.2 (b)**
23.2.3	Charge de travail	ISO 20000			Les rapports de service doivent contenir des caractéristiques concernant la charge de travail.	**cf. ISO/CEI 20000:2011 partie 6.2 (c)**
23.2.4	Non-conformités	ISO 20000			Formaliser dans les rapports de service les non-conformités par rapport aux exigences du système de management des services et les causes préalablement identifiées.	**cf. ISO/CEI 20000:2011 partie 6.2 (d)**
23.2.5	Tendances en matière d'informations	ISO 20000			Mettre en œuvre une mesure de la performance du service par rapport aux objectifs initialement prévus.	**cf. ISO/CEI 20000:2011 partie 6.2 (e)**
23.2.6	Mesures de satisfaction des clients	ISO 20000			Intégrer dans les rapports de service les informations concernant la satisfaction des clients, les plaintes et les résultats de l'analyse des mesures et des plaintes.	**cf. ISO/CEI 20000:2011 partie 6.2 (f)**
23.3 - Continuité de services et gestion de la disponibilité						
23.3.1 - Exigences en termes de continuité et disponibilité de services						
23.3.1.1	Les droits d'accès à un service	ISO 20000			Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.	**cf. ISO/CEI 20000:2011 partie 6.3.1 (a)**
23.3.1.2	Le temps de réponse d'un service	ISO 20000			Les exigences de continuité et de disponibilité doivent comporter au moins les temps de réponse du service d'hébergement.	**cf. ISO/CEI 20000:2011 partie 6.3.1 (b)**
23.3.1.3	La disponibilité d'un service	ISO 20000			La disponibilité du service d'hébergement doit être définie par le prestataire.	**cf. ISO/CEI 20000:2011 partie 6.3.1 (c)**

23.3.2 - La continuité de service et disponibilité du service						
23.3.2.1	Les procédures en cas d'une perte importante d'un service	ISO 20000	X	X	Formaliser une procédure en cas de perte importante du service d'hébergement.	**cf. ISO/CEI 20000:2011 partie 6.3.2 (a)**
23.3.2.2	Les objectifs de disponibilité lorsque le plan est appliqué	ISO 20000	X	X	Le plan de continuité de service doit comprendre au moins les objectifs de disponibilité lorsque le plan est appliqué.	**cf. ISO/CEI 20000:2011 partie 6.3.2 (b)**
23.3.2.3	Les exigences de rétablissement	ISO 20000	X	X	Le plan de continuité de service doit contenir les exigences de rétablissement du service lors d'une interruption.	**cf. ISO/CEI 20000:2011 partie 6.3.2 (c)**
23.3.2.4	Les approches de retour aux conditions normales de travail	ISO 20000	X	X	Les approches de retour aux conditions normales de travail doivent être définies dans le plan de continuité.	**cf. ISO/CEI 20000:2011 partie 6.3.2 (d)**
23.3.3 - Supervision et tests de continuité et disponibilité de services						
