	Direction du Système d'Information	
CENTRE HOSPITALIER - LE MANS	**Charte de bon usage du Système d'Information à destination des prestataires externes du Centre Hospitalier du Mans**	**Création :** 21 Janvier 2019 **Version 1.0** **Statut :** Applicable

Action	*Nom*	*Fonction*	*Visa*	*Date*
Rédaction	*Olivier Faglain*	*Responsable Sécurité du Système d'Information du GHT 72*		*21 Janvier 2019*
Vérification	*Stéphane Lemardeley*	*Directeur Technique des SI du GHT 72*		*07 Juin 2019*
Validation	*Conrad Breuer*	*Directeur du SI du GHT 72*		*07 Juin 2019*

Centre Hospitalier du Mans
Direction des Systèmes d'Information
194 avenue Rubillard
72037 LE MANS

SOMMAIRE

1 Préambule 2
2 Contexte Général 2
3 Cadre réglementaire 3
3.1 Respect de la Politique générale de Sécurité des Systèmes d'Information de Santé 3
3.2 Respect de la Politique la Politique de Sécurité des Systèmes d'Information de l'Etat 4
3.3 Conformité avec les exigences de la CNIL (Commission Nationale Informatique et Liberté) et du décret confidentialité et autres dispositions relatives à la confidentialité des données 4
3.4 Contrôles du SIH en matière de sécurité 5
4 Les objectifs de sécurité 6
5 Champ d'application 7
6 Dispositions de sécurité 10
6.1 Responsabilité 10
6.2 Confidentialité 11
6.3 Connexion d'équipement au Système d'information du Centre Hospitalier du Mans 13
6.4 Protection de l'information 13
6.5 Usage des outils de communication 14
6.6 Protection Antivirale 17
6.7 Authentification 17
6.8 Mises à jour et correctifs 18
6.9 Traçabilité, imputabilité 18
7 Acceptation de la Charte de bon usage du Système d'Information à destination des prestataires du CH du Mans 19
8 Glossaire : 20

1 Préambule

Cette charte a pour objet de préciser la responsabilité des structures sous quelque forme que ce soit (sociétés, organismes, autres établissements hospitaliers,...) ci-après désignées par le terme Prestataire Externe et ayant des personnels appelés à accéder au Système d'Information du Centre Hospitalier du Mans. Ce document est réalisé en accord avec la législation en vigueur afin d'instaurer un usage correct des ressources du système d'information du CH du Mans.

Ce document énonce les exigences du Centre Hospitalier du Mans en termes de sécurité vis-à-vis des 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 son Directeur Général et ci-après désigné par les termes « CH du Mans», « l'Etablissement » ou « CHM ».
- Le Prestataire Externe ci-après désigné, représente également ses sous-traitants ou cotraitants éventuellement appelés à participer à l'exécution de sa prestation.
- Les « utilisateurs » ci-après désignés sont les personnels des prestataires externes, de leurs sous-traitants ou cotraitants.

2 Contexte Général

L'évolution rapide et la standardisation des technologies ont tendance à faire disparaitre les barrières qui autrefois séparaient les différents domaines intervenant dans le fonctionnement d'un Etablissement de Santé (Equipements biomédicaux, Equipements Informatiques, Systèmes de gestion des installations techniques...).
La disparition de ces barrières a permis de créer un Système d'Information Hospitalier ou l'ensemble de ces équipements communiquent ou peuvent communiquer.
Le Système d'Information a donc pris une place de plus en plus importante au sein des Etablissements de Santé. Les Autorités de l'Etat ont pris conscience de l'impact des technologies numériques. Elles demandent aux établissements de s'assurer que toutes les mesures de sécurité soient prises pour minimiser les risques liés à cette évolution qui a pour effet d'accroitre les menaces pesant sur les informations conservées sous forme électronique et plus généralement sur les processus de production. Les Systèmes d'Information Hospitaliers représentant de plus en plus un maillon vital dans la prise en charge du patient, les exigences de sécurité demandées sont à la hauteur de l'enjeu.
Ces exigences auxquelles doivent faire face les Etablissements de Santé et donc indirectement leurs prestataires, ont été formalisées par différents textes officiels d'une part, et d'autre part sont soumises à contrôles réguliers de divers organismes ou instances.

