

ANNEXE N° 01

SOMMAIRE

1. Introduction.....	2
2. Exigences Générales.....	4
3. Identités	11
4. Gestion des habilitations.....	12
5. Authentification et Authentification unique	13
6. Traçabilité.....	16
7. Cryptographie.....	18
8. Maintenance à distance et/ou sur site	19
9. Specifications wi-fi (802.11G ou 802.11B)	23
10. Continuité de service	24
11. Conformité	26
12. Protection des données médicales.....	27
13. Cas particuliers selon le périmètre	28
14. Glossaire des termes employés	33

1. Introduction

Ce document énonce les exigences et recommandations du Centre Hospitalier du Mans (CHM) en termes de sécurité vis-à-vis de ses prestataires externes ayant accès à un ou plusieurs éléments constituant son Système d'Information.

Les parties ci-après mentionnées sont :

Le Centre Hospitalier du Mans représenté par M. Olivier Bossard, Directeur Général est ci-après désigné par les termes «CHM» ou « Centre Hospitalier du Mans ».

ET

Le Titulaire ci-après désigné, représente les prestataires externes et le cas échéant leurs sous-traitants ou cotraitants appelés à participer à l'exécution d'une prestation nécessitant l'accès à un ou plusieurs éléments constituant le Système d'Information du CHM.

Les solutions informatiques déployées au sein du Système d'Information du Centre Hospitalier du Mans (CHM) doivent :

- Respecter les préconisations en matière de sécurité de l'Agence du Numérique en Santé (ANS), l'ANSSI et du Ministère de la santé (PSSI –MCAS qui pourra être fournie sur demande).
- Respecter les exigences complémentaires propres à des systèmes critiques spécifiques

Les **exigences de sécurité sont obligatoires** et sont notées **O comme Obligatoire**.

Les **recommandations sont des orientations techniques** fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles sont notées **R comme Recommandé**.

Toutes les cases « **description de la prise en charge** » doivent être renseignées. Si une règle n'est pas applicable la mention **N/A** est inscrite et **doit être justifiée**.

De manière générale, le titulaire doit respecter les précautions mentionnées dans le guide de sécurité des données personnelles de la CNIL Edition 2018.

Les présentes exigences de sécurité seront soit, annexées :

- Aux clauses de sous-traitance RGPD du CHM intégrées aux contrats de sous-traitance conclus avec le CHM et s'imposeront dans le cadre de leur exécution.

Et/Ou

- A la Charte de bon usage du système d'Information à destination des prestataires externes du CHM.

Dans tous les cas elles constituent un engagement de la part du titulaire dans le cadre d'un Marché.

Le titulaire pourra établir un PAS (Plan Assurance Sécurité) afin de faire connaître les dispositions de sécurité qu'il met en place pour sa prestation. Le PAS traite :

- Des critères de sécurité utilisés dans la désignation des personnes chargées des interventions.
- De la désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés.
- Des règles de protections des informations du Système d'Information associées à la prestation de maintenance.
- De l'architecture générale de la plateforme d'intervention (cloisonnement technique etc.).
- Des accès logiques à la plateforme, identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité...
- Des dispositions prises pour assurer la continuité de l'activité après un sinistre ou un incident majeur.
- De l'assurance et des contrôles de la sécurité des services de l'intervention fournis.
- De la politique de sécurité physique et environnementale au niveau de son Datacenter/de son centre à partir duquel interviennent ses équipes, en particulier :
 - Contrôle d'accès physique dans le bâtiment, dans les locaux, dans la zone dédiée à la mission ;
 - Sécurisation des bureaux et salles informatiques et télécom ;
 - Protection contre des menaces extérieures et environnementales (ex. vandalisme, incendie, dégât des eaux,...) ;
 - Procédures spécifiques pour garantir la confidentialité des données du CHM ;
 - Protection des équipements et matériels informatiques ;
 - Protection contre des menaces portant atteinte à des services essentiels : électricité, climatisation, accès réseau, écoute,... ;
 - Engagement de maintenance sur les équipements concernés ;
 - Protection des actifs contenant des informations sensibles, lors de la sortie des locaux ;
 - Engagement de destruction sécurisée des données lors de la mise au rebut d'un équipement.