23.3.3.1	Supervision de la disponibilité des services	ISO 20000	X	X	La disponibilité des services doit être surveillée, les résultats enregistrés et comparés avec les objectifs convenus. Les non-disponibilités imprévues doivent être étudiées et des mesures nécessaires doivent être prises en compte.	**cf. ISO/CEI 20000:2011 partie 6.3.3**
23.3.4 - Budgétisation et comptabilité des services						
23.3.4.1	Budgétisation et comptabilité	ISO 20000			Définir une politique de budgétisation et comptabilité des composants de services tels que les actifs (licences par exemple), les ressources partagées, les frais généraux, les capitaux et dépenses d'exploitation, etc.	**cf. ISO/CEI 20000:2011 partie 6.4 (a)**
23.3.4.2	Coûts indirects et directs aux services	ISO 20000			Définir une procédure décrivant la répartition des coûts indirects et la répartition des coûts directs aux services ainsi que la fourniture d'un coût global à chaque service.	**cf. ISO/CEI 20000:2011 partie 6.4 (b)**

23.3.4.3	Approbation et contrôle financier efficace	ISO 20000			Les approbations financières doivent être régulièrement contrôlées afin de s'assurer qu'ils répondent au cadre réglementaire et législatif et que les contrôles financiers sont pertinents.	**cf. ISO/CEI 20000:2011 partie 6.4 (c)**
23.3.5 - Gestion de la capacité						
23.3.5.1	Plan de capacité	ISO 20000	X	X	Le prestataire de services doit créer, mettre en œuvre et maintenir un plan de capacité traitant des aspects humains, financiers, techniques et informationnels.	**cf. ISO/CEI 20000:2011 partie 6.5 (a)**
23.3.5.2	Exigences relatives à la disponibilité, la continuité et les niveaux de services	ISO 20000	X	X	Le plan de capacité doit identifier les impacts potentiels et définir les exigences relatives à la disponibilité, la continuité de service et les niveaux de services.	**cf. ISO/CEI 20000:2011 partie 6.5 (b)**
23.3.5.3	Délais, seuils et coûts de mise à niveau de la capacité d'un service	ISO 20000	X	X	Le plan de capacité doit définir les délais, seuils et coûts de mise à niveau de la capacité du service d'hébergement de données de santé.	**cf. ISO/CEI 20000:2011 partie 6.5 (c)**
23.3.5.4	Impacts réglementaires	ISO 20000			Identifier les impacts potentiels des modifications statutaires, réglementaires, contractuels et organisationnels.	**cf. ISO/CEI 20000:2011 partie 6.5 (d)**
23.3.5.5	Identifications de l'impact potentiel des nouvelles technologies et des nouvelles techniques	ISO 20000			Identifier l'impact potentiel des nouvelles technologies et des nouvelles techniques.	**cf. ISO/CEI 20000:2011 partie 6.5 (e)**
