

## SOMMAIRE

<b>1</b>	<b>INTRODUCTION.....</b>	<b>2</b>
<b>2</b>	<b>EXIGENCES GENERALES SUR LES LOGICIELS.....</b>	<b>3</b>
<b>3</b>	<b>IDENTITES.....</b>	<b>3</b>
<b>4</b>	<b>AUTHENTIFICATION ET SINGLE SIGN ON.....</b>	<b>4</b>
4.1	GESTION DES HABILITATIONS.....	4
<b>5</b>	<b>TRACABILITE.....</b>	<b>5</b>
<b>6</b>	<b>PROTECTION DES SYSTEMES.....</b>	<b>5</b>
<b>7</b>	<b>CRYPTOGRAPHIE.....</b>	<b>6</b>
<b>8</b>	<b>MAINTENANCE ET TELEMANTENANCE .....</b>	<b>6</b>
<b>9</b>	<b>SPECIFICATIONS WI-FI.....</b>	<b>8</b>
<b>10</b>	<b>PROTECTION DES DONNEES MEDICALES .....</b>	<b>8</b>
<b>11</b>	<b>CAS PARTICULIERS SELON PERIMETRE.....</b>	<b>8</b>
11.1	CAS DE MOYENS MOBILES :.....	8
11.2	CAS DES DISPOSITIF CONNECTES (BIOMEDICAL) .....	8
11.2.1	<i>Gestion des configurations.....</i>	<i>9</i>
11.2.2	<i>Sécurité Physique .....</i>	<i>10</i>
11.2.3	<i>Exploitation et communications .....</i>	<i>10</i>
11.2.4	<i>Maîtrise des accès.....</i>	<i>12</i>
11.2.5	<i>Développement et maintenance des logiciels.....</i>	<i>12</i>
11.2.6	<i>Conformité.....</i>	<i>13</i>
11.3	CAS DE SERVICE HEBERGE EN DEHORS DU SI DE LA DSI DE L'ETABLISSEMENT DE SANTÉ ET DE PRESTATION DE TYPE SAAS/IAAS ET INFOGERANCE DANS LE SI DE L'ETABLISSEMENT .....	13
<b>12</b>	<b>REFERENCES DOCUMENTAIRES .....</b>	<b>16</b>
<b>13</b>	<b>GLOSSAIRE DES TERMES EMPLOYES.....</b>	<b>16</b>

## **1 INTRODUCTION**

Les solutions informatiques déployées au sein du Système d'Information (noté SI) de l'ETABLISSEMENT DE SANTÉ doivent :

- Satisfaire les exigences de sécurité informatique définies dans le présent référentiel de sécurité de l'ETABLISSEMENT DE SANTÉ.
- Respecter les préconisations en matière de sécurité de l'ANS (Agence du Numérique en Santé), de l'ANSSI (Agence Nationale de la Sécurité des Systèmes de l'Information) et du Ministère de la santé (PSSI –MCAS qui pourra être fournie sur demande).
- Respecter les exigences du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Respecter les exigences complémentaires propres à des systèmes critiques spécifiques.

Le titulaire, éditeur de logiciel ou intégrateur d'une application du périmètre de Santé, doit être engagé dans la démarche de certification Qualité Hôpital Numérique (QHN) soit en étant certifié QHN ou soit engagé dans une démarche de certification QHN.

Le titulaire devra respecter les exigences de sécurité de ce référentiel. Dans le cas où il n'est pas en capacité de respecter une exigence au moment de la réponse à la consultation, il devra préciser son plan d'action et la date à laquelle la mise en œuvre de ce plan sera effective.

Les **recommandations référencées qui sont à décrire dans l'annexe SSI sont des orientations techniques** fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles font partie de l'annexe au format Excel et sont notées **R** comme **Recommandée**. Elles doivent obligatoirement être renseignées par le titulaire pour décrire sa réponse. Toutes les cases « description de la prise en charge » doivent être renseignées. Si une recommandation n'est pas applicable la mention N/A est inscrite et doit être justifiée. Elles seront prises en compte dans l'évaluation technique de l'offre.