Dans ce cas, le Plan d'Assurance Sécurité intégrera toutes les réponses aux exigences énoncées dans ce document :

- En respectant le plan de ce document,
- En inscrivant pour chacune des réponses, la référence de l'exigence. (colonne Ref.)

2. Exigences Générales

- Sur les ressources humaines :

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.1	O	La Charte de bon usage du Système d'Information du CHM à destination des prestataires externes devra être retournée au CH du Mans, signée par le représentant légal du titulaire avant toute délivrance de prestation. Ceci vaudra pour acceptation de l'ensemble du document.	
2.2	O	<p>Le titulaire s'assurera que tout son personnel, et celui de ses sous-traitants éventuels devant accéder au SI du CH du Mans ait au préalable pris connaissance de cette « Charte de Bon Usage du SI du CH du Mans à destination des prestataires externes » et signé la « convention pour les accès au SIH du CH du Mans » reconnaissant ainsi qu'il s'engage à respecter toutes les exigences de sécurité demandées par l'Etablissement.</p> <p>Les exigences de sécurité du présent document seront portées à la connaissance de tout le personnel du titulaire, et celui de ses sous-traitants éventuels devant accéder au SI du CH du Mans</p> <p>Chaque personnel du titulaire et celui de ses sous-traitants éventuels amené à accéder au Système d'Information de l'Etablissement devra retourner un exemplaire signé de la « convention pour les accès au SIH du CH du Mans » à la Direction du Système d'Information du CH du Mans.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.3	O	Les contrats de travail des personnels employés par le titulaire, ou par le personnel de son ou ses sous-traitant(s) susceptibles d'intervenir sur le Système d'Information du CH du Mans doivent contenir une clause relative au secret médical ou au secret professionnel et à la confidentialité des données clients.	
2.4	O	Concernant la formation des personnels du Titulaire ou de celui de son ou ses sous-traitant(s), le titulaire précisera : <ul style="list-style-type: none"> • Les organismes formateurs ; • La fréquence et le contenu des actions de formation, de sensibilisation de ses personnels aux enjeux de sécurité et de confidentialité des données personnelles, à leur non divulgation et à leur destruction et non conservation ainsi qu'au secret professionnel. 	
2.5	O	Avant toute prestation, le titulaire devra fournir une liste de ses personnels (Nom, Prénom, Adresse Mail) ou de celui de son ou ses sous-traitant(s), amenés à accéder au Système d'information du CHM. Cette liste servira à établir les identifiants des comptes d'accès et les mots de passe associés. Ces identifiants et mots de passe associés seront transmis individuellement aux personnels du titulaire ou le cas échéant celui de son ou ses sous-traitants par tout moyen jugé sécurisé par la Direction du Système d'Information de l'Etablissement.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
2.6	O	Pour permettre au CH du Mans, de procéder à des revues d'accès régulières, le titulaire s'engage à fournir tous les 6 mois la liste à jour des personnes habilitées (son personnel ou celui de son ou ses sous-traitant(s)) à se connecter sur le Système d'Information du CH du Mans ainsi que leur niveau d'habilitation (type d'accès et ressources concernées du CH du Mans).	
2.7	O	<p>Le titulaire s'engage à porter immédiatement à la connaissance de la Direction du Système d'Information du CHM, le départ de sa société, d'un de ses personnels ou le cas échéant celui d'un de son ou ses sous-traitants détenant un compte d'accès sur le SI de l'établissement afin que la DSI procède à la désactivation ou la suppression du compte d'accès concerné.</p> <p>Pour ce faire, le titulaire ou le cas échéant son ou ses sous-traitant(s) procéderont par écrit en indiquant, le nom et le prénom du personnel concerné, ainsi que la date à laquelle le compte d'accès concerné doit être désactivé ou supprimé.</p> <p>En cas de non-respect de cet article de la part du Titulaire ou de son ou ses sous-traitant(s), la responsabilité de ces derniers, resterait engagée.</p>	
2.8	O	En cas de recours à un ou plusieurs sous-traitant(s), le titulaire devra en aviser le CH du Mans avant toute intervention de ce ou ces sous-traitant(s). Les sous-traitants éventuels et leurs personnels auront les mêmes obligations que le titulaire en ce qui concerne la satisfaction aux exigences de sécurité du Système d'Information du CHM.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