3 Cadre réglementaire

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :
  - Le traitement de données à caractère personnel et le respect de la vie privée ;
  - Le traitement de données personnelles de santé ;
- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données médicales et l'échange ;
- Le secret professionnel et le secret médical ;
- La signature électronique des documents;
- Le secret des correspondances ;
- La lutte contre la cybercriminalité ;
- La protection des logiciels et des bases de données et le droit d'auteur.

3.1 Respect de la Politique générale de Sécurité des Systèmes d'Information de Santé

Le Ministère de la Santé au travers de l'Agence des Systèmes d'Information partagés de Santé (ASIP Santé) a élaboré la Politique Générale de Sécurité des Systèmes d'Information de Santé **(PGSSI-S V1.0) publiée en Juillet 2013** et applicable à tous les Systèmes d'Information de Santé (SIS).

La PGSSI-S tire parti des bonnes pratiques de sécurité issues notamment des documents de référence suivants :

- Le **Référentiel Général de Sécurité 1.0 (RGS)** élaboré par l'Agence Nationale de Sécurité des Systèmes D'Information (ANSSI) et rendu officiel par **arrêté du Premier ministre en date du 06 Mai 2010** et par extension **Le Référentiel Général de Sécurité 2.0** publié par **arrêté du Premier ministre en date du 13 Juin 2014**.

- Les **Normes ISO 2700X** définissant les règles de conception et mise en œuvre d'un système de gestion de la sécurité de l'Information

- **Guides de la CNIL** (Commission Nationale Informatique et Liberté.

Les responsables des SIS et les fournisseurs de solutions technologiques doivent appliquer tous les principes présentés dans la PGSSI-S et les guides ou référentiels élaborés par l'ASIP Santé pour appuyer la mise en application de la PGSSI-S.

L'Article 127 de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'Hôpital et relative aux Patients, à la Santé et aux Territoires précise que l'échange et le partage des données de santé doivent aussi respecter les référentiels de sécurité et d'interopérabilité définis par l'ASIP Santé.

3.2 *Respect de la Politique la Politique de Sécurité des Systèmes d'Information de l'Etat*

La Circulaire du Premier ministre N° 5725/SG - PRMX1420095C datée du 17 Juillet 2014 impose à toutes les administrations de l'Etat la mise en conformité de leur SI avec **la Politique de Sécurité des Systèmes d'Information de l'Etat** (PSSIE) élaborée par l'ANSSI.

La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans les SI, qu'il s'agisse des Administrations de l'Etat, de leurs agents **ou bien de tiers (prestataires ou sous-traitants) et de leurs employés**.

L' Arrêté du 1er octobre 2015 du Ministre de la Santé portant approbation de la politique de sécurité des systèmes d'information pour les **M**inistères **C**hargés des **A**ffaires **S**ociales (MCAS) précise les dispositions de la PSSIE. Cette PSSI-MCAS concerne les directions, Services centraux, les services déconcentrés, des ministères chargés des affaires sociales ainsi que les établissements placés sous leurs tutelles. Elle concerne également, par voie contractuelle ou conventionnelle toute personne physique ou morale tierce intervenant dans un système d'information dont l'activité concourt aux missions des MCAS (fournisseurs, prestataires de service, sous-traitants, employés, agents ...).

3.3 *Conformité avec les exigences de la CNIL (Commission Nationale Informatique et Liberté) et du décret confidentialité et autres dispositions relatives à la confidentialité des données*

L'article 34 de la loi du 6 janvier 1978 Modifiés par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004 précise que *« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

L'article 35 de la loi du 6 janvier 1978 Modifiés par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004 ajoute :

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. »

*« Le contrat liant **le sous-traitant au responsable du traitement** comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »*

Pour rappel **l'article 226-17 du code pénal** Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 prévoit que :

*« Le fait de procéder ou **de faire procéder** à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».*

Le **Décret confidentialité n° 2007-960 du 15 mai 2007** fixe les mesures de sécurité relatives à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique.