## **2 EXIGENCES GENERALES SUR LES LOGICIELS**

Ref.	Exigence de sécurité
O-2.1	Le titulaire s'engage à fournir et maintenir la liste exhaustive des logiciels et éventuels équipements installés. La cartographie doit être documentée (niveau de version, prérequis, ...) et doit contenir les informations détaillant chaque logiciel ainsi que les interactions entre eux. Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent de la DSI de L'ETABLISSEMENT DE SANTÉ le Document d'Architecture Technique (DAT) et le Document d'Exploitation (DEX).
O-2.2	Pour tout ce qui est fourni au titre de l'offre, le titulaire s'engage à acquérir et à concéder à L'ETABLISSEMENT DE SANTÉ l'ensemble des licences d'utilisation nécessaires à son bon fonctionnement. Si nécessaire, il détaillera les conditions spécifiques ou exclusions. Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance...).
O-2.3	Le titulaire s'engage à n'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché. Si des logiciels complémentaires sont nécessaires ils devront être validés par la DSI.
O-2.4	Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. Ils devront aussi respecter les exigences de sécurité décrites dans ce document.
O-2.5	Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité décrites dans ce document.
O-2.6	Pour les logiciels de type SaaS (Software as a Service : logiciel hébergé), la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité.
O-2.7	Les personnels du titulaire devront respecter la Charte d'Accès et d'Utilisation du Système d'Information de l'établissement lors de toute intervention à l'installation ou en maintenance. Le titulaire s'engage à en informer ses personnels.
O-2.8	Toute opération réalisée par le titulaire et ses personnels lors de l'installation devra respecter les mêmes exigences que celles décrites dans le chapitre Maintenance et Télémaintenance durant son exécution.
O-2.9	Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité. Les clauses spécifiques au RGPD fournies en annexe dédiée doivent être signées par le représentant légal du sous-traitant.
O-2.10	Pour les applications web le titulaire s'engage à fournir avec l'offre un audit externe de sécurité de type top 10 de l'OWASP prouvant l'absence de faille de sécurité.

## **3 IDENTITES**

Ref.	Exigence de sécurité
	Aucune exigence mais des recommandations sont présentes en annexe.

#### **4 AUTHENTIFICATION ET SINGLE SIGN ON**

Ref.	Exigence de sécurité
O-4.1	Sauf disposition spécifique du CCTP, l'ETABLISSEMENT DE SANTÉ impose une compatibilité avec une authentification unique (Single Sign On) au travers de son système SSO utilisant une identité de domaine portée par les protocoles communément utilisés en environnement Windows. La politique de sécurité de l'authentification de l'ETABLISSEMENT DE SANTÉ s'applique de fait aux comptes d'accès au système. Si une gestion de comptes utilisateurs et de mot de passe locale au système est spécifiée dans le CCTP, le système doit permettre d'imposer une politique de mots de passe robustes en accord avec la politique de sécurité de l'ETABLISSEMENT DE SANTÉ (8 à 12 caractères selon le niveau de privilège comprenant Majuscules, minuscules, chiffres et caractères spéciaux / délais de renouvellement / historisation).
O-4.2	Les mots de passe des comptes nécessaires à l'administration de la solution doivent pouvoir être modifiés par l'ETABLISSEMENT DE SANTÉ.
O-4.3	Pour les applications web exposées sur internet et qui intégreront une authentification et/ou une gestion des comptes : Les pages réservées à l'authentification et à la création de comptes doivent intégrer un dispositif de prémunition contre l'usage de robots (type test de défi-réponse). Des mécanismes empêchant de réutiliser des informations de connexion ou de session pour contourner l'authentification doivent être en place.
O-4.4	Pour les applications web exposées sur internet et qui intégreront une authentification et/ou une gestion des comptes, les mécanismes d'authentification doivent être adaptés à la criticité des données Une authentification forte est notamment exigée pour l'accès à des données de santé par carte CPS ou équivalent et pour toutes données dites sensibles au sens du RGPD (sauf disposition contraire du CCTP qui conduirait l'ETABLISSEMENT DE SANTÉ à prendre en charge une authentification forte en préalable à l'accès à l'application objet du marché : cas d'un portail d'authentification en amont de l'application).
O-4.5	La politique de sécurité de l'authentification sera celle du SSO de l'ETABLISSEMENT DE SANTÉ. Si la solution impose la gestion de comptes utilisateurs, ils devront pouvoir suivre la politique d'authentification de l'ETABLISSEMENT DE SANTÉ.

##### **4.1 GESTION DES HABILITATIONS**

L'ETABLISSEMENT DE SANTÉ a pris le parti de maintenir un référentiel central de gestion des habilitations sur son Système d'Information.

O-4.1.1	Sauf disposition spécifique du CCTP, l'ETABLISSEMENT DE SANTÉ impose une gestion des habilitations à partir de son référentiel d'identité. L'interface destinée à gérer les habilitations dans l'application sera fournie et maintenue par le titulaire. Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent de la DSI de l'ETABLISSEMENT DE SANTÉ le Document de spécifications fonctionnelles et techniques de l'interface.
---------	--

Ref.	Exigence de sécurité
	Des recommandations complémentaires sont présentes en annexe.

## **5 TRACABILITE**

Ref.	Exigence de sécurité
O-5.1	La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite dans l'annexe sécurité Recommandation R-5.1)
O-5.2	Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec dans le système fourni.
O-5.3	Dans le cadre de systèmes gérant des données à caractère personnel au sens du RGPD les traces de consultation et de modification sont obligatoires dans le système fourni.
O-5.4	Les traces produites devront être accessibles par l'outil de centralisation des traces de l'ETABLISSEMENT DE SANTÉ dans un format et un mode d'accès rendus possibles et décrits avec la fourniture du système par le titulaire (ATNA : format IHE, syslog, requête dans une base de données à fournir, fichier à décrire).
O-5.5	Les traces doivent pouvoir être épurée au-delà du temps légal de rétention
O-5.6	Le titulaire s'engage une fois le marché obtenu à formaliser avec le référent de la DSI de L'ETABLISSEMENT DE SANTÉ le détail des traces générées, leur sécurisation et leur épuración dans le Document d'Architecture Technique (DAT) et le Document d'Exploitation (DEX).