▪ Sur les logiciels :

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.9	O	Le titulaire s'engage à fournir la liste exhaustive des logiciels installés, documentée (niveau de version, prérequis, ...) et contenant les informations détaillant chaque logiciel ainsi que les interactions entre eux.	
2.10	O	<p>Pour tout ce qui est fourni au titre de la prestation, le titulaire s'engage à acquérir et à concéder au CHM l'ensemble des licences d'utilisation nécessaires à son bon fonctionnement.</p> <p>Si nécessaire, il détaillera les conditions spécifiques ou exclusions.</p> <p>Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance...).</p>	
2.11	O	Le titulaire s'engage à n'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du contrat de sous-traitance.	
2.12	O	Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. ils devront aussi respecter les exigences de sécurité.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.13	O	Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité.	
2.14	O	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.	
2.15	O	Toute opération réalisée par le titulaire et ses personnels lors de l'installation devra respecter les mêmes règles que celles décrites dans le chapitre Maintenance et Télémaintenance durant son exécution.	
2.16	R	Lorsque des données à caractère personnel sont gérées par l'application, le titulaire fournit une procédure ou un outil d'anonymisation pour pouvoir être appliqué à tout autre environnement que celui de production.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.17	O	<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"> • Déploiement de ses propres utilitaires et politiques de mise à jour. • Intégration de ses dispositifs dans la démarche sécurité du CHM en installant l'antivirus du CHM et en inscrivant ses systèmes dans les règles 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 pour décider d'un éventuel complément de sécurité • A défaut, ou en cas d'une insuffisance de l'analyse antivirale, une solution de sécurité externe en interface avec le dispositif sera installée (équipement de type pare-feu avec antivirus). <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>	
2.18	R	<p>Les applications ou services nécessitant un fonctionnement permanent, doivent être hébergés sur des machines ayant un système d'exploitation de type serveur et ne doivent pas dépendre d'une session utilisateur (fonctionnement en mode service).</p>	
2.19	R	<p>Seules des versions de système d'exploitation maintenues par l'éditeur en termes de mise à jour de sécurité doivent être installées.</p> <p>Le titulaire décrira tous les cas particuliers nécessitant une protection supplémentaire.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.	CHM	Règle de sécurité	Description de la prise en charge par le titulaire
2.20	R	Si la solution proposée doit être hébergée sur un serveur de l'établissement, elle doit être compatibles avec les prérequis fournis par la DSI.	
2.21	R	Si la solution proposée comporte des objets connectés (IOT), un rapport d'audit par un organisme spécialisé indépendant du titulaire ou une certification par un organisme accrédité par le COFRAC est demandé. Ce rapport ou cette certification porteront sur la sécurité numérique et la protection des données personnelles dans le cadre de la mise en œuvre de ces objets connectés	
2.22	O	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 de sous-traitance RGPD du CH du Mans fournies doivent être signées, paraphées par le représentant légal du sous-traitant.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

3. Identités

LE CHM exploite le service d'annuaire de la société Microsoft (AD : Active Directory) en référentiel garant de l'unicité des comptes utilisateurs.