23.3.5.6	Mise en place des procédures permettant l'analyse prédictive	ISO 20000			Mettre en œuvre des procédures permettant une analyse prédictive de la capacité du service d'hébergement.	**cf. ISO/CEI 20000:2011 partie 6.5 (f)**

24 - Exigences spécifiques santé						
24.1 - Consentement et choix						
24.1.1	Obligation de coopérer en ce qui concerne les droits des informations personnelles	ISO 27018	X	X	L'hébergeur doit mettre en œuvre des mesures pour aider son client à respecter ses obligations vis-à-vis des personnes concernées par les données à caractère personnel (droit d'accès, de rectification, de suppression).	**cf. ISO/CEI 27018:2014 Annexe A. 1.1**
24.2 - Légitimité et spécification						
24.2.1	Finalité des processus de traitement	ISO 27018		X	Les informations à caractère personnel hébergées dans le cadre d'un contrat ne doivent pas être traitées à des fins autres que celles définies avec le client.	**cf. ISO/CEI 27018:2014 Annexe A. 2.1**
24.2.2	Utilisation commerciale de données de santé à caractère personnel	ISO 27018		X	Les informations à caractère personnel hébergées ne doivent pas être traitées à des fins publicitaires ou commerciales sans le consentement exprès de la personne propriétaire des informations.	**cf. ISO/CEI 27018:2014 Annexe A. 2.2**
24.3 - Minimisation des données						
24.3.1	Effacement sécurisé des fichiers temporaires	ISO 27018			Les fichiers temporaires et les documents doivent être effacés ou détruits après une période définie et documentée.	**cf. ISO/CEI 27018:2014 Annexe A. 4.1**
24.4 - Limite de l'utilisation, rétention et divulgation des données de santé						
24.4.1	Notification lors de la communication de données à caractère personnel	ISO 27018	X	X	L'hébergeur est tenu d'informer son client de toute requête légale d'accès à des données à caractère personnel, dans le respect de la règlementation.	**cf. ISO/CEI 27018:2014 Annexe A. 5.1**
24.4.2	Enregistrement des traces de communication de données à caractère personnel	ISO 27018	X	X	Toute communication des données à caractère personnel à un tiers doit être enregistrée (l'enregistrement doit contenir l'identification de ce qui a été révélé, à qui et à quel moment).	**cf. ISO/CEI 27018:2014 Annexe A. 5.2**

24.5 - Transparence						
24.5.1	Divulgation d'information personnelle lors de sous-traitance	ISO 27018	X	X	Le recours à des sous-traitants par l'hébergeur afin de traiter des informations à caractère personnel doit être communiqué au client.	**cf. ISO/CEI 27018:2014 Annexe A. 7.1**
24.6 - Responsabilité						