Enfin pour rappel, l'**article L1110-4 du Code de la Santé Publique**, Modifié par la **loi du n°2011-940 du 10 août 2011 - art. 2** indique que :

« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

*Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret 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**. »*

3.4 Contrôles du SIH en matière de sécurité

La Sécurité des Systèmes d'Information Hospitaliers est soumis pour tout ou partie à des contrôles réguliers dans les cadres suivants :

- Procédure de certification des établissements de santé et des structures visées aux **articles L.6133-7, L.6321-1, L. 6147-7 et L.6322-1 du Code de la santé publique**, menée par la Haute Autorité de Santé (HAS). **Les critères 5.a et 5b** portant plus précisément sur le système d'information.

- Inspection des Agences Régionales de Santé (ARS) dans le cadre du programme Hôpital Numérique évaluant la maturité du SIH sur les domaines identité-mouvements, fiabilité-disponibilité, confidentialité conformément **aux instructions DGOS/MSIOS/2012/376 du 31 Octobre 2012 et DGOS/MSIOS/2013/225 du 4 Juin 2013**.

- **L'Article 17 de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'Hôpital et relative aux Patients, à la Santé et aux Territoires** a inscrit dans le code de la santé publique (**article L. 6145-16**) le principe de la certification des comptes des établissements publics de santé par un commissaire aux comptes ou par la Cour des comptes. Pour préparer cette certification des comptes, la DGOS (Direction générale de l'Offre de Soins) a élaboré le « Guide Méthodologique pour l'Auditabilité des Systèmes d'Information » et l'a officialisé par **l'instruction DGOS/MSIOS/2013/62 en date du 21 février 2013**. Les Etablissements de Santé doivent répondre aux exigences de ce guide.

4 Les objectifs de sécurité

Le Système d'Information du Centre Hospitalier du Mans se définit par l'ensemble des données et des ressources matérielles, logicielles permettant de les stocker ou de les faire circuler. Le Système d'Information représente un patrimoine essentiel du CH du Mans, qu'il convient de protéger.
Le CH du Mans héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médicotechniques, ...), et sur les personnels (paie, gestion du temps, évaluations, accès à Internet et à la messagerie, ...).
L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone,...
La sécurité du Système d'Information, consiste à assurer que toutes ces ressources sont uniquement utilisées dans le cadre prévu.

La sécurité du Système d'Information vise généralement cinq principaux objectifs :

- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
- L'**intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La **non répudiation** et **la traçabilité** associée, permettant de garantir qu'une transaction ne peut être niée ;
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

Ces objectifs s'appliquent aux domaines suivants :

- La sécurité physique (accès aux locaux du CHM, aux salles informatiques ...) ;
- La sécurité logique reposant sur la mise en œuvre d'un système de contrôle d'accès s'appuyant sur un service d'authentification, d'identification et d'autorisation, mais aussi sur la mise en place de dispositifs de cryptage des données, d'antivirus et une gestion efficace des mots de passe ;
- La sécurité d'exploitation comprenant la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance ou télémaintenance, de test, diagnostic et de mise à jour;
- La sécurité des télécommunications reposant sur la mise en place d'infrastructures réseau sécurisées entre les différentes parties liées au SI du CH du Mans;

Ainsi, pour garantir la sécurité de son Système d'Information ou tout du moins réduire les risques de dommages pouvant l'affecter, le Centre Hospitalier du Mans, impose à ses prestataires, des exigences de sécurité.

Les exigences de sécurité imposées aux partenaires, fournisseurs et prestataires de services sont en accord avec les dispositifs législatifs et réglementaires énoncés dans le paragraphe « 3 Cadre Réglementaire » du présent document.

Pour rappel **le Code Pénal**, notamment les **articles 323-1 à 323-7**, prévoit les sanctions pour toutes actions portant atteinte aux systèmes de traitement automatisé de données.