## **6 PROTECTION DES SYSTEMES**

Ref.	Exigence de sécurité
O-6.1	<p>Le titulaire s'engage à mettre en œuvre les dispositifs et paramétrages nécessaires pour prémunir ses systèmes contre les attaques virales et intrusives selon l'une des formes suivantes :</p> <ul style="list-style-type: none"> <li>• Déploiement de ses propres utilitaires et politiques de mise à jour.</li> <li>• Intégration de ses dispositifs dans la démarche sécurité de l'ETABLISSEMENT DE SANTÉ en installant l'antivirus de l'ETABLISSEMENT DE SANTÉ et en inscrivant ses systèmes dans les exigences de gestion des correctifs de sécurité en vigueur pour le reste du SI.</li> <li>• Les types de fichiers nécessitant une exclusion d'analyse par l'antivirus conditionnant le bon fonctionnement doivent être communiqués avant installation pour décider d'un éventuel complément de sécurité</li> <li>• A défaut, ou en cas d'insuffisance de l'analyse antivirus et de la gestion des correctifs de sécurité une solution de sécurité externe en interface avec le dispositif objet du marché sera installée (à la charge du titulaire ou de l'ETABLISSEMENT DE SANTÉ selon disposition du CCTP) selon les préconisations du RSSI de l'ETABLISSEMENT DE SANTÉ (équipement de type pare-feu avec antivirus et/ou logiciel de type EDR End Point Detection and Réponse).</li> </ul> <p>De fait, en cas d'intrusion ou de contamination, le titulaire est responsable de la vulnérabilité de ses systèmes vis à vis des définitions virales et correctifs publics.</p>

## 7 Cryptographie

Ref.	Exigence de sécurité
O-7.1	Dans le cas d'applications web publiées sur internet comme sur l'intranet, l'usage de SSL à un niveau de version conforme aux exigences de sécurité des données concernées est impératif. Le titulaire devra recourir à des certificats adaptés à la criticité du service fournis par l'ETABLISSEMENT DE SANTÉ.
O-7.2	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.
O-7.3	De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux standards du marché, et au Référentiel Général de Sécurité (RGS).
O-7.4	Si les logiciels fournis intègrent la gestion de données à caractère personnel au sens du RGPD au sein de systèmes de gestion de base de données standards (Microsoft SQL, Oracle, Mysql, ...) qui proposent le chiffrement des données, celui-ci devra être supporté par le titulaire et activable à décision de l'ETABLISSEMENT DE SANTE. Les algorithmes et clefs de chiffrement seront conformes aux préconisations de la CNIL et au RGS.

## 8 Maintenance et Télémaintenance

Lorsqu'une télémaintenance est prévue par le titulaire, des exigences strictes doivent être prises en compte :

Ref.	Exigence de sécurité
O-8.1	Pour ce qui concerne la remontée d'informations issues des dispositifs maintenus vers le site de diagnostic du titulaire, cet envoi doit être décrit précisément en indiquant toutes les données transférées avant l'installation du système. Cet usage exclusif à des fins de surveillance du maintien en condition opérationnelle et l'absence de données personnelles directement ou indirectement liées à nos patients (ou autres personnes liées au traitement) doivent être garantis. Cette remontée d'information devra utiliser des protocoles sécurisés, être tracée et passer par les dispositifs de sécurité de l'ETABLISSEMENT DE SANTÉ : passerelles de contrôle d'accès à internet ou VPN IPSEC site à site avec le site de télédiagnostic (cette dernière option est vivement souhaitée).
O-8.2	La connexion de télémaintenance doit se faire via la passerelle Internet sécurisée mise à disposition par l'ETABLISSEMENT DE SANTÉ (VPN IPSEC uniquement, en conformité avec les recommandations de l'ANSSI)). La demande de ce VPN devra suivre la procédure de l'ETABLISSEMENT DE SANTÉ.
O-8.3	Au niveau des postes de travail standard de l'ETABLISSEMENT DE SANTÉ, aucun outil de prise de contrôle à distance ne peut être installé dans le cadre d'une application. Le seul outil de prise de contrôle à distance autorisé est celui servant à l'administration système gérée par la DSI DE L'ETABLISSEMENT DE SANTÉ.
O-8.4	Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (données et logiciels)
O-8.5	L'ETABLISSEMENT DE SANTÉ se réserve le droit de faire (ou de faire faire) des contrôles de sécurité de façon périodique ou ponctuelle chez le titulaire afin de s'assurer que le niveau de sécurité requis est conforme aux exigences de sécurité du présent référentiel.
O-8.6	Le titulaire doit garantir l'application d'une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance.