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
3.1	R	<p>Le titulaire décrira la gestion des identités au sein de son dispositif, notamment les possibilités suivantes :</p> <ul style="list-style-type: none"> ✓ Déport de la gestion d'identité de l'application au sein de l'annuaire Active Directory du CHM. ✓ Mise à disposition d'un point d'entrée (web service, connecteur...) permettant au CHM de synchroniser le référentiel d'identités de l'application avec un référentiel d'identité et d'authentification (IAM). <p>En l'absence de ces modes le titulaire décrira la gestion des identités au sein de son dispositif.</p>	
3.2	O	<p>Si pour des contraintes techniques acceptées par la Direction du Système d'Information du CHM, les identifiants des comptes nécessaires à l'administration de la solution (comptes de services, d'administration de bases de données, d'administration de serveurs, ...) mis en place par le titulaire dans le cadre de l'exécution de sa prestation ne peuvent être nominatifs, le titulaire présentera les mesures techniques et/ou organisationnelles pour en garantir l'imputabilité.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

4. Gestion des habilitations

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
4.1	O	<p>La gestion des habilitations doit pouvoir reposer sur un moteur d'habilitation du CHM. Un moteur de ce type fournit pour chaque utilisateur un ensemble d'information dont notamment le profil à utiliser dans l'application (fonctionnalités autorisées) et son périmètre d'habilitation (liste des Unités Fonctionnelles pour lesquelles il peut accéder aux informations).</p> <p>Si son dispositif intègre ce type de service, Le titulaire décrira par quels moyens :</p> <ul style="list-style-type: none"> ✓ Appel de web service, provisionning par EAI ✓ Intégration spécifique, auquel cas l'éditeur devra fournir les éléments pour un accès direct et documenté à son système d'habilitation ne présentant pas de risque pour le fonctionnement du produit (web service, tables de base de données, procédures stockées ...) <p>Si le titulaire a déjà mis en place ce type de service, il précisera avec quel moteur d'habilitation.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

5. Authentification et Authentification unique

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
5.1	O	Les mots de passe des comptes nécessaires à l'administration de la solution (comptes de services, d'administration de bases de données, d'administration de serveurs, ...) doivent pouvoir être modifiés par Le CHM.	
5.2	O	Les règles de complexité des mots de passe nécessaires à l'administration de la solution (comptes de services, d'administration de bases de données, d'administration de serveurs, ...) doivent pouvoir satisfaire aux contraintes de complexité suivantes (exigence de la CNIL) : <ul style="list-style-type: none"> ✓ Longueur minimale d'au moins 8 caractères; ✓ Comporter au minimum une majuscule, un chiffre et un caractère spécial ; ✓ Ne pas être vulnérables aux attaques par dictionnaire. 	
5.3	O	Les règles de complexité des mots de passe des utilisateurs standards de la solution doivent pouvoir satisfaire aux contraintes de complexité exigées par la CNIL, notamment : <ul style="list-style-type: none"> ✓ Longueur minimale d'au moins 8 caractères; ✓ Comporter au minimum une majuscule, un chiffre et un caractère spécial ; ✓ Ne pas être vulnérables aux attaques par dictionnaire. 	
5.4	O	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données.	
5.5	R	La gestion des mots de passe doit intégrer un mécanisme de renouvellement du secret avec historisation et la possibilité de ne pas réutiliser ces secrets.	
5.6	R	S'agissant des applications WEB, l'usage des protocoles NTLM ou Kerberos est attendu en vue de perpétuer implicitement et de manière sécurisée l'identité de l'utilisateur connecté au serveur web.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
5.7	R	<p>Concernant les applications usant d'un client lourd :</p> <ul style="list-style-type: none"> Lorsque le référentiel d'identités de l'application est déporté dans l'AD, l'authentification auprès d'un serveur AD du ticket de session associé au processus applicatif est fortement préconisée. Si l'application n'offre pas – en l'état – la possibilité de récupérer l'identité Windows, un plan d'intégration le permettant est souhaité. A minima, l'authentification de l'utilisateur par mot de passe reposera sur LDAP. Lorsque le référentiel d'identités est propre à l'application et seulement synchronisé à l'AD, la simple récupération de l'identité du propriétaire du processus applicatif pourra être tolérée dans l'attente d'une intégration de LDAP à l'application. Ce mode transitoire aux bonnes pratiques est justifié lors du recours à une authentification forte (CPS ou équivalent) à l'ouverture de session Windows. 	
5.8	R	<p>Dans le cas d'architecture N-Tiers, l'origine de la connexion fera partie du processus d'authentification. Ainsi lorsque l'application permet la propagation des identités utilisateurs jusqu'aux données, l'utilisateur ne saurait se connecter directement au SGBD. La chaîne d'accès devra donc être garantie pour chaque strate applicative.</p>	
5.9	O	<p>Pour les applications web exposées sur internet et qui intégreront une authentification et/ou une gestion des comptes :</p> <p>Les pages réservées à l'authentification et à la création de comptes doivent intégrer un dispositif de prémunition contre l'usage de robots.</p> <p>Des mécanismes empêchant de réutiliser des informations de connexion ou de session pour contourner l'authentification doivent être en place.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
5.10	O	<p>Pour les applications web exposées sur internet et qui intégreraient une authentification et/ou une gestion des comptes, les mécanismes d'authentification doivent être adaptés à la criticité des données.</p> <p>Une authentification forte (à double facteurs) est exigée pour l'accès à des données de santé par carte CPS ou équivalent (sauf disposition contraire qui conduirait Le CHM à prendre en charge une authentification forte en préalable à l'accès à la solution : cas d'un portail d'authentification en amont de l'application).</p>	

