CLAUSIER SÉCURITÉ

2024

Historique du document

Version	*Nature de la modification*	*Date de modification*
1	Version initiale	Mai 2023
2	Révision des exigences, ajout de précisions sur le volet RGPD et les dispositifs médicaux	Mai 2024

Sommaire

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 ;
- 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.

En fonction du périmètre de la prestation, le titulaire s'engage à se conformer à la règlementation applicable listée ci-dessous :

- l'arrêté du 28 Mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé ;
- le Décret hébergeur de données de santé n° 2006-6 du 4 janvier 2006 si le titulaire héberge des données de santé ;
- le secret des communications (Article 9 du code civil et loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications) ;
- la protection de la propriété intellectuelle et la protection des logiciels (Article L111-1 et L113-9 du code de la propriété intellectuelle) ;
- la fraude informatique et cybercriminalité (Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique) ;
- la cryptologie (Décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie) ;
- la signature électronique (Loi n°2000-230 du 13 mars 2000 portant sur l'adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique) ;
- la loi de sécurité quotidienne du 15 Novembre 2001 portant sur la lutte contre le terrorisme et notamment sur la conservation des données de connexion ;
- le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS - https://esante.gouv.fr/produits-services/ci-sis), qui fixe les règles d'une informatique de santé communicante dans le secteur de la santé, du médico-social et du social ;
- le référentiel d'exigences à destination des prestataires d'administration et de maintenance sécurisées (PAMS - https://cyber.gouv.fr/sites/default/files/2022-10/ANSSI_PAMS_referentiel_v1.1_vFR.pdf) ;

- l'arrêté du 25 juillet 2022 portant approbation du référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques de télésurveillance (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046115270) ;
- l'arrêté du 17 avril 2023 fixant les règles de sécurité des systèmes d'information d'importance vitale du sous-secteur d'activités d'importance vitale « Etablissements de santé » ;
- l'instruction N°SG/HFDS/PDS/2018/54 du 31 janvier 2018 relative à la mise en œuvre du plan Vigipirate au sein des périmètres des ministères sociaux.

Le présent référentiel est le fruit du partenariat entre l'APHM, le Club des RSSI Santé, les centrales UniHA et CAIH. Il a fait l'objet d'une collaboration étroite avec l'Association Française des Ingénieurs Biomédicaux (AFIB) et le réseau des dpo hospitaliers. Il évoluera dans ce cadre pour prendre en compte les besoins de sécurité et les évolutions réglementaires.

Les exigences de sécurité de ce référentiel sont obligatoires et non négociables. Certaines exigences identifiées dans ce document peuvent être adaptées ou faire l'objet d'une dérogation dans le CCTP.

Les ETABLISSEMENTS de SANTE pourront compléter les présentes clauses par leurs propres exigences. Une signature commune (titulaire et ETABLISSEMENT DE SANTE) de ces obligations sera effectuée.
Les présentes exigences de sécurité seront intégrées dans la convention/le marché/le contrat conclu avec l'ETABLISSEMENT DE SANTÉ le cas échéant et s'imposeront dans le cadre de son exécution.

Tous les documents référencés seront fournis au titulaire après la notification du marché et avant le démarrage des services associés.

Ref.	*Exigence de sécurité*
O-1.1	Le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment : • l'interlocuteur privilégié de l'établissement pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'établissement ou le titulaire suite à des incidents de sécurité opérationnels ; • chargé du maintien et de la mise en application du PAS (Plan d'Assurance Sécurité) ; • joignable aux horaires précisés dans le contrat. Tout remplacement de ce correspondant doit être notifié à l'établissement. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

2 EXIGENCES SPÉCIFIQUES SUR LA SOUS-TRAITANCE

Ref.	Exigences liées au Règlement Général de la Protection des Données
O-2.1	***Nature du traitement de données à caractère personnel*** Le titulaire est informé qu'il aura accès, dans le cadre des présentes, en tant que sous-traitant, à des données à caractère personnel (ci-après « les Données ») appartenant à L'ETABLISSEMENT DE SANTE. À ce titre, le titulaire s'engage à traiter les données qui lui sont confiées par L'ETABLISSEMENT DE SANTE dans le strict respect des présentes dispositions contractuelles et de la législation et réglementation en vigueur et notamment au 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 (ci-après « RGPD »). L'ETABLISSEMENT DE SANTE demeure seul responsable du traitement des données. L'ETABLISSEMENT DE SANTE autorise le titulaire, pour la durée et les seuls besoins du présent contrat/marché à procéder au traitement des données uniquement pour les services faisant l'objet du présent contrat/marché. Le candidat doit décrire : • le type de prestation (maintenance, infogérance, hébergement, etc ...), • la nature des opérations réalisées sur les données, • la ou les finalité(s) du traitement (pourquoi le titulaire a accès aux données pour les services fournis), • les données traitées et les catégories de personnes concernées, • la durée du traitement. Le titulaire s'engage à ne pas traiter de données à caractère personnel pour ses besoins propres ou pour le compte de tiers.

Ref.	Exigences liées au Règlement Général de la Protection des Données
O-2.2	***Obligations générales du sous-traitant*** Dans le cadre de ses prestations, le titulaire mettra en œuvre toutes les mesures techniques et organisationnelles adaptées à l'état des connaissances, au contexte, aux finalités du traitement et aux risques afin de protéger les Données et prendra toutes les précautions nécessaires pour préserver la sécurité, la disponibilité, la confidentialité et l'intégrité de ces Données, notamment contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. Le titulaire communiquera à l'ETABLISSEMENT DE SANTE l'ensemble des mesures prises pour garantir la sécurité des Données. Par ailleurs, le titulaire s'engage notamment à : • traiter les données uniquement pour la ou les seule(s) finalité(s) énoncée(s) ci-dessus et conformément aux instructions de l'ETABLISSEMENT DE SANTE. Si le titulaire considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement L'ETABLISSEMENT DE SANTE ; • informer L'ETABLISSEMENT DE SANTE s'il est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis ; • garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat/marché ; • veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat/marché s'engagent à respecter elle-même la confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel ; • prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ; • aider L'ETABLISSEMENT DE SANTE pour la réalisation d'analyses d'impact relatives à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle ; • communiquer à l'ETABLISSEMENT DE SANTE le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du RGPD, et de son responsable de la sécurité des systèmes d'information ; • indiquer à l'ETABLISSEMENT DE SANTE si le traitement fait l'objet d'un transfert de données hors de l'Union Européenne, le cas échéant apporter les éléments de preuve exigés par le RGPD, notamment la signature des clauses contractuelles types de la commission européenne concernant un transfert de données dans un pays ne remplissant pas les garanties adéquates. Le titulaire doit fournir le nom et les coordonnées directes du DPO ou Référent à la Protection des Données à Caractère Personnel.