Ref.	Exigence de sécurité
O-8.7	Les données à caractère personnel ou technique (configuration des équipements) de l'ETABLISSEMENT DE SANTÉ exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée).
O-8.8	L'intervention de maintenance doit être encadrée par un règlement, un contrat ou une convention entre l'ETABLISSEMENT DE SANTÉ et le titulaire, définissant les engagements de chacun, les modalités pratiques, ... Ce document devra être fourni au RSSI avant de démarrage du système
O-8.9	Le titulaire s'engage sur la sécurité de la prestation, son représentant légal devra signer l'engagement du titulaire de maintenance fourni par la DSI DE L'ETABLISSEMENT DE SANTÉ rappelant la confidentialité des données et l'engageant à informer ses personnels que tous les accès et actions sont tracés.
O-8.10	Il est de la responsabilité du titulaire de restreindre les accès physiques et logiques de ses postes aux seules personnes autorisées (par sensibilisation et mise à disposition de moyens de sécurité adéquats).
O-8.11	Il est de la responsabilité du titulaire de connaître en toutes circonstances l'identité de toute personne qui se connecte ou s'est connectée sur la plateforme de télémaintenance et d'en assurer la traçabilité (cette traçabilité pourra être communiquée sur demande de l'ETABLISSEMENT DE SANTÉ).
O-8.12	Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées en application du principe de minimisation des données.
O-8.13	Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs fournis et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés.
O-8.14	Le titulaire s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge.
O-8.15	Le titulaire doit fournir un rapport détaillé de l'intervention effectuée, un modèle pourra être fourni.
O-8.16	Si l'ETABLISSEMENT DE SANTÉ dispose d'un bastion d'administration ou le met en place ultérieurement, le titulaire s'engage à l'utiliser pour accéder aux systèmes qu'il devra maintenir ou exploiter (de fait l'accès direct aux serveurs et applications est interdit). Selon les besoins d'intervention l'accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par la DSI DE L'ETABLISSEMENT DE SANTÉ à la demande (du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance). Si l'établissement ne dispose pas d'un bastion d'administration, le cas d'utilisation d'un bastion équivalent du titulaire pourra être étudié s'il apporte des garanties de protection, de traçabilité, de preuve opposable et d'accès avec la possibilité d'audit DE L'ETABLISSEMENT DE SANTÉ (une description précise devra être fournie).
O-8.17	Le titulaire doit informer le RSSI DE L'ETABLISSEMENT DE SANTÉ de tout incident de sécurité concernant ses dispositifs connectés ou son SI d'entreprise pouvant impacter son matériel, le service ou les données de L'ETABLISSEMENT DE SANTÉ. Le titulaire s'engage à mobiliser les ressources nécessaires pour assurer le traitement de l'incident de sécurité sur les dispositifs déployés dans L'ETABLISSEMENT DE SANTÉ. Si l'incident concerne un traitement relatif RGPD les dispositions relatives au traitement des incidents s'appliqueront aussi.



## 9 SPECIFICATIONS WI-FI

Ref.	Exigence de sécurité
O-9.1	Le chiffrement et l'intégrité des informations circulant sur le réseau doivent être assurés par la mise en place sur les équipements concernés du mécanisme WPA2 ou ultérieurs garantissant le plus haut niveau de sécurité (version de la norme IEEE 802.11i certifiée par la Wifi Alliance).
O-9.2	Pour l'authentification, l'association de WPA2 ou supérieur (« WPA2 – Entreprise ») avec un serveur d'authentification 802.1X (Radius) par le biais du protocole EAP est demandée. Pour éviter la gestion redondante des comptes, le serveur devra s'appuyer sur l'annuaire LDAP centralisé de l'établissement. Pour des équipements spécifiques qui seraient incompatibles avec ce paramétrage, une description des niveaux possibles et des compléments de sécurisation doivent être fournis pour évaluation d'un mode de prise en charge de la sécurité acceptable (à renseigner dans l'annexe SSI R-9.1)

## 10 PROTECTION DES DONNEES MEDICALES

Ref.	Exigence de sécurité
O-10.1	Le titulaire et son personnel comme le personnel de l'ETABLISSEMENT DE SANTÉ sont soumis à un engagement de confidentialité conformément aux préconisations de la CNIL et au Code de la Santé Publique.

### Article L1110-4 du Code de la Santé Publique

*....Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.*

Ref.	Exigence de sécurité
O-10.2	En conséquence, notamment, les jeux de données fournies par l'ETABLISSEMENT DE SANTÉ sont strictement confidentiels et sont liés au secret professionnel.

## 11 CAS PARTICULIERS SELON PERIMETRE

### 11.1 CAS DE MOYENS MOBILES :

Ref.	Exigence de sécurité
O-11.1.1	Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent être remises à l'ETABLISSEMENT DE SANTÉ.

### 11.2 CAS DES DISPOSITIF CONNECTES (BIOMEDICAL)

Les exigences contenues dans ce chapitre sont issues du guide pratique [[G\\_DISP\\_CON\\_SIS](#)].