6. Traçabilité

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

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
6.1	R	la solution proposée doit exposer de manière sécurisée ses éléments de traçabilité. Décrire les systèmes d'accès.	

▪ Contenu de la trace :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
6.2	O	La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite.	
6.3	O	Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec.	
6.4	O	Dans le cadre de systèmes gérant des données personnelles les traces de consultation et de modification sont obligatoires.	
6.5	O	Les traces produites devront être accessibles par l'outil de centralisation des traces du CHM dans un format et un mode d'accès rendus possibles et décrits par le titulaire (format IHE, syslog, requête dans une base de données à fournir, fichier à décrire).	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
6.6	R	S'agissant des modifications de valeurs sensibles au sein du dispositif, il est souhaité que les traces correspondantes comportent la valeur en amont et en aval de l'événement. La suppression d'une donnée du point de vue applicatif ne saurait engendrer la perte de l'historique des accès et modifications associées à cette donnée.	
6.7	R	Lorsque la gestion des autorisations applicatives – même partiellement – est du ressort de l'application, il est souhaitable que tout événement relatif à l'édition d'un profil ou d'un utilisateur soit tracé.	
6.8	R	Dans le cas d'architectures N-Tiers ou lors de l'usage de comptes applicatifs, les traces devront comporter l'utilisateur d'origine et l'ordinateur source de la connexion. Si cela s'avérait impossible, la mise en corrélation des traces des différentes strates applicatives par le biais des identifiants de session devra permettre de déterminer avec certitude la continuité de l'accès.	

7. Cryptographie

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
7.1	O	Dans le cas d'applications web publiées sur internet comme sur l'intranet, l'usage de SSL est impératif. Le titulaire pourra recourir à des certificats fournis par Le CHM.	
7.2	O	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.	
7.3	O	De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux standards du marché, et au Référentiel Général de Sécurité (RGS).	