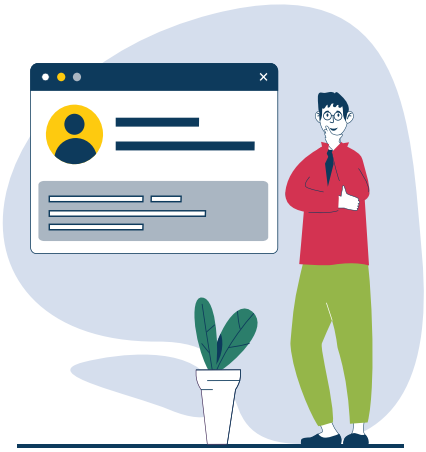
Ref.	Exigences liées au Règlement Général de la Protection des Données
O-2.3	***Sous-traitance ultérieure*** Le titulaire peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit L'ETABLISSEMENT DE SANTE de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. L'ETABLISSEMENT DE SANTE dispose d'un délai maximum de vingt-et-un (21) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si L'ETABLISSEMENT DE SANTE n'a pas émis d'objection pendant le délai susvisé. Il appartient au titulaire de s'assurer que le sous-traitant respecte les obligations du présent contrat/marché et présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant L'ETABLISSEMENT DE SANTE de l'exécution par l'un autre sous-traitant de ses obligations.
O-2.4	***Exercice de droits*** Dans la mesure du possible, le titulaire doit aider L'ETABLISSEMENT DE SANTE à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage). Si les personnes concernées venaient à exercer auprès du titulaire des demandes d'exercice de leurs droits, ce dernier doit adresser ces demandes dès réception par courrier électronique à *DPO [at] ETABLISSEMENT DE SANTE [.fr]*
O-2.5	***Violation de données*** Le titulaire notifie à l'ETABLISSEMENT DE SANTE toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, par mail à l'adresse *DPO [at] ETABLISSEMENT DE SANTE [.fr]*. Cette notification est accompagnée de la description de la violation, les données concernées, la cause et toute documentation utile afin de permettre à l'ETABLISSEMENT DE SANTE, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Ref.	Exigences liées au Règlement Général de la Protection des Données
O-2.6	***Registre des traitements*** Conformément au RGPD, le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'ETABLISSEMENT DE SANTE.
O-2.7	***Droit d'audit*** L'ETABLISSEMENT DE SANTE pourra faire procéder, une fois par an, par un cabinet d'audit tenu au secret professionnel et agréé par les deux parties, à l'examen de tout élément permettant de s'assurer de la bonne exécution des dispositions définies au présent contrat/marché. Cet audit aura lieu aux heures d'ouverture des bureaux du titulaire et sous réserve d'en avoir informé le titulaire au moins quinze (15) jours avant sa mise en œuvre, par lettre recommandée avec accusé de réception. Les frais d'audit seront à la charge de l'ETABLISSEMENT DE SANTE sauf dans le cas où l'audit révèlerait un manquement dans le cadre des obligations du titulaire. Cet audit pourra être effectué par un cabinet extérieur, pour autant que celui-ci n'exerce pas également lui-même une activité concurrente de celle du titulaire. Un exemplaire du rapport d'audit sera remis au titulaire. Si le rapport d'audit fait apparaître un non-respect des obligations du titulaire, ce dernier s'engage, dans le cadre d'un plan d'action, à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai de trente (30) jours calendaires à compter de la remise du rapport d'audit. Les Parties conviennent qu'en tout état de cause, la procédure d'audit ou son absence de mise en œuvre n'exonèrent d'aucune manière le titulaire du respect de ses obligations contractuelles et ne peuvent être interprétées comme valant acceptation de la qualité des Prestations effectuées.
O-2.8	***Engagement du Responsable de traitement*** L'ETABLISSEMENT DE SANTE s'engage à : • fournir au titulaire les données nécessaires à la fourniture des services prévus au Contrat/marché ; • documenter par écrit toute instruction concernant le traitement des données par le titulaire ; • veiller, au préalable et pendant toute la durée du contrat/marché, au respect des obligations prévues par la réglementation sur la protection des données et notamment à l'information des personnes concernées ; • superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

3 EXIGENCES GÉNÉRALES SUR LES LOGICIELS

Ref.	*Exigence de sécurité*
O-3.1	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, pré-requis, ...) 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 L'ETABLISSEMENT DE SANTÉ, le Document d'Architecture Technique (DAT) et le Document d'Exploitation (DEX).
O-3.2	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-3.3	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 L'ETABLISSEMENT DE SANTÉ
O-3.4	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-3.5	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 décrites dans ce document.