On entend par **dispositif connecté** tout dispositif médical particulier connecté à un SI de Santé directement ou à distance (par exemple via Internet). Ce dispositif intègre des matériels (serveurs, périphériques, dispositifs électroniques spécifiques, ...), des logiciels (système d'exploitation, logiciels embarqué, micrologiciel) et des données (fichiers, bases de données, ...) et assure dans un processus de soin, une fonction de traitement médical, d'analyse médicale, de surveillance, de diagnostic ou de



supervision. Les recommandations européennes de cyber sécurité pour les dispositifs médicaux connectés [MDCG 2019-16] pourront être prises en compte  
<https://ec.europa.eu/docsroom/documents/41863>.

### 11.2.1 Gestion des configurations

Ref.	Exigence de sécurité
O-11.2.1.1	Le titulaire doit identifier dans sa documentation (accessible par exemple au travers d'un espace client sur Internet) l'ensemble des composants matériels (serveurs, périphériques, ...) et logiciels (versions des logiciels, systèmes d'exploitation, bases de données, ...) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques.
O-11.2.1.2	Le titulaire doit identifier dans sa documentation l'ensemble des spécifications portant sur le poste d'administration/utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques, ...).

### 11.2.2 Sécurité Physique

Ref.	Exigence de sécurité
O-11.2.2.1	Le titulaire doit identifier dans sa documentation l'ensemble des mesures de sécurité physique (sécurité des locaux, clés du coffret protégeant le dispositif connecté, contraintes d'environnement notamment compatibilité électromagnétique avec les réseaux WiFi ou de téléphone mobile, sécurité des câblages...) préconisées pour la mise en œuvre du système dispositif connecté au sein de son environnement d'usage.

### 11.2.3 Exploitation et communications

Ref.	Exigence de sécurité
	<b>Vérification du bon fonctionnement</b>
O-11.2.3.1	Les dispositifs connectés doivent disposer d'une fonction permettant de garantir l'intégrité des logiciels et des données sensibles du dispositif au démarrage du dispositif et lors de son fonctionnement. La date de dernière modification des logiciels et des données sensibles dont celles inhérentes à l'appareil est présentée lors de la connexion des utilisateurs.
	<b>Mise à jour des dispositifs</b>
O-11.2.3.2	Les dispositifs connectés et les logiciels des postes utilisateurs doivent disposer d'une fonction de mise à jour sécurisée des logiciels (logiciels, micrologiciel) permettant de garantir l'origine et l'intégrité des mises à jour.
O-11.2.3.3	Les dispositifs connectés doivent vérifier la bonne installation d'une mise à jour logicielle avec une possibilité de retour arrière en cas de dysfonctionnement détecté.
	<b>Protection contre les codes malveillants</b>
O-11.2.3.4	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d'utilisation de supports amovibles. Si le dispositif ne comporte pas de solution de type antivirus l'utilisation de support externe doit pouvoir être interdite ou contrôlée
O-11.2.3.5	Les postes utilisateurs des dispositifs connectés doivent s'adapter aux systèmes de protection contre les codes malveillants (antivirus) de l'ETABLISSEMENT DE SANTÉ ou comporter des moyens de sécurité permettant de détecter et d'éradiquer les menaces liées aux codes malveillants. Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés installés sur les postes utilisateurs sont compatibles avec des solutions de sécurité contre les codes malveillants. Le fabricant doit fournir la liste des outils de type antivirus avec lesquels ses logiciels et matériels sont compatibles (dans l'annexe SSI R-11.2.3.1).
	<b>Sécurité des réseaux</b>
O-11.2.3.6	La documentation du dispositif connecté doit comporter une matrice exhaustive des flux réseaux nécessaires à son intégration (types de protocoles, origine/destination des flux, plan d'adressage...).
O-11.2.3.7	Les postes utilisateurs des dispositifs connectés doivent être compatibles avec des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, ...). Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés, installés sur les postes de travail, sont compatibles avec les solutions de sécurité de filtrage réseaux de type firewall personnel.