24.6.1	Notification d'une violation de données impliquant des informations personnelles	ISO 27018	X	X	L'hébergeur doit au plus tôt notifier le client dans les cas d'accès non autorisé à des informations personnelles pouvant provoquer une altération, divulgation ou perte d'intégrité de l'information.	**cf. ISO/CEI 27018:2014 Annexe A. 9.1**
24.6.2	Période de conservation des politiques et des directives de sécurité	ISO 27018	X	X	Des copies des politiques de sécurité et procédures opérationnelles doivent être conservées en cas de changement de celles-ci.	**cf. ISO/CEI 27018:2014 Annexe A. 9.2**
24.6.3	Gestion des informations personnelles	ISO 27018	X	X	L'hébergeur doit définir une politique de gestion des données à caractère personnel pour la restitution, le transfert et la destruction des données à caractère personnel. Il doit communiquer cette politique à ses clients.	**cf. ISO/CEI 27018:2014 Annexe A. 9.3**
24.7 - Sécurité de l'information						
24.7.1	Les accords de confidentialité ou de non-divulgation	ISO 27018	X	X	Les personnes sous responsabilité de l'hébergeur ayant un accès aux informations à caractère personnel doivent être sujettes à un devoir de confidentialité.	**cf. ISO/CEI 27018:2014 Annexe A. 10.1**
24.7.2	Restriction de copie matérielle	ISO 27018			La création de copies papier de documents contenant des informations à caractère personnel doit être restreinte.	**cf. ISO/CEI 27018:2014 Annexe A. 10.2**
24.7.3	Contrôle et exploitation de la restauration de données	ISO 27018	X	X	L'hébergeur doit formaliser et tracer les actions de restauration de données.	**cf. ISO/CEI 27018:2014 Annexe A. 10.3**

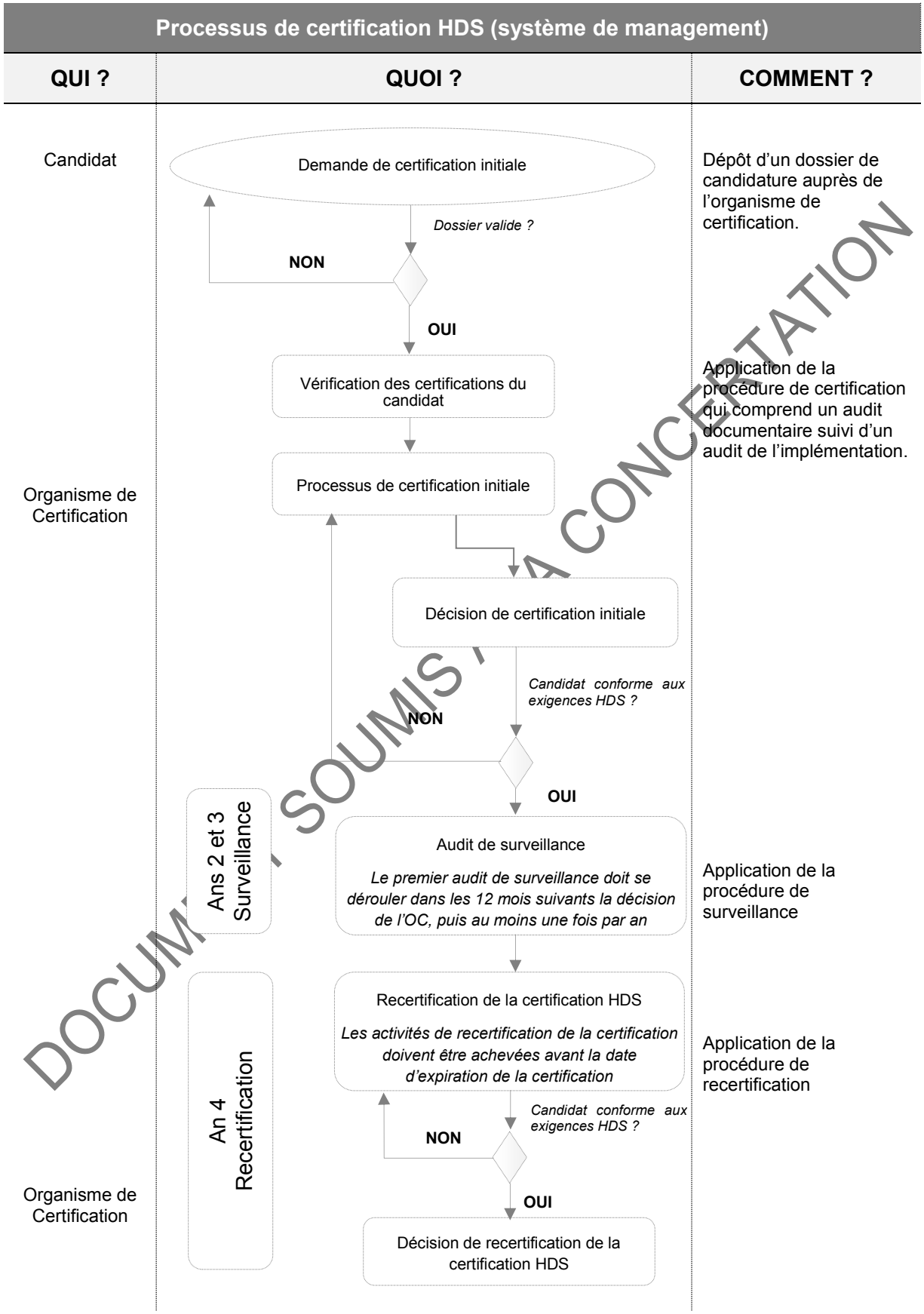
24.7.4	Protection des données présentes sur un support de stockage quittant le lieu d'hébergement	ISO 27018	X	X	Les informations personnelles présentent sur des supports amovibles doivent faire l'objet d'une procédure d'autorisation de sortie et ne doivent pas être accessibles aux personnes non autorisées.	**cf. ISO/CEI 27018:2014 Annexe A. 10.4**
24.7.5	Utilisation de support de stockage portable non chiffré	ISO 27018	X	X	Les supports de stockage portables non chiffrés ne doivent pas être utilisés sauf si cela s'avère inévitable. Cet usage doit alors être documenté.	**cf. ISO/CEI 27018:2014 Annexe A. 10.5**
24.7.6	Chiffrement des données personnelles transmises sur des réseaux publics	ISO 27018	X	X	Toute information à caractère personnel transmise via un réseau public doit faire l'objet d'un chiffrement.	**cf. ISO/CEI 27018:2014 Annexe A. 10.6**
24.7.7	Destruction des supports papier	ISO 27018			Les supports papier contenant des données à caractère personnel doivent être détruits avec des moyens appropriés : déchiqueteuse, incinération, etc.	**cf. ISO/CEI 27018:2014 Annexe A. 10.7**