Ref.	Exigence de sécurité
O-3.6	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-3.7	Les personnels du titulaire devront respecter les chartes informatiques si existantes lors de toute intervention à l'installation ou en maintenance. Le titulaire s'engage à en informer ses personnels.
O-3.8	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-3.9	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.
O-3.10	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 de niveau supérieur à 7 et de composant obsolète (sans maintenance de correctif de vulnérabilité de l'éditeur)
O-3.11	Sauf spécification d'exclusion dans le CCTP, le logiciel, service ou application doit proposer un mode et/ou fonctionnalité dégradé(e) permettant un passage en mode manuel en cas d'interruption. Une extraction des données doit être réalisable à une périodicité définie. Les données extraites doivent être imprimables en version papier et correspondre au formalisme initial du service numérique proposé. Cette fonctionnalité et ce passage en mode manuel doit être décrit dans les spécifications fonctionnelles du service.



4 IDENTITÉS

L'ETABLISSEMENT DE SANTÉ a pris le parti d'établir le service d'annuaire de la société Microsoft (AD : Active Directory) ou un référentiel tiers en référentiel garant de l'unicité des comptes utilisateurs.

Ref.	*Exigence de sécurité*
O-4.1	Le titulaire s'engage à fournir et maintenir un système destiné à répercuter dans son application le cycle de vie d'un utilisateur (arrivée, départ). Ce système devra prendre la forme d'une interface entre l'application et le référentiel d'identité de l'ETABLISSEMENT de SANTE. Cette interface sera fournie et maintenue par le titulaire. Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent de L'ETABLISSEMENT DE SANTÉ le Document de spécifications fonctionnelles et techniques de l'interface.

5 AUTHENTIFICATION, SINGLE SIGN ON ET HABILITATIONS

Ref.	*Exigence de sécurité*
O-5.1	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) et respectant les recommandations de la CNIL.
O-5.2	Les mots de passe des comptes nécessaires à l'administration de la solution doivent pouvoir être modifiés par l'ETABLISSEMENT DE SANTÉ et chiffrés avec chiffrement à l'état de l'art si stockés localement.
O-5.3	Pour les applications web exposées sur internet et qui intègreraient 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, • l'interface d'administration doit être accessible seulement en interne.

Ref.	Exigence de sécurité
O-5.4	Pour les applications web exposées sur internet et qui intègreraient 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) en conformité avec l'Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé, applicable depuis juin 2022.
O-5.5	Le processus d'authentification doit être, sauf disposition contraire du CCTP, compatible avec un service d'annuaire ou à un mécanisme SSO du type LDAP, SAML, OpenID.

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

Ref.	Exigence de sécurité
O-5.1.1	Sauf disposition spécifique du CCTP, l'ETABLISSEMENT DE SANTÉ impose une gestion des habilitations à partir de son référentiel d'identité. Le titulaire s'engage une fois le marché obtenu à rédiger avec le référent de L'ETABLISSEMENT DE SANTÉ le Document de spécifications fonctionnelles et techniques de l'interface.

6 TRACABILITÉ

Les exigences fonctionnelles de traçabilité du CCTP peuvent être supérieures à celle citées ici d'une manière générale pour la sécurité.

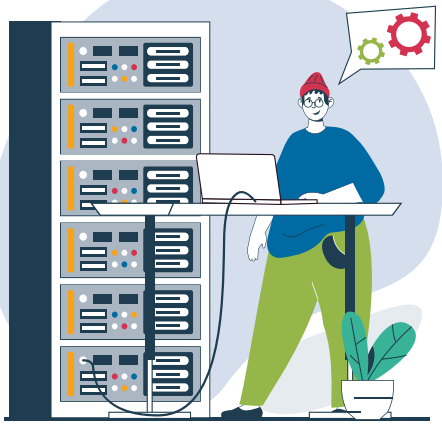
Ref.	*Exigence de sécurité*
O-6.1	La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite et conforme à la réglementation liée au projet.
O-6.2	Les accès utilisateurs (dont administrateurs) seront tracés en réussite et en échec dans le système fourni.
O-6.3	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-6.4	Les traces produites sont un prérequis et devront être mise à disposition et accessibles gratuitement 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-6.5	Les traces doivent pouvoir être épurée au-delà du temps légal de rétention notamment en conformité avec le RGPD
O-6.6	Le titulaire s'engage une fois le marché obtenu à formaliser à la demande de L'ETABLISSEMENT de SANTE le détail des traces générées, leur sécurisation et leur épuration dans un format de type Document d'Architecture Technique (DAT) et Document d'Exploitation (DEX).

7 PROTECTION DES SYSTÈMES

<table>
<tr><th>Ref.</th><th>Exigence de sécurité</th></tr>
<tr><td>O-7.1</td><td>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 :
maintenir les composants à niveau en termes de sécurité et garantit une administration sécurisée intégrant a minima 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 ;
Intégrer ses dispositifs dans la démarche sécurité de l'ETABLISSEMENT DE SANTÉ en installant l'antivirus de l'ETABLISSEMENT DE SANTÉ et l'EDR en inscrivant ses systèmes dans les exigences de gestion des correctifs de sécurité en vigueur pour le reste du SI ;
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.
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.</td></tr>
<tr><td>O-7.2</td><td>L'ETABLISSEMENT DE SANTE assure un suivi des vulnérabilités. Aussi le titulaire s'engage à proposer une application de correctif (couvrant 100 % des vulnérabilités concernées) selon la graduation et la temporalité suivante :<table><tr><th>Score CVE</th><th>Délai de mise à disposition de correctif</th></tr><tr><td>> 4.0 et < 7.0</td><td>Prochaine mise à jour mineure de l'outil</td></tr><tr><td>> 7.0 et < 8.9</td><td>Sous 3 mois</td></tr><tr><td>> 8.9</td><td>Sous 1 mois</td></tr></table>Les corrections dont le score CVE est supérieur à 7 sont à la charge du titulaire.
La mise en œuvre des actions correctives (ou de contournement) sera faite en collaboration avec l'équipe opérationnel de l'établissement.
L'installation du ou des correctifs ne doit pas avoir d'impact fonctionnel pour les utilisateurs.</td></tr>
</table>

8 CRYPTOGRAPHIE

Ref.	Exigence de sécurité
O-8.1	Dans le cas d'applications web publiées sur internet comme sur l'intranet, l'usage du TLS 1.2 ou plus est impératif.
O-8.2	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.
O-8.3	De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux exigences de l'arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé, et au Référentiel Général de Sécurité (RGS).
O-8.4	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.