Ref.	Exigence de sécurité
O-11.2.3.8	En cas de mise en œuvre de communications sans fil, le dispositif connecté doit être conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode WiFi, se référer aux documents de référence de l'ANSSI <a href="https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/">https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/</a> et aux exigences WIFI du présent référentiel.
	<b>Sécurité des données</b>
O-11.2.3.9	Afin de garantir l'intégrité des données, le dispositif connecté doit mettre en œuvre des protocoles de transmission adaptés permettant de vérifier l'équivalence des données reçues à celles émises.
O-11.2.3.10	Lors de la numérisation et de la compression des images (imagerie médicale), des procédures normalisées doivent être mises en œuvre afin de garantir l'intégrité de ces données.
O-11.2.3.11	Les échanges de données du dispositif connecté doivent être conformes aux exigences de sécurité (notamment authentification et chiffrement) identifiées dans le Cadre d'Interopérabilité des SIS publié par l'Agence Numérique de Santé (ANS) et aux recommandations du Référentiel Général de Sécurité (RGS). Le chiffrement des communications doit concerner tous les échanges depuis et vers le dispositif connecté avec toute autre ressource utile à son bon fonctionnement.
O-11.2.3.12	L'accès aux fonctions d'export de données du dispositif connecté doit être limité à des personnes dûment habilitées. Les exports vers une destination hors de l'ETABLISSEMENT DE SANTE, devront être conformes aux dispositions définies dans la convention RGPD.
	<b>Gestion des supports amovibles</b>
O-11.2.3.13	La fonction de démarrage du dispositif connecté à partir d'un support amovible doit être désactivée en fonctionnement nominal.
	<b>Surveillance</b>
O-11.2.3.14	Le dispositif connecté doit comporter une fonction d'alerte locale permettant de surveiller le bon fonctionnement, et tout événement pouvant avoir un impact critique sur son fonctionnement.
	<b>Journalisation</b>
O-11.2.3.15	Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement en particulier les événements identifiés par l'exigence 11.2.3.14. Le titulaire doit indiquer dans sa documentation les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif connecté et les recommandations en matière de sauvegarde des journaux. Il doit également fournir une procédure d'épuration automatique des journaux selon le délai légal de rétention.
	<b>Sauvegardes</b>

Ref.	Exigence de sécurité
O-11.2.3.16	<p>Le dispositif connecté doit comporter une fonction de sauvegarde conforme aux exigences en vigueur dans les bonnes pratiques et intégrer les éléments suivants :</p> <ul style="list-style-type: none"> <li>• la liste des données jugées vitales ;</li> <li>• les différents types de sauvegarde (par exemple le mode hors ligne) ;</li> <li>• la fréquence des sauvegardes ;</li> <li>• la procédure d'administration et d'exécution des sauvegardes ;</li> <li>• les informations de stockage et les restrictions d'accès aux sauvegardes ;</li> <li>• les procédures de test de restauration ;</li> <li>• la destruction des supports ayant contenu les sauvegardes.</li> </ul> <p>Des tests de restauration doivent être réalisés périodiquement et une trace technique des résultats doit être conservée.</p>
	<b>Destruction des données lors de transfert de matériels informatiques</b>
O-11.2.3.17	<p>Le titulaire doit mettre en œuvre des fonctions de sécurité d'effacement des données conformes aux exigences en vigueur dans les bonnes pratiques. L'effacement des données devra être réalisé lors de la fin de vie du dispositif connecté, de sortie des locaux de l'établissement ou de fin de contrat. Une preuve de cet effacement devra être fournie.</p>

#### 11.2.4 Maîtrise des accès

Ref.	Exigence de sécurité
	<b>Contrôle d'accès au réseau</b>
	<b>Authentification des utilisateurs</b>
O-11.2.4.1	<p>Le dispositif connecté doit comporter une fonction d'authentification des utilisateurs sur la base de comptes nominatifs et au minimum de mots de passe modifiables par les utilisateurs.</p> <p>Les mots de passe par défaut doivent être changés lors de l'installation ou de la première connexion d'un utilisateur et être spécifiques à chaque client.</p>
O-11.2.4.2	Tout accès au système dispositif connecté nécessite une authentification préalable.
O-11.2.4.3	Les logiciels du dispositif connecté doivent offrir des fonctionnalités de verrouillage automatique en cas d'inactivité prolongée et de blocage (temporaires a minima) de comptes en cas de tentative d'accès non autorisé répétée.
	<b>Droits d'accès</b>
O-11.2.4.4	Les droits d'accès des utilisateurs doivent être organisés selon des rôles.

#### 11.2.5 Développement et maintenance des logiciels

Ref.	Exigence de sécurité
O-11.2.5.1	<p>L'architecture générale du dispositif connecté et des logiciels développés doit être sans adhérence avec les briques système standards utilisées, en vue de faciliter les migrations de versions de logiciels.</p> <p>A défaut, le fournisseur doit assurer la compatibilité ascendante avec les évolutions des briques adhérentes.</p>
O-11.2.5.2	Le processus de développement doit prévoir la gestion des exceptions (débordement de plages de valeurs, erreurs internes des composants, ...).
O-11.2.5.3	Le titulaire doit implémenter une fonction permettant de vérifier l'intégrité des logiciels lors de leur démarrage ou lors de leur mise à jour.

Ref.	Exigence de sécurité
O-11.2.5.4	Les fonctionnalités de télémaintenance du dispositif connecté doivent être conformes au guide PGSSI-S – Exigences pour les interventions à distance sur les SIS.
O-11.2.5.5	Les modes de tests et de maintenance du dispositif connecté doivent être exclusifs du mode opérationnel.
O-11.2.5.6	Le dispositif connecté doit disposer d'un mode dégradé (sécurisé) permettant son fonctionnement déconnecté du SIS avec une fonction de reprise des données lors du retour en mode nominal.
O-11.2.5.7	Le titulaire doit proposer des solutions de restitution des données permettant une reprise de celles-ci par L'ETABLISSEMENT DE SANTE, notamment en cas de changement d'équipement, dans un format réutilisable par le client.