8. Maintenance à distance et/ou sur site

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
8.1	O	Dans le cas où la prestation s'effectuerait à distance en utilisant, via une ligne de communication dédiée, ou des ressources informatiques de l'établissement, le Titulaire a pour obligation d'utiliser les moyens de connexion et les procédures imposées par la Direction du Système d'Information du CHM. (Passerelle Internet sécurisée mise à disposition par Le CHM (VPN IPSEC ou VPN SSL))	
8.2	O	Les identifiants des comptes d'accès utilisés pour se connecter au Système d'information du CHM, par le titulaire ou son personnel sont nominatifs .	
8.3	O	L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par la Direction du Système d'Information du CHM. Dans ce cas, le titulaire présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité. L'utilisation de mots de passe constructeur ou par défaut est interdite.	
8.4	O	L'accès au Système d'Information du CHM doit être réalisé en accord avec l'établissement et nécessite de prévoir un créneau horaire pour éviter d'intervenir pendant une plage d'utilisation. La règle impose que la ou les personnes du CHM qui ont été désignées au personnel du Titulaire ou le cas échéant au personnel de son ou ses sous-traitant(s) pour l'accompagner dans ses actions soit informée au préalable de toute action sur le Système d'information du CHM. Il est obligatoire de planifier les actions hors aspects d'urgences ou de dysfonctionnement perturbant un système ou un logiciel.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
8.5	O	Le Titulaire acceptera sans réserve que les connexions à distance effectuées par son personnel, puissent être enregistrées sous forme vidéo et conservées le temps jugé nécessaire par le CHM et dans le respect de la réglementation en vigueur.	
8.6	O	Au niveau des serveurs et postes de travail standard du CHM aucun logiciel de prise en main à distance (exemples Logmein ou Teamviewer) ne doit être installé et/ou utilisé par le titulaire sans que celui-ci n'y ait été autorisé explicitement par la Direction du Système d'Information du CHM. Le titulaire et ses personnels n'installeront aucune porte dérobée ou ouverte sur les postes, encore moins sur les serveurs.	
8.7	O	Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (données et logiciels)	
8.8	O	Le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance.	
8.9	R	Les postes de télémaintenance doivent être isolés physiquement du réseau local du titulaire.	
8.10	R	Le titulaire garantit la mise à niveau de ses logiciels et plateformes en cas d'obsolescence du système d'exploitation. Il en est de même pour tous les autres logiciels indispensables au bon fonctionnement du dispositif. A défaut il fournira à titre gracieux les moyens pour maintenir un niveau de sécurité suffisant.	
8.11	O	les données à caractère personnel ou technique du CHM (configuration des équipements) exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée).	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
8.12	O	L'intervention de maintenance est encadrée par un règlement, un contrat ou une convention entre Le CHM et le titulaire, définissant les engagements de chacun.	
8.13	O	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).	
8.14	O	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 du CHM). Ce journal de connexion devra être horodaté et permettre d'identifier précisément (nominativement) les personnes ayant accédé au Système d'Information du CH du Mans.	
8.15	R	Ce journal de connexion devra comporter les informations suivantes : Entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ; Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ; Création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ; Actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action ; Ces traces de connexions devront être conservées sur une période d'au moins 18 mois glissants à partir de la première connexion.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
8.16	O	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.	
8.17	O	LE CHM 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 en vigueur.	
8.18	O	<p>Pour ce qui concerne la remontée d'informations issues des dispositifs maintenus vers votre site de diagnostic, cet envoi doit être décrit précisément en indiquant toutes les données transférées. Cet usage exclusif à des fins de surveillance du maintien en condition opérationnelle et/ou l'absence de données personnelles directement ou indirectement liées à nos patients doivent être garantis.</p> <p>Cette remontée d'information devra utiliser des protocoles sécurisés, être tracée et passer par nos passerelles de contrôle d'accès à internet ou par un VPN IPSEC site à site avec votre site de télédiagnostic (recommandé).</p>	
8.19	O	<p>Le titulaire doit fournir un rapport détaillé de l'intervention effectuée. le titulaire s'engage à ce que la ou les personnes du Centre Hospitalier du Mans, qui lui ont été désignées pour l'accompagner, soi(en)t informée(s) des actions entreprises et des éventuelles difficultés rencontrées. Ce compte rendu se fait par écrit sous forme de rapport précisant notamment : la date, la nature des opérations effectuées et les noms des intervenants.</p> <p>Dans le cas d'une intervention en horaires non-ouvrés, le rapport sera expédié le jour même de l'intervention à une adresse courriel communiquée au préalable.</p>	
8.20	O	Si Le CHM 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 (Dans ce cas, et de fait l'accès direct aux serveurs et applications serait interdit).	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

9. Specifications wi-fi (802.11G ou 802.11B)

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
9.1	O	<p>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) au moment de l'installation de la solution.</p> <p>La sécurité de ce type de réseau sera validée par le département technique de la DSI du CHM avant mise en production.</p>	
9.2	O	<p>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.</p> <p>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.</p>	