9 MAINTENANCE ET TÉLÉMAINTENANCE

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

Ref.	*Exigence de sécurité*
O-9.1	Si le titulaire propose un système de supervision destiné au maintien en condition opérationnelle et de sécurité du système d'information, il devra en décrire précisément les catégories de données transférées. La protection de ces dernières devra être encadré et conforme au RGPD.
O-9.2	La connexion de télémaintenance doit se faire via la passerelle Internet sécurisée mise à disposition par l'ETABLISSEMENT DE SANTÉ conformément à sa politique de sécurité.
O-9.3	Au niveau des postes de travail standard de l'ETABLISSEMENT DE SANTÉ, aucun outil de prise de contrôle à distance ne peut être installé ou exécuté. Le seul outil de prise de contrôle à distance autorisé est celui DE L'ETABLISSEMENT DE SANTÉ.
O-9.4	Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (locaux, matériels, données, logiciels, habilitations), notamment mise à jour des correctifs de sécurité et dispositif de protection contre les codes malveillants
O-9.5	L'ETABLISSEMENT DE SANTÉ se réserve le droit de faire des contrôles de sécurité du titulaire afin de s'assurer que le niveau de sécurité requis est conforme aux exigences de sécurité du présent référentiel.
O-9.6	Les données à caractère personnel ou technique (configuration des équipements) de l'ETABLISSEMENT DE SANTÉ exploitées par les équipes de support chez le titulaire doivent être protégées et ne doivent pas être divulguées.

Ref.	Exigence de sécurité
O-9.7	L'intervention de maintenance doit être encadrée entre l'ETABLISSEMENT DE SANTÉ et le titulaire, définissant notamment les engagements de chacun, l'applications des chartes, les modalités pratiques.
O-9.8	Il est de la responsabilité du titulaire de sensibiliser son personnel à l'application des mesures de sécurité.
O-9.9	Il est de la responsabilité du titulaire de connaître en toutes circonstances les actions et l'identité de toute personne qui se connecte ou s'est connectée sur le SI de l'ETABLISSEMENT DE SANTÉ et d'en assurer la traçabilité. Cette traçabilité devra être communiquée sur demande de l'ETABLISSEMENT DE SANTÉ.
O-9.10	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-9.11	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-9.12	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. Les résultats des tests pourront être communiquées sur demande de l'ETABLISSEMENT DE SANTÉ.
O-9.13	Le titulaire doit fournir un rapport détaillé de l'intervention effectuée.
O-9.14	La connexion de télémaintenance doit se faire via la passerelle Internet sécurisée mise à disposition par l'ETABLISSEMENT DE SANTÉ conformément à sa politique de sécurité. Si l'ETABLISSEMENT DE SANTÉ ne dispose pas d'une passerelle Internet sécurisée, le cas d'utilisation d'une passerelle équivalente fournie par le 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 Selon les besoins d'intervention l'accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par l'établissement 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).
O-9.15	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 au RGPD, les dispositions relatives au traitement des incidents s'appliqueront aussi.

9.1 PRESTATAIRE D'ADMINISTRATION ET DE MAINTENANCE SÉCURISÉE

Le prestataire d'administration et de maintenance sécurisées (PAMS) doit proposer à l'ETABLISSEMENT DE SANTÉ un service à l'état de l'art en termes de sécurité de l'information, permettant aussi bien d'offrir des garanties face au risque de malveillance interne, que de se prémunir d'un scénario d'attaque pouvant conduire à la compromission du SI administré à travers les moyens d'administration qu'il met en œuvre.

L'ANSSI a établi un référentiel d'exigences pour les prestataires d'administration et de maintenance sécurisées [PAMS_RE] permettant leur qualification. Le prestataire prendra en compte ce référentiel pour améliorer sa prestation de maintenance et d'administration. L'ETABLISSEMENT DE SANTÉ disposera ainsi de garanties sur la capacité du prestataire à assurer un niveau de sécurité suffisant aux prestations d'administration et de maintenance réalisées.

Une prestation d'administration et de maintenance sécurisées non qualifiée, c'est-à-dire ne respectant pas intégralement les exigences du présent chapitre, peut potentiellement exposer l'ETABLISSEMENT DE SANTÉ à des risques critiques et notamment la fuite d'informations confidentielles, la compromission depuis un autre commanditaire du prestataire, la perte ou l'indisponibilité du service. Ainsi, dans le cas d'une prestation non qualifiée, l'ETABLISSEMENT DE SANTÉ connaîtra (sera informé par le prestataire) les risques auxquels il s'expose par l'ensemble des exigences non couvertes par le prestataire.

Ref.	*Exigence de sécurité*
O-9.1.1	Le prestataire renseigne annuellement son niveau de conformité aux exigences et recommandations du référentiel d'exigences pour les prestataires d'administration et de maintenance sécurisées de l'ANSSI [PAMS_RE].

10 SPÉCIFICATIONS WI-FI

Ref.	*Exigence de sécurité*
O-10.1	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-10.2	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.

11 PROTECTION DES DONNÉES MÉDICALES

Ref.	Exigence de sécurité
O-11.1	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-11.2	En conséquence, notamment, les jeux de données fournies par l'ETABLISSEMENT DE SANTÉ sont strictement confidentiels et sont liés au secret professionnel.

12 CAS PARTICULIER SELON PÉRIMÈTRE

12.1 CAS DES MOYENS MOBILES

Ref.	*Exigence de sécurité*
O-12.1.1	Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent pouvoir être mis à disposition et gérés par l'ETABLISSEMENT DE SANTÉ.

12.2 CAS DES DISPOSITIFS MÉDICAUX CONNECTÉS

Les exigences contenues dans ce chapitre sont issues du guide pratique [G_DISP_CON_SIS] de l'ANS, actualisé par les travaux de l'Associations Française des Ingénieurs Biomédicaux (AFIB), d'autre part.