### 11.2.6 Conformité

Ref.	Exigence de sécurité
O-11.2.6.1	<p>Le titulaire doit réaliser une analyse de risques du système dispositif connecté et doit adapter les mesures de sécurité à mettre en œuvre dans ses produits au regard des risques résiduels.</p> <p>Il doit informer le RSSI de L'ETABLISSEMENT DE SANTÉ de la méthode d'analyse de risques retenue, des risques couverts et des risques résiduels qui seront portés par le client. Il peut en outre préconiser des mesures de sécurité à mettre en œuvre par l'ETABLISSEMENT DE SANTÉ afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif</p> <p>Enfin, il doit proposer à l'ETABLISSEMENT DE SANTE et au référent Métier en particulier l'état des risques résiduels et leur acceptation.</p>

### 11.3 CAS DE SERVICE HEBERGE EN DEHORS DU SI DE LA DSI DE L'ETABLISSEMENT DE SANTÉ ET DE PRESTATION DE TYPE SAAS/IAAS ET INFOGERANCE DANS LE SI DE L'ETABLISSEMENT

Cas de service hébergé en dehors du SI de la DSI DE L'ETABLISSEMENT DE SANTÉ (pour tout ou partie de l'objet du marché) et cas de services installés dans le SI de l'ETABLISSEMENT DE SANTÉ mais administrés en autonomie par le titulaire.

Ref.	Exigence de sécurité
O-11.3.1	<p>Si le centre de maintenance ou d'hébergement est en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires associées au type de système à protéger selon la politique de sécurité de l'état et du ministère de rattachement.</p> <p>Le candidat doit préciser les pays où sont réalisés les hébergements. Dans le cas d'hébergement hors communauté européenne les dispositions adaptées doivent être préalablement réalisées et validées par les autorités compétentes.</p>
O-11.3.2	Si des données de santé sont « hébergées » (cf sens donné par le Code de la Santé Publique) chez le titulaire ou un de ses sous-traitants celui-ci doit être certifié hébergeur de données de santé par un organisme certificateur qui devra être accrédité par le COFRAC (ou équivalent au niveau européen). Pour le cadre spécifique de la recherche uniquement, des dispositions spécifiques de conformité au RGPD seront établies pour des hébergements hors UE.
O-11.3.3	Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce

Ref.	Exigence de sécurité
	règlement à date d'application et accepter des audits de vérification de conformité. A cette fin sont annexées au contrat <i>les clauses de conformité au RGPD</i> .
O-11.3.4	Si des données nominatives à caractère personnel font l'objet de traitement par le système, une conformité au RGPD est nécessaire et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données. Cette démonstration doit être intégrée dans les descriptions de la prise en charge des mesures concernées du présent document, en accord avec <i>les clauses de conformité au RGPD</i> annexées au contrat.

- **Concernant l'accès par des utilisateurs de l'ETABLISSEMENT DE SANTÉ, au service hébergé :**

Ref.	Exigence de sécurité
O-11.3.5	Une authentification d'accès doit permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger. Les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification). La confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et de sa saisie. Pour l'accès aux données de santé l'authentification devra être conforme aux exigences d'authentification forte de la CNIL et de l'ANS (carte CPS ou équivalent).
O-11.3.6	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données.
O-11.3.7	Le titulaire doit remettre un compte et authentifiant pour audit au RSSI de l'ETABLISSEMENT DE SANTÉ et accepte que l'ETABLISSEMENT DE SANTÉ réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.

- **Concernant la continuité du service hébergé :**

Ref.	Exigence de sécurité
O-11.3.8	Le service ne doit pas être indisponible plus que la durée décrite dans le CCTP.

- **Concernant la réversibilité du service hébergé :**

Ref.	Exigence de sécurité
O-11.3.9	Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise à l'ETABLISSEMENT DE SANTÉ 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration.
O-11.3.10	Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise à l'ETABLISSEMENT DE SANTÉ en fin de contrat.

- **Concernant la garantie de Confidentialité des données hébergées :**

Ref.	Exigence de sécurité
O-11.3.11	Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins de l'ETABLISSEMENT DE SANTÉ
O-11.3.12	Les intervenants sont identifiés et doivent signer un engagement de confidentialité individuel. Les accès et actions réalisées pourront être tracés.
O-11.3.13	Le titulaire s'engage à détruire les données selon les dispositions prévues dans le CTPP ou à défaut en fin de contrat après les avoir restituées à l'ETABLISSEMENT DE SANTÉ sous une forme exploitable. Une preuve de la destruction sera fournie.