24.7.8	Utilisation d'identifiant unique	ISO 27018		X	Si plusieurs personnes ont accès aux données à caractère personnel, chacune doit disposer d'un identifiant spécifique à des fins d'identification, d'authentification et d'autorisation.	**cf. ISO/CEI 27018:2014 Annexe A. 10.8**
24.7.9	Gestion des utilisateurs autorisés	ISO 27018	X	X	L'hébergeur doit maintenir la liste des utilisateurs ou profils d'utilisateurs ayant accès au système d'information.	**cf. ISO/CEI 27018:2014 Annexe A. 10.9**
24.7.10	Traces des administrateurs	ISO 27018	X	X	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.	**cf. ISO/CEI 27018:2014 Partie 12.4.3**
24.7.11	Gestion des identifiants	ISO 27018		X	Un identifiant désactivé ou expiré ne doit pas être transmis à une autre personne.	**cf. ISO/CEI 27018:2014 Annexe A. 10.10**

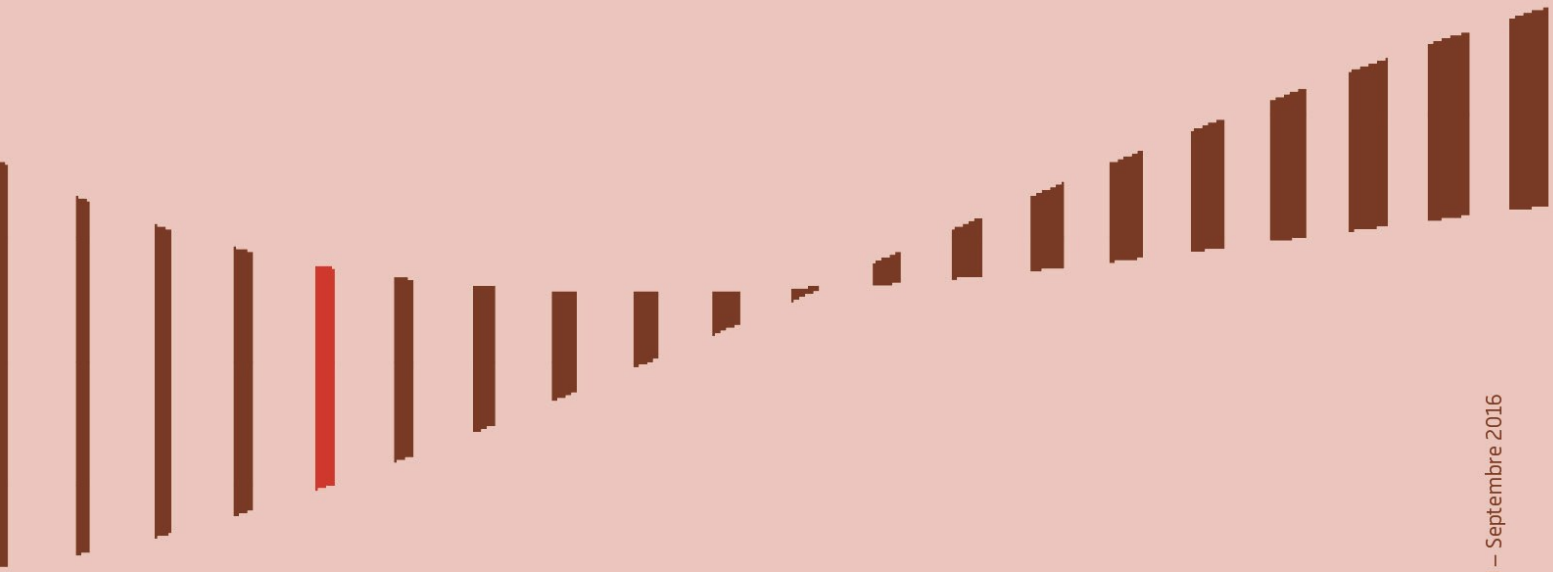
24.7.12	Clauses contractuelles	ISO 27018	X	X	Les contrats entre l'hébergeur et son client doivent comporter des clauses permettant la vérification de la mise en œuvre effective des mesures de sécurité par l'hébergeur et la vérification de l'utilisation des données à caractère personnel.	**cf. ISO/CEI 27018:2014 Annexe A. 10.11**
24.7.13	Sous-traitance du traitement des données personnelles	ISO 27018		X	Les contrats entre l'hébergeur et ses sous-traitants doivent comporter des mesures techniques et organisationnelles permettant de garantir un niveau de sécurité identique.	**cf. ISO/CEI 27018:2014 Annexe A. 10.12**
24.7.14	Réutilisation des espaces de stockage	ISO 27018	X	X	L'hébergeur doit s'assurer que lorsqu'un espace de stockage est attribué à un client, aucune donnée à caractère personnelle précédemment présente dans cet espace n'est accessible.	**cf. ISO/CEI 27018:2014 Annexe A. 10.13**
24.8 - Respect de la vie privée						
24.8.1	Lieux d'hébergement	ISO 27018	X	X	L'hébergeur doit spécifier et documenter les pays dans lesquels les informations à caractère personnel seront hébergées.	**cf. ISO/CEI 27018:2014 Annexe A. 11.1**
24.8.2	Destination prévue des données personnelles	ISO 27018	X	X	Les transferts de données de santé à caractère personnel doivent faire l'objet de contrôle afin de s'assurer de l'identité du destinataire.	**cf. ISO/CEI 27018:2014 Annexe A. 11.2**
24.9 - Vérification de la conformité des applications						
24.9.1	Conformité aux référentiels opposables de la PGSSI-S	Spécifique Santé	X	X	Informer le client qu'il doit se conformer à la PGSSI-S et conserver la déclaration de conformité.	<u>Hébergeur d'infrastructure et hébergeur infogérant</u> S'assurer que le candidat informe ses clients de leurs obligations de conformité à la PGSSI-S.