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources du Système d'Information et des services Internet du CH du Mans et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans son utilisation.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement

5 Champ d'application

Définition **Système d'information :** ensemble des moyens humains, matériels et immatériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

En conséquence, la présente Charte couvre l'ensemble des systèmes d'information du CH du Mans. Cela implique une forte diversité à la fois dans les lieux d'utilisation, les personnes concernées et les usages rencontrés. Le niveau de sécurité à appliquer doit être considéré en fonction du type de fonctionnalités, du type de données concernées (vitales pour le fonctionnement de l'établissement, à caractère nominatif,

données de santé, relevant de l'espace privé...) et des interactions existantes entre les systèmes ou les réseaux.

En termes d'actifs, le périmètre du présent document inclut notamment :

Les actifs matériels :

- Les serveurs hébergeant les systèmes d'information dédiés à l'administration de l'établissement (comptabilité, ressources humaines, restauration du personnel...) ;
- Les dispositifs médicaux connectés;
- Les dispositifs médicaux non connectés dès lors qu'ils intègrent un stockage de données de santé nominatives ;
- Les serveurs hébergeant les système d'information dédiés à la production de soins (Dossier Patient Informatisé, Gestion Administrative du patient, Système de Gestion de Laboratoire, Système de Gestion du Service d'urgences ...) ;
- les serveurs hébergeant les systèmes d'information dédiés à la communication (messagerie, web, échanges de données...) ;
- les équipements dédiés à la gestion de service (téléphonie, réseau informatique, contrôle d'accès...) ;
- les systèmes d'information des services et les entités à usage personnel (ordinateur fixe ou portable, ordiphone, tablettes, logiciels bureautiques, de traitements de données) fournis ou non par l'établissement ;
- les systèmes de support de l'information (disques, CD, DVD, clé USB, documents papiers...) et d'impression (imprimantes, photocopieurs...) ;
- les réseaux de communication internes à l'établissement, filaires ou non, à vocation d'échange de données informatiques mais aussi de téléphonie, de visioconférence, de télésurveillance ;
- les réseaux de communication inter-sites, filaires ou non ;
- l'usage d'un moyen informatique privé ou extérieur connecté au réseau de l'établissement ;

Remarque : Tous les matériels mobiles appartenant à l'Etablissement ou fournis par l'Etablissement sont partie intégrante du périmètre de ce document, même lorsqu'ils sont utilisés hors des sites du CHM.

Les actifs immatériels :

- les données administratives liées à la gestion (ressources humaines, données comptables, gestion des stocks...) ;
- les données médicales liées aux personnes (Dossier Patient Informatisé, Gestion Administrative du patient, Système de Gestion de Laboratoire, Système de Gestion du Service d'urgences ...) ;
- Les données nominatives stockées sur des dispositifs médicaux connectés ou non ;
- les données liées à l'activité de recherche réalisée au sein de l'établissement y compris au titre de collaborations ou de contrats. Cela inclut les données destinées à la publication ou à la vulgarisation (livres, photographies, films...) ;
- les données liées à l'activité de l'Institut de Formation des Professionnels de Santé (supports de cours...) ;
- les données associées aux services gérant les échanges d'informations (téléphonie, informatique...) ;
- les données associées à la gestion de la sécurité des personnes et des biens (contrôle d'accès, hygiène et sécurité...) ;
- et d'une manière plus générale toutes les données et prestations associées à l'établissement ;

Remarque : les données propres à l'établissement se trouvant hors de l'établissement (sur des matériels mobiles par exemple) sont partie intégrante du périmètre du présent document.

6 Dispositions de sécurité

6.1 Responsabilité

Article 1

Le Prestataire Externe sera soumis à une obligation de résultat pour l'ensemble de ses engagements en matière de sécurité au titre de sa prestation.

Article 2

Pour les prestations entrant dans le périmètre de sous-traitant du Règlement Général sur la Protection des Données (RGPD) , les documents suivants devront être retournés (au format électronique) au CH du Mans, signés et paraphés sur toutes leurs pages par le représentant légal de la société prestataire avant toute délivrance de prestation :

- Le présent document,
- Les clauses de conformité au RGPD du CH du Mans,
- le document **REFERENTIEL DE SECURITE DU SYSTEME D'INFORMATION** en annexe 1 des clauses de conformité au RGPD,
- Les conventions d'accès signés par les salariés du prestataire accédant au SI du CHM.