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, microgiciel) 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.

12.2.1 CONFORMITÉ

Ref.	Exigence de sécurité
O-12.2.1.1	***Droit d'audit*** L'ETABLISSEMENT DE SANTE se réserve le droit de contrôler la qualité et la sécurité du Système fourni par le titulaire, via des audits et/ou des tests d'intrusion. Un accord formel du titulaire doit préciser : • les types de tests d'intrusion et d'audit technique autorisés, • les audits techniques qui nécessitent de prévenir le titulaire. Les types d'audits techniques à considérer sont les tests d'intrusion (de niveau réseau et/ou applicatif), les audits de configuration de composants logiciels et les audits de code source. À l'issue de l'audit, si un plan de rémédiation est proposé, le titulaire s'engage sur un planning de mise en oeuvre.
O-12.2.1.2	***Sous-traitance*** En cas de recours à de la sous-traitance pour les actions d'administration et de maintenance du DM, le titulaire s'engage à faire respecter à ses propres sous-traitants les mêmes objectifs de sécurité que ceux auxquels il est soumis.

12.2.2 GESTION DES ACCÈS

Ref.	Exigence de sécurité
O-12.2.2.1	***Gestion des profils et des droits*** Le titulaire doit décrire les fonctions accédées par les différents profils d'utilisateur du dispositif médical. Il doit également décrire les fonctions avancées accédées spécifiquement par le ou les profils d'administrateur (accès aux configurations, aux paramètres, au mode sans échec, au mode debug...).

12.2.3 CONNECTIVITÉ ET SÉCURITÉ DES RÉSEAUX

Ref.	Exigence de sécurité
O-12.2.3.1	***Protocoles d'authentification*** Le titulaire doit pouvoir fournir la procédure de connexion du dispositif médical sur le réseau de l'établissement, notamment une description des mécanismes standards d'identification et d'authentification supportés par le dispositif. Les protocoles de chiffrement utilisés pour sécuriser l'authentification et la connexion doivent être surs et connus (ex: SHA256, AES, AES-CBC, RSA-OAEP).

Ref.	Exigence de sécurité
O 12.2.3.2	***Matrice de flux réseaux*** Le titulaire assure la mise à disposition d'une matrice des flux réseaux qui décrit les flux entrants et sortants du dispositif médical. Elle décrit notamment : • l'identification et la description de chaque flux, • l'exposition à Internet (télésupervision, télémaintenance, Big Data…), • l'émetteur (application, poste, serveur, base de données…), • le récepteur (application, poste, serveur, base de données…), • le protocole réseau utilisé, • le chiffrement (algorithme), si applicable. Si le dispositif médical est composé de plusieurs matériels connectés en réseau, le titulaire doit pouvoir fournir la matrice des flux réseaux entre ces matériels. Les flux réseaux doivent être limités au strict nécessaire.
O-12.2.3.3	***Schéma d'architecture*** Si le dispositif médical est composé de plusieurs composants physiques (poste, serveur, appareil…) qui sont connectés entre eux, le titulaire doit fournir un schéma d'architecture réseau à l'établissement. Il doit notamment faire apparaître : • les serveurs physiques et/ou virtuels • les postes clients et de pilotage • les matériels médicaux • les sous-réseaux traversés par les flux entre ces composants.

12.2.4 EXPLOITATION ET COMMUNICATION

Ref.	Exigence de sécurité
O-12.2.4.1	***Mise en service*** Si le dispositif médical nécessite des actions de la part de l'établissement, le titulaire doit fournir un guide d'installation et de mise en service intégrant les modalités ci-dessous : • la liste des éventuels services à désactiver, • la liste des comptes inutiles ou obsolètes à désactiver ou à supprimer, • la liste des comptes à privilèges dont les mots de passe doivent être modifiés.

Ref.	Exigence de sécurité
O-12.2.4.2	***Détection d'une vulnérabilité critique*** En cas de mise en évidence d'une vulnérabilité critique (niveau de CVSS supérieur à 7) affectant le dispositif médical, le titulaire doit mettre à disposition de l'établissement et dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du DM. Le titulaire collabore également avec l'établissement pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.
O-12.2.4.3	***Mise au rebut*** En cas de maintenance du matériel ou de mise au rebut, le titulaire doit supprimer de manière sécurisée les données à caractère personnel de santé présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l'établissement.

12.2.5 DÉVELOPPEMENT ET MAINTENANCE DES LOGICIELS

Ref.	Exigence de sécurité
O-12.2.5.1	***Maintenance*** Le titulaire doit pouvoir fournir une procédure de maintenance précisant les modalités de mise à jour en toute sécurité du dispositif médical. Ces modalités doivent inclure : • méthodes et outils (logiciels ou matériels) utilisés par les intervenant, • sécurité appliquée sur ces outils (configuration, contrôle d'accès, traçabilité), • fonctionnalités du dispositif médical qui restent actives durant l'opération de maintenance, • mesures de sécurité qui empêchent l'accès aux données personnelles de santé stockées dans le dispositif médical par le mainteneur, • contrôle de l'origine et de l'intégrité des fichiers de mise à jour, • modalités de retour arrière en cas d'échec de la mise à jour. Cette procédure doit être validée par l'ETABLISSEMEMNT DE SANTE. Chaque opération de maintenance doit faire l'objet d'un compte-rendu de l'opération notifié et consultable par l'établissement.
O-12.2.5.2	Il doit être possible de faire scanner le contenu de la mise à jour avant son installation dans le DM, quel que soit le moyen de support utilisé par le mainteneur (portail fabricant, clé USB, disque dur, PC d'opérateur, etc.).