10. Continuité de service

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
10.1	R	<p>Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité.</p> <p>En cas d'évolution, le Titulaire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du CHM.</p> <p>Le Titulaire précisera :</p> <ul style="list-style-type: none"> ✓ les conditions d'accès à distance pour mettre à jour son système ; ✓ les méthodes de qualification et de non régression de son système mis à jour ; ✓ les moyens de retour en arrière ; ✓ la méthodologie d'analyse des risques et les actions de traitement des risques avant toute mise à jour majeure. 	
10.2	O	<p>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.</p>	
10.3	O	<p>Dans le cadre de l'application de plans gouvernementaux, il peut être décidé la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications des opérateurs d'infrastructures vitales et de services essentiels. Si le titulaire était amené à être concerné par ces directives décidées au niveau gouvernemental, il s'engage à appliquer les consignes de sécurité données par le CHM.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
10.4	R	<p>Le titulaire a pris des dispositions internes pour assurer la continuité d'activité et la reprise d'activité de son système, il précisera en particulier :</p> <ul style="list-style-type: none"> ✓ L'organisation mise en place ; ✓ Les moyens et procédures de supervision, de réaction face à un incident, de gestion de crise ; ✓ La définition des critères de continuité et de redémarrage des environnements des clients ; ✓ La cellule de gestion de crise ; ✓ Le plan de communication ; ✓ Le plan d'évolution de l'architecture, des procédures en fonction des exigences des clients et des évolutions technologiques. 	
10.5	O	<p>Le Titulaire s'engage à alerter les établissements concernés par le présent marché de toute menace ou vulnérabilité dont il aurait connaissance. Il indiquera les dispositifs de veille technologique mis en place au sein de sa structure pour se tenir informé de ces menaces et vulnérabilités.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

11. Conformité

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
11.1	R	<p>Le Titulaire devra dans la mesure où il détient la certification, fournir au CHM un rapport type ISAE 3402, ou SSAE16 de niveau II de moins de 24 mois.</p> <p>Le Titulaire précisera si sa société détient des certifications ou agréments applicables (ex. ISO27001, ISO27005, HDSCP, Qualité HN, ISO9001, ITIL,...) à son offre/prestation/système, en particulier :</p> <ul style="list-style-type: none"> ○ l'intitulé exact ; ○ la date d'émission et la durée d'applicabilité ; ○ l'organisme certificateur; ○ le dispositif de contrôle : <ul style="list-style-type: none"> ▪ Contrôle interne ; ▪ Contrôle externe ; <p>Le Titulaire précisera si sa société entretient des relations avec des autorités ou des groupes reconnus sur la SSI (ex. ANSSI, CNIL, ASIP Santé, CLUSIF...) et les implications dans son offre/prestation/système.</p>	
11.2	O	<p>Toutes les prestations réalisées le sont soit à partir de la zone de l'Union Européenne, soit en respectant les règles définies par la CNIL pour les prestations hors zone de l'Union Européenne.</p>	

12. Protection des données médicales

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
12.1	O	Le titulaire et son personnel, le personnel du CHM 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.		Règle de sécurité	Description de la prise en charge par le titulaire
12.2	O	En conséquence, notamment, les jeux de données que le CHM serait amené à fournir sont strictement confidentiels et sont liés au secret professionnel.	
12.3	R	Un outil de codage des données est souhaité. Cet outil doit permettre de banaliser (anonymisation totale et/ou pseudonymisation) les informations de la base de données ou bien des fichiers de données pour préserver le secret médical.	
12.4	R	En outre, cet outil de codage doit pouvoir être utilisé pour préserver l'anonymat des personnes dans un environnement de test ou de formation.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

▪ Article R. 6113-9-2 du Code de la Santé Publique

« Les traces de tout accès, consultation, création et modification de données relatives aux patients sont conservées pendant une durée de six mois glissants par l'établissement de santé. »

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
12.5	O	Si l'objet de la prestation entre dans le périmètre du Décret n° 2018-1254 du 26 décembre 2018 relatif aux départements d'information médicale, le titulaire décrit de quelle manière son dispositif est conforme à l'article R. 6113-9-2 du Code de la Santé Publique.	