- **Exigences supplémentaires si la solution est installée dans l'infrastructure informatique de l'ETABLISSEMENT DE SANTÉ mais administrée intégralement par le titulaire :**

Ref.	Exigence de sécurité
O-11.3.14	Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant au moins un antivirus mis à jour et un système d'exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.
O-11.3.15	L'accès depuis l'extérieur de l'ETABLISSEMENT DE SANTÉ pour l'exploitation et la maintenance doivent respecter les conditions décrites au paragraphe Maintenance et Télémaintenance.
O-11.3.16	Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit au RSSI de l'ETABLISSEMENT DE SANTÉ et accepte que l'ETABLISSEMENT DE SANTÉ réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.
O-11.3.17	Les échanges avec l'extérieur de l'ETABLISSEMENT DE SANTÉ doivent être sécurisés : utilisation de protocoles sécurisés, du filtrage et du contrôle par les équipements de sécurité de l'ETABLISSEMENT DE SANTÉ (l'ETABLISSEMENT DE SANTÉ se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure).

- **Concernant la perte ou le renouvellement de certification d'hébergement de données de santé :**

O-11.3.18	Le titulaire certifié hébergeur de données de santé doit transmettre à l'ETABLISSEMENT DE SANTE, dans les 10 jours, les résultats des audits de certification, de contrôle et de renouvellement.
-----------	--



## 12 REFERENCES DOCUMENTAIRES

Renvoi	Document
[G_DISP_CON_SIS]	Guide Pratique Exigences pour les dispositifs connectés d'un Système d'Information de Santé - Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S] - Novembre 2013 – v1.0 Disponible sur <a href="https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf">https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf</a>
[HYGIENE]	Guide d'hygiène informatique, ANSSI, version en vigueur. Disponible sur <a href="https://www.ssi.gouv.fr">https://www.ssi.gouv.fr</a>
[ISO27001]	Norme internationale ISO/IEC 27001:2013 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences. Disponible sur <a href="https://www.iso.org">https://www.iso.org</a>
[ISO27002]	Norme internationale ISO/IEC 27002:2013 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information. Disponible sur <a href="https://www.iso.org">https://www.iso.org</a>
[PAMS_RE]	Prestataires d'administration et de maintenance sécurisées – Référentiel d'exigence, version 0.9 du 30 septembre 2019 <a href="https://www.ssi.gouv.fr/uploads/2019/10/anssi-pams-referentiel_exigences-v0.9.pdf">https://www.ssi.gouv.fr/uploads/2019/10/anssi-pams-referentiel_exigences-v0.9.pdf</a>
[MDCG 2019-16]	Les recommandations européennes de cyber sécurité pour les équipements biomédicaux <a href="https://ec.europa.eu/docsroom/documents/41863">https://ec.europa.eu/docsroom/documents/41863</a> .
[RGPD]	Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sur <a href="https://eur-lex.europa.eu">https://eur-lex.europa.eu</a>

## 13 GLOSSAIRE DES TERMES EMPLOYES

Sigle / Terme	Signification
AD	<b>Active Directory</b> : Service d'annuaire de la société Microsoft.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
Application Web	Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques.
HTTP	<b>Hypertext Transfer Protocol</b> : Protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire.
IAM	<b>Identity and Authorization Manager</b> : Service de gestion et de synchronisation des identités et autorisations entre les différents composants du SI.
Kerberos	Protocole d'authentification reposant sur un chiffrement symétrique.
LDAP	<b>Lightweight Directory Access Protocol</b> : Protocole standard de communication avec un service d'annuaire.
NTLM	Protocole d'authentification reposant sur un mécanisme de challenge.
OWASP	Open Web Application Security Project.
PAMS	Prestataires d'Administration et de Maintenance Sécurisées
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé

PKI	<b>Public Key Infrastructure</b> : Dispositif de gestion des clefs publiques. Permet l'édition des bi-clefs nécessaires au cryptage asymétrique.
QHN	Le certificat Qualité Hôpital Numérique est attribué à un industriel dont le système de management de la qualité (SMQ) respecte le Référentiel Qualité Hôpital Numérique spécifiant les exigences relatives à ce dernier.
RGPD	Règlement Général sur la Protection des Données.
RGS	Le <b>Référentiel Général de Sécurité</b> a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative.
SGBD	Dispositif de dépôt et d'indexation de données permettant l'adressage de grands volumes.
SIH	Système Informatique Hospitalier
SI	Système d'Information
SIS	SI de Santé
SSI	Sécurité des Systèmes d'Information
SSO	Single Sign On est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques en ne procédant qu'à une seule authentification.
SOAP	Protocole applicatif mis en œuvre dans le cadre de web services reposant sur l'échange de flux XML par le biais d'un serveur HTTP.
Web Service	Service applicatif exposé sous forme d'API selon le protocole SOAP.
XML	<b>Extended Markup Language</b> : « langage de balisage extensible » en français) est un métalangage informatique de balisage générique.

L'organisme paraphe toutes les pages et signe ce document ou l'Etablissement de santé intègre ces exigences dans son CCAP selon le mode d'acquisition.

Fait à ..... , le.../.../...

**Pour l'organisme**  
**(nom et qualité du signataire et cachet de l'organisme)**