Ref.	Exigence de sécurité
O-12.2.5.3	***Télémaintenance*** Dans le cadre d'un accès de télémaintenance, le titulaire doit utiliser les moyens de connexion à distance mis en œuvre par l'ETABLISSEMENT DE SANTE. Toute opération de télémaintenance doit être annoncée à l'établissement par le titulaire. L'opération doit être planifiée et cadrée dans le temps avec une date de début et de fin. La connexion ne sera accordée et ouverte uniquement que durant la période convenue. Une procédure d'exception peut être prévue pour autoriser temporairement, afin de répondre à des besoins d'intervention en urgence. Un compte-rendu de l'intervention doit être dressé par le titulaire à la fin de l'opération de télémaintenance et transmis à l'établissement. Le titulaire doit fournir les IP publiques à partir desquelles les opérateurs de maintenance réalisent leurs opérations.
O-12.2.5.4	***Gestion des logiciels tiers*** Le titulaire doit fournir la liste exhaustive des logiciels tiers (OS, firmwares, librairies, outil de télésurveillance, outil de télémaintenance, etc.), i.e. qui n'ont pas été développés par le titulaire, avec leurs versions au moment de la commande. Le titulaire s'engage à maintenir ces logiciels tierces pendant la durée de vie du dispositif médical, notamment dans le cadre de la matériovigilance. Le temps de garantie de fourniture des logiciels doit être inclus dans le marché de maintenance.

12.2.6 PROTECTION DES DONNÉES

Ref.	Exigence de sécurité
O-12.2.6.1	***Protection des données personnelles de santé*** Le titulaire doit pouvoir décrire les modalités de transfert et d'export des données personnelles de santé, en précisant les protocoles utilisés. Les protocoles de chiffrement utilisés pour sécuriser l'authentification et la connexion doivent être surs et connus (ex: SHA256, AES, AES-CBC, RSA-OAEP). Si des données sont stockées dans le dispositif médical, les modalités d'accès et de stockage doivent être conformes au RGPD, aux exigences identifiées dans le Cadre d'Interopérabilité des SIS publiés par l'ANS et à la PSSI de l'établissement.

12.2.7 SÉCURITÉ PHYSIQUE

Ref.	Exigence de sécurité
O-12.2.7.1	***Sécurité physique du dispositif médical*** Les mesures de sécurité physique sur le dispositif médical doivent être documentées pour limiter les risques liés à de l'intrusion physique. L'ensemble des ports physiques (USB, RJ45, et autres) doivent être listés et placés sur un schéma. Il doit être possible notamment de : • désactiver les ports de debug, • limiter la possibilité de détourner le démarrage via un support amovible. L'ETABLISSEMEMNT DE SANTE doit pouvoir placer sur les ports USB des bloqueurs physiques. Les ports USB doivent donc être accessibles physiquement pour l'établissement.

12.2.8 RÉSILIENCE

Ref.	Exigence de sécurité
O-12.2.8.1	***Mise en sécurité*** Le dispositif médical doit pouvoir décrire un mode de «mise en sécurité» en cas d'attaque cybersécurité sur le réseau informatique garantissant la non mise en danger du patient. Les éléments suivants doivent être décrits dans la documentation du dispositif médical : • modalités de mise en sécurité, • fonctionnalités maintenues, • modalités de remise en service, • alertes et messages décrivant l'état de compromission du DM.
O-12.2.8.2	***Mode dégradé*** Le titulaire doit pouvoir décrire les modalités d'activation d'un mode dégradé en cas d'attaque cybersécurité sur le DM. Le mode dégradé est une situation où le DM doit pouvoir fonctionner malgré les impacts d'une cyberattaque. Ces modalités contiennent : • le mode opératoire pour le faire fonctionner sans connexion réseau, • le mode opératoire pour le faire fonctionner en cas de compromission d'un poste ou d'un serveur qui constitue le DM. Les modes opératoires doivent tenir compte de l'écosystème dans lequel se trouve le DM.

Ref.	Exigence de sécurité
O-12.2.8.3	***Traitement des incidents de sécurité*** Le titulaire s'engage à contacter les interlocuteurs sécurité de l'établissement désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'établissement. Le titulaire dispose d'une procédure de gestion des incidents de sécurité formalisant les étapes de traitement et de résolution d'un incident. De plus : • si cet incident a lieu sur le SI de l'établissement, un contact sécurité du titulaire est désigné et participe activement à la gestion de l'incident si l'équipement est impliqué ; • si cet incident a lieu sur le SI du titulaire, un contact sécurité du titulaire est désigné et doit fournir régulièrement un état de la situation aux établissements concernés, à l'ANSM et au CERT-Santé. Le titulaire doit obligatoirement fournir une description des impacts éventuels sur le SI des établissements. En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'établissement (traitement des causes profondes).
O-12.2.8.4	***Gestion de crise sécurité*** Sur son domaine de responsabilité SI, le titulaire applique une procédure formalisée et opérationnelle de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'établissement le respect des engagements de sécurité du DM. Ce plan précise au minimum : • les principes d'escalade (critères de déclenchement, synoptique d'escalade), • la composition de la cellule de crise : fonctions et responsabilités des membres (établissement et titulaire) — la liste nominative des membres et de leurs suppléants est référencée dans un annuaire, • les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

12.2.9 GESTION DES LICENCES

Ref.	Exigence de sécurité
O-12.2.9.1	***Gestion de la propriété intellectuelle*** Le titulaire s'assure de l'acquisition de l'ensemble des licences ou des abonnements nécessaires et de la concession des droits d'usage à l'établissement dans le cadre du service (droits d'usage de matériels, de progiciels et/ou de couches logiques). Le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de l'établissement dans le cadre de la prestation, et ce durant toute la durée du marché. Par exemple, concernant les licences Windows, le titulaire s'engage à fournir des licences à jour ou à apporter la preuve qu'un contrat de support étendu qui court sur la période prévue de la prestation.

12.2.10 PROTECTION DES DONNÉES

Ref.	Exigence de sécurité
O-12.2.10.1	***Protection des secrets stockés*** Les secrets stockés dans l'appareil (mots de passe, certificats électroniques, clés de chiffrement, etc.) doivent être protégés par des algorithmes de chiffrement surs et connus.