24.9.2	Critères de vérification de l'application	Spécifique Santé		X	Des critères d'acceptation du service doivent être fixés pour les nouveaux services ou services modifiés, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.	Hébergeur infogérant - S'assurer que l'hébergeur a mis en place une méthodologie de vérification des applications qu'il héberge. - Vérifier que l'hébergeur a formalisé une procédure permettant de définir les pré-requis à l'hébergement et une procédure de vérification de ces prés requis (ces pré-requis doivent comporter, a minima, le manuel d'installation et le manuel d'exploitation). - Vérifier que l'hébergeur a formalisé un processus structuré de test et de validation permettant d'apporter la preuve objective que le futur service ne perturbera pas les performances globales du système hébergé (saturation de CPU, saturation espace mémoire, etc.).
24.10 - Exigences Complémentaires						
24.10.1	Externalisation des sauvegardes	Spécifique Santé		X	En cas d'externalisation des sauvegardes (quel qu'en soit le support), définir les moyens permettant d'assurer la confidentialité et l'intégrité des données de santé.	Hébergeur infogérant : En cas d'externalisation des supports de sauvegarde, présenter : - Les procédures d'externalisation; - Les moyens permettant d'assurer la confidentialité et l'intégrité des données contenues sur les supports sur ce lieu et pendant le transport.

24.10.2	Accès aux traces pour les personnes concernées	Spécifique Santé		X	Définir les moyens techniques et organisationnels permettant l'accès aux données de traçabilité par les personnes concernées par les données hébergées.	Hébergeur Infogérant : - S'assurer que le processus de traitement des demandes d'accès par les personnes concernées est formalisé et mis en œuvre. - Présenter les habilitations nécessaires pour accéder aux données de traçabilité. - Présenter les moyens techniques et organisationnels permettant l'accès aux données de traçabilité, pour toute personne intervenant sur le système d'information (personnel de l'hébergeur ou prestataire extérieur)
24.10.3	Liste des contacts à fournir à l'organisme de certification	Spécifique Santé	X	X	Fournir à l'organisme de certification une liste des contacts client et la maintenir à jour.	Hébergeur d'infrastructure et infogérant : Vérifier que l'hébergeur a formalisé et maintient à jour une liste de contact à fournir à l'organisme de certification.

Annexe B : Processus de certification HDS





Agence des Sytèmes d'Information Partagés de Santé
9, rue Georges Pitard
Standard : 01 58 45 32 50
Du lundi au vendredi (hors jours fériés)
de 8h30 à 13h et de 14h à 17h
esante.gouv.fr