13. Cas particuliers selon le périmètre

▪ Cas de mise en œuvre de moyens mobiles

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.1	O	Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent être remises au CHM.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

- Cas de service hébergé en dehors du Système d'information de la DSI (pour tout ou partie) et cas de services installés dans le SI du CHM mais administrés en autonomie par le titulaire (cas SaaS)

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.2	O	<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>	
13.3	O	<p>Si des données de santé sont hébergées chez le titulaire ou un de ses sous-traitants celui-ci doit être agréé ou certifié hébergeur de données de santé par l'ASIP (ou toute commission compétente désignée par la réglementation).</p>	
13.4	O	<p>Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité. A cette fin <i>les clauses de sous-traitance RGPD du CH du Mans</i> sont annexées au contrat liant le CHM et le titulaire.</p>	
13.5	O	<p>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 sous-traitance du CH du Mans</i> annexées au contrat.</p>	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

-Accès au service hébergé par des utilisateurs du CHM :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.6	R	Un accès identifié, authentifié et habilité selon les conditions décrites dans les paragraphes précédents (Identité, Gestion des habilitations, Authentification et authentification unique) pour un logiciel installé dans le SI du CHM est fortement souhaité, en cas d'impossibilité technique, un identifiant sera communiqué aux utilisateurs ou un mode de gestion permettra à un utilisateur identifié comme administrateur des comptes utilisateurs de gérer les utilisateurs.	
13.7	O	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'ASIP (carte CPS ou équivalent).	
13.8	O	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données.	
13.9	O	Le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHM et accepte que Le CHM réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

-Continuité du service hébergé :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.10	O	Le service ne doit pas être indisponible plus que la durée décrite dans le CCTP ou de x heures . A défaut le fournisseur précisera les durées sur lesquelles il s'engage.	
13.11	R	Une copie exploitable des données (fichier informatique avec champs délimités et décrits) est transmise ou accessible régulièrement dans un délai décrit dans le CCTP ou tous les x jours . A défaut le fournisseur indiquera le délai possible. Il décrira le mode de mise à disposition.	

-Réversibilité du service hébergé :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.12	O	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise à Le CHM 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)	
13.13	O	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise à Le CHM en fin de contrat (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)	

Centre Hospitalier du Mans

Référentiel de Sécurité du Système d'Information

-Concernant La garantie de Confidentialité des données hébergées :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.14	O	Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins du CHM	
13.15	O	Les intervenants sont identifiés et doivent signer un engagement de confidentialité individuel. Les accès et actions réalisées pourront être tracés.	
13.16	O	Le titulaire s'engage à détruire les données en fin de contrat après les avoir restituées au CHM sous une forme exploitable.	

- Règles supplémentaires si la solution est installée dans l'infrastructure informatique du CHM mais administrée intégralement par le titulaire :

Ref.		Règle de sécurité	Description de la prise en charge par le titulaire
13.17	O	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.	
13.18	O	L'accès depuis l'extérieur du CHM pour l'exploitation et la maintenance doivent respecter les conditions décrites au paragraphe Maintenance et Télémaintenance.	
13.19	O	Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHM et accepte que Le CHM réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.	
13.20	O	Les échanges avec l'extérieur du CHM doivent être sécurisés : utilisation de protocoles sécurisés et filtrage et contrôle par les équipements de sécurité du CHM (Le CHM se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure.	

14. Glossaire des termes employés

AD (Active Directory) : Service d'annuaire de la société Microsoft

Application Web : Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques

EAI : L'intégration d'applications d'entreprise ou IAE(en anglais Enterprise Application Integration, **EAI**) est une application permettant à des applications hétérogènes de gérer leurs échanges.

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 système d'information

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

PKI (Public Key Infrastructure): Dispositif de gestion des clefs publiques. Permet l'édition des bi-clefs nécessaires au cryptage asymétrique.

RGPD : Règlement Général sur la Protection des Données.

SGBD : Dispositif de dépôt et d'indexation de données permettant l'adressage de grands volumes

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.

L'organisme paraphe toutes les pages et signe ce document

Fait à , le.../.../...

Pour l'organisme

(Nom et qualité du signataire et cachet de l'organisme)