12. 3 CAS DE SERVICE HÉBERGÉ EN DEHORS DU SI DE L'ÉTABLISSEMENT DE SANTÉ ET DE PRESTATION DE TYPE SAAS/IAAS

Ref.	Exigence de sécurité
O-12.3	Les services hébergés devront respecter les exigences de sécurité des réglementations en vigueur

Cas de service hébergé en dehors du SI 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-12.3.1	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. 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.
O-12.3.2	Si des données sont « hébergées » en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires. 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 l'établissement de santé et les autorités compétentes.
O-12.3.3	Si le titulaire ou un de ses sous-traitants « héberge » des données de santé (cf sens donné par le Code de la Santé Publique) celui-ci doit être certifié hébergeur de données de santé conformément à l'article L 1111-8 du Code de la Santé Publique. Le titulaire devra fournir ses certifications HDS et ISO27001. Pour le cadre spécifique de la recherche uniquement, des dispositions spécifiques de conformité au RGPD seront établies pour des hébergements hors UE.

Ref.	Exigence de sécurité
O-12.3.4	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.

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

Ref.	Exigence de sécurité
O-12.3.5	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 l'Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé.
O-12.3.6	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données. Le chiffrement utilisé doit être conforme au RGS.
O-12.3.7	Le titulaire doit remettre un compte et authentifiant pour audit à la demande de l'ETABLISSEMENT DE SANTÉ et accepte que l'ETABLISSEMENT DE SANTÉ réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité.

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

Ref.	Exigence de sécurité
O-12.3.8	Le service ne doit pas être indisponible plus que la durée décrite dans le CCTP.
O-12.3.9	Sauf spécification d'exclusion dans le CCTP, le logiciel, service ou application doit proposer un mode et/ou fonctionnalité dégradé(e) permettant un passage en mode manuel en cas d'interruption. Une extraction des données doit être réalisable à une périodicité définie. Les données extraites doivent être imprimables en version papier et correspondre au formalisme initial du service numérique proposé. Cette fonctionnalité et ce passage en mode manuel doit être décrit dans les spécifications fonctionnelles du service.

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

Ref.	Exigence de sécurité
O-12.3.9	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/marché pour permettre la réalisation de tests de migration.
O-12.3.10	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/marché.

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

Ref.	Exigence de sécurité
O-12.3.11	Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins de l'ETABLISSEMENT DE SANTÉ
O-12.3.12	Les intervenants sont identifiés et doivent signer un engagement de confidentialité individuel. Les accès et actions réalisées devront être tracés.
O-12.3.13	Le titulaire s'engage à détruire les données selon les dispositions prévues dans le CTTP ou à défaut en fin de contrat/marché après les avoir restituées à l'ETABLISSEMENT DE SANTÉ sous une forme exploitable. Un procès-verbal de la destruction sera fourni au plus tard 1 mois après la fin de contrat/marché.

12. 4 CAS DE SERVICE HÉBERGÉ PAR L'ÉTABLISSEMENT DE SANTÉ ET INTÉGRALEMMENT ADMINISTRÉ PAR LE TITULAIRE

Ref.	Exigence de sécurité
O-12.4.1	Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant prioritairement les dispositifs de lutte contre les codes malveillants de l'ETABLISSEMENT de SANTE. Sinon le titulaire fournira ces dispositifs. Le système d'exploitation ainsi que tous les composants seront mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.
O-12.4.2	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-12.4.3	Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit à la demande de l'ETABLISSEMENT DE SANTÉ et accepte que l'ETABLISSEMENT DE SANTÉ réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité.

Ref.	Exigence de sécurité
O-12.4.4	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 :**

Ref.	Exigence de sécurité
O-12.4.5	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. 5 CAS DU FOURNISSEUR DE SERVICE DE DÉVELOPPEMENT

Ref.	Exigence de sécurité
O-12.5.1	Les licences et modalités de la propriété intellectuelle relatifs au code source de l'applicatif contractualisé doit être explicitées et définies dans le contrat de services avec le titulaire. Les délais de validité des licences doivent être acceptés par l'ETABLISSEMENT de SANTE.
O-12.5.2	Les accords de séquestre concernant le code source du logiciel doivent être explicités et définis dans le contrat de service avec le titulaire afin de statuer sur des modalités de conservation du code source lors des différents jalons de développement.
O-12.5.3	Toute application à destination de l'ETABLISSEMENT de SANTE doit être développée et testée dans un environnement sécurisé, différent de la production au sein des infrastructures de l'éditeur de la solution.
O-12.5.4	Un plan de test doit être déterminé avec le fournisseur de services, comprenant : a) un programme détaillé des activités et des tests, b) les données d'entrée et les données de sorties attendues sous un ensemble de conditions, c) les critères pour évaluer les résultat, d) la décision de mener des actions supplémentaires, si besoin.
O-12.5.5	Des tests de sécurité doivent être menés par rapport à un ensemble d'exigences qui peuvent être exprimées comme fonctionnelles ou non fonctionnelles. Il convient que les tests de sécurité incluent les tests : a) des fonctions de sécurité : l'authentification des utilisateurs, les restrictions d'accès et l'utilisation de la cryptographie, b) du codage sécurisé, c) des configurations sécurisées, y compris celles des systèmes d'exploitation, des pares-feux et autres composants de sécurité.

Ref.	Exigence de sécurité
O-12.5.6	Le fournisseur de service, dans le cadre de la livraison de développement pour l'ETABLISSEMENT de SANTE, doit présenter des preuves montrant que les tests suffisants ont été réalisés pour protéger le code source de la présence de contenus malveillants. L'ETABLISSEMENT de SANTE pourra valider les preuves communiquées, et demander des compléments si celles-ci ne sont pas conformes avec ses attendus.
O-12.5.7	Les développements du titulaire doivent respecter les principes de sécurité énoncés par l'organisme OWASP en vigueur, qui fournit une liste de dix domaines de vulnérabilités majeurs et les guides pratiques associés pour s'en prémunir.
O-12.5.8	Les développeurs ne doivent en aucun cas utiliser du code provenant d'une source inconnue ou qui n'a pas été vérifiée (forums, internet, etc.). De plus, l'utilisation d'un code sous copyright est également prohibée, ou doit comporter une description contractuelle.
O-12.5.9	Le « codage en dur » d'identifiants dans le code source est prohibé. Les identifiants ne devant pas être « codés en dur » sont, de façon non exhaustive, les suivants : • nom d'utilisateur, • mot de passe, • certificat électronique, • numéro de jeton (token), • numéro de téléphone. Les mesures de protection contre cette vulnérabilité sont décrites dans l'OWASP 2021 : A2 « Défaillances cryptographiques »
O-12.5.10	Le développement externalisé doit être supervisé et contrôlé par les équipes projet et les référents de l'ETABLISSEMENT de SANTE. En cas de développement externalisé, des contrats intégrant les bonnes pratiques de sécurité du présent clausier doivent être passés avec l'éditeur et l'ETABLISSEMENT de SANTE.
O-12.5.11	L'application doit être développée et testée dans un environnement sécurisé, différent de la production. En développement « cycle en V » comme en méthode agile, l'équipe projet doit s'assurer que l'environnement de développement est bien distinct et cloisonné (dans la mesure du possible physiquement) par rapport aux environnements de préproduction/qualité et production.
O-12.5.12	Lors de l'utilisation de données de test en environnement de développement, un mécanisme d'anonymisation ou de pseudonymisation des données de production devrait être mis en place consistant à rendre peu probable, au mieux impossible, l'identification des personnes.

Ref.	Exigence de sécurité
O-12.5.13	Les développeurs ne doivent pas publier le code source sur des forums ou sites internet spécialisés (ex : afin de demander des conseils). De plus, le code source doit être protégé dans un environnement sécurisé. Si la contribution à une communauté open source est nécessaire, le développeur doit demander autorisation à l'ETABLISSEMENT de SANTE.
O-12.5.14	Parce qu'ils peuvent contenir des informations qui peuvent être utilisées par des attaquants, les développeurs doivent supprimer tous les commentaires sensibles de leur code avant la mise en production de l'application.
O-12.5.15	Les tests de sécurité, pour les applications considérées comme sensibles (notamment manipulant de la donnée de santé nominative), doivent permettre de s'assurer que les exigences de sécurité ont été correctement appliquées. Lorsque la conception de l'application est terminée, des tests de sécurité doivent être réalisés avant sa mise en production (revue du code, test d'intrusion, scan de vulnérabilité, ...). Ces tests doivent également perdurer après la mise en production.
O-12.5.16	En complément des tests de sécurité, des audits techniques et tests d'intrusion devraient être planifiés avant une mise en production d'un applicatif. À la suite des tests de sécurité, le plan de traitement doit être validé afin de limiter la possibilité de découvrir de nouveaux risques ou à minima d'amoindrir leurs impacts s'ils sont inévitables.
O-12.5.17	L'ETABLISSEMENT de SANTE, dans le cadre de la prestation de service contractualisé avec le fournisseur de service de développement, peut demander une fois par an un audit technique sur le développement engagé. Les modalités et les couts de cet audit sont à la charge de l'ETABLISSEMENT. L'ETABLISSEMENT de SANTE doit prévenir le fournisseur de services afin que celui-ci propose un planning de réalisation dans les 60 jours suivant la demande initiale. Le titulaire s'engage à corriger les vulnérabilités, dans un calendrier établi en accord avec l'ETABLISSEMENT de SANTE.
O-12.5.18	En cas de violation de données à caractère personnel, l'ETABLISSEMENT de SANTE, dans le cadre de la prestation de service contractualisé avec le fournisseur de service de développement, peut demander un audit technique sur le développement engagé. Les modalités et les couts de cet audit sont à la charge du TITULAIRE. L'ETABLISSEMENT de SANTE doit prévenir le fournisseur de services afin que celui-ci propose un planning de réalisation dans les 15 jours suivant la demande initiale. Le titulaire s'engage à corriger les vulnérabilités, dans un calendrier établi en accord avec l'ETABLISSEMENT de SANTE.

RÉFÉRENCES DOCUMENTAIRES

Renvoi	Document
[G_DISP_CON_SIS]	Guide Pratique de l'Agence du Numérique en Santé (ANS) : « 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 https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf
[HYGIENE]	Guide d'hygiène informatique, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[ISO27001]	Norme internationale ISO/IEC 27001:2022 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences. Disponible sur https://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002:2022 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information. Disponible sur https://www.iso.org
[PAMS_RE]	titulaires d'administration et de maintenance sécurisées – Référentiel d'exigence, version 1.1 du 6 Octobre 2022 https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf
[G_DEST_TRANS]	Guide Pratique Destruction des données lors du transfert de matériel informatique - Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S] – Août 2022 – v2.0 Disponible sur https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI-S_Guide_Pratique-Destruction_de_donnees-V2.0.pdf
[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 https://eur-lex.europa.eu

GLOSSAIRE DES TERMES EMPLOYÉS

Sigle / Terme	Signification
AD	**Active Directory** : 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	**Hypertext Transfer Protocol** : Protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire.
IAM	**Identity and Authorization Manager** : 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	**Lightweight Directory Access Protocol** : 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	**Public Key Infrastructure** : 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 **Référentiel Général de Sécurité** 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	**Extended Markup Language** : « langage de balisage extensible » en français) est un métalangage informatique de balisage générique.

Nous remercions tous ceux qui ont contribué
à l'écriture de ce clausier :

C.A.I.H.
Centrale d'Achat de l'Informatique Hospitalière

https://rssi-sante.fr/

Conception graphique et mise en page : www.marie-graphiste.com