Pour les prestations n'entrant pas dans le périmètre de sous-traitant du Règlement Général sur la Protection des Données (RGPD) , les documents suivants devront être retournés (au format électronique) au CH du Mans, signés et paraphés sur toutes leurs pages par le représentant légal de la société prestataire avant toute délivrance de prestation :

- Le présent document,
- le document **REFERENTIEL DE SECURITE DU SYSTEME D'INFORMATION** en annexe 1.
- Les conventions d'accès signés par les salariés du prestataire accédant au SI du CHM.

Article 3

Le Prestataire Externe désignera en son sein un interlocuteur responsable de la Sécurité du Système d'Information, ainsi qu'un suppléant dans le cadre de l'exécution de sa prestation. Ce responsable sécurité, sera l'interlocuteur privilégié du CH du Mans durant la durée d'exécution de sa prestation, pour tous les aspects de sécurité du Système d'Information.

Article 4

En cas de recours à un ou plusieurs sous-traitant(s), le Titulaire devra en aviser le CHM. Les sous-traitants éventuels auront les mêmes obligations que le Titulaire en ce qui concerne la satisfaction aux exigences de sécurité du CHM. Ces obligations devront être contractualisées par l'acceptation écrite par le(s) sous-traitant(s) des documents précités à l'article 2 du présent document. Le Titulaire sera le garant de la bonne application par son ou ses sous-traitant(s) des règles de sécurité énoncées. En cas de cotraitance, chaque cotraitant s'engage à répondre contractuellement aux mêmes obligations.

Article 5

Le Prestataire Externe s'engage à alerter l'établissement de toute menace ou vulnérabilité dont il aurait connaissance.

De manière générale, tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la Sécurité du Système d'Information ou manquement substantiel à cette charte doit être signalé.

Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle des personnels du CH du Mans soient respectées.

Article 6

Il est de la responsabilité du Prestataire Externe de communiquer au CH du Mans, toute modification de sa situation administrative (ex : changement de raison sociale, changements de coordonnées,...), dés connaissance du changement par le titulaire avec précision de la date d'effet.

6.2 Confidentialité

Article 7

Chacune des parties s'interdira, pendant la durée de la prestation et suivant le terme ou la résiliation de celle-ci, de divulguer à des tiers, directement ou indirectement, les informations de nature « confidentielle », ce terme recouvrant toutes informations ou données qu'elle aura reçu de l'autre partie, ou qu'elle aura reçu pour le compte de l'autre partie, ou dont elle aurait pris connaissance dans le cadre de la prestation.

Article 8

Le Prestataire Externe se portera garant du respect par son personnel de cette obligation de confidentialité.

Article 9

Chacune des parties s'interdira, pendant la durée de la prestation et suivant le terme ou la résiliation de celle-ci, d'utiliser lesdites informations à d'autres fins que l'exécution de celle-ci, ainsi que de les communiquer à des membres de son personnel et sous-traitants éventuels n'ayant pas le besoin d'en connaître.

Article 10

Le Prestataire Externe certifiera que les informations en sa possession concernant les travaux effectués dans le cadre de sa prestation, que les données financières ainsi que les données à caractère personnel manipulées pour produire les différents documents objets de la prestation seront supprimées de tout support informatique et qu'il ne conservera aucune édition ou copie à l'issue du contrat le liant au CH du Mans. Le Prestataire Externe devra à l'issue du contrat le liant au CHM, procéder à la destruction de toutes données numériques en sa possession, appartenant à l'Etablissement. La preuve de cette destruction sera apportée par une attestation sur l'honneur du prestataire externe.

Article 11

Le Prestataire Externe, respectant ses engagements en matière de sécurité, mettra en œuvre toutes actions nécessaires afin d'assurer la confidentialité des informations, données et traitements, et au même niveau de précaution qu'il prend pour protéger ses propres informations confidentielles.

Article 12

Les données du CHM sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont le prestataire externe prend connaissance à l'occasion de l'exécution de sa prestation.

Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels des prestataires externes se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

Article 13

Le Prestataire Externe s'engage à respecter les obligations suivantes et à les faire respecter par son personnel et par ses sous-traitants :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue au contrat; l'accord préalable du propriétaire du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- ne pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques ;
- ne pas nuire à l'image de marque de l'établissement en utilisant des informations acquise dans le cadre de la prestation effectuée.

Article 14

En cas de non-respect des clauses de confidentialité du présent document, la responsabilité du Prestataire Externe peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

Le CH du Mans pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du Prestataire Externe, en cas de violation du secret professionnel ou de non-respect des clauses de confidentialité du présent document.

Article 15

Le Prestataire Externe renoncera à publier, reproduire, traduire ou mettre sur le marché des éléments dont il aura cédé les droits, il est seulement autorisé à faire état dans ses références professionnelles de l'existence et du contenu succinct de la prestation réalisée.

6.3 *Connexion d'équipement au Système d'information du Centre Hospitalier du Mans*

Article 16

La connexion d'équipements non référencés et non homologués par la Direction du Système d'Information du CH du Mans est interdite sur les réseaux informatiques de l'Etablissement. Une dérogation peut être obtenue par autorisation expresse et écrite de la Direction du Système d'Information du CHM.

Article 17

Il est strictement interdit de connecter un équipement présent sur le réseau de l'établissement, à un réseau privé ou à Internet via un modem ou un équipement similaire.

6.4 *Protection de l'information*

Dans le cas où le prestataire externe serait amené à travailler physiquement dans les locaux du CHM sur des postes de travail mis à disposition par l'Etablissement ou non, les dispositions de l'article 18 ci-après sont applicables :

Article 18

- Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux).les documents bureautiques produits doivent être stockés sur des serveurs de fichiers.
- Les ressources de stockage réseau sont à usage professionnel uniquement. Le stockage de données privées y est interdit.
- Par ailleurs, l'utilisateur est responsable de ses sauvegardes. La restauration de documents perdus enregistrés sur le PC et non sur le réseau n'est pas garantie.
- Le cas échéant, en cas de mise à disposition d'un matériel portable (exemples : poste, tablette, smartphone, ...), celui-ci ne doit pas être mis en évidence pendant un déplacement, et son contenu ne doit pas être exposé à la vue d'un tiers (voisin de train par exemple).
- L'utilisateur ne doit jamais transporter des fichiers qui auraient un caractère sensible ou une valeur stratégique pour le CHM sur un équipement mobile quel qu'il soit.

- Le matériel doit être rangé en lieu sûr (sous clé). De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, clé, disque dur, ...).
- Lorsque l'on quitte son espace de travail, Il faut également mettre sous clé tout dossier ou document confidentiel, fermer ou au moins verrouiller la session ouverte sur son poste.
- Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.
- Les medias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs ...) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit être fait avec une très grande vigilance. L'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.
- L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne au CHM.
- Il convient que lors de l'utilisation d'un poste de travail libre-service, l'utilisateur soit vigilant sur les données qu'il pourrait stocker sur ledit poste et sur les traces informatiques qu'il pourrait laisser (mot de passe enregistrés par exemple).

6.5 *Usage des outils de communication*

Dans le cas où le prestataire externe serait amené à utiliser les outils de communication du CHM, les dispositions des articles 19, 20, 21, 22 et 23 sont applicables :

Article 19 : généralités

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre du droit du salarié à sa liberté résiduelle et des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de l'établissement de santé. Il ne doit en aucun cas être porté à la vue des patients ou de visiteurs et accompagnants.

Article 20 : usage du téléphone et du fax

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.

Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après

avoir vérifié l''identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou professionnels.
La communication d'informations médicales (exemples : résultats d'examens, ...) aux patients et aux professionnels extérieurs est strictement réglementée. Les utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'Etablissement en vigueur.
En cas d'envoi de fax via des photocopieurs du CHM, l'utilisateur s'assurera de ne laisser aucune traces de ses envois sur l'appareil utilisé et/ou sur des partages réseau.

Article 21 : usage d'Internet

L'accès à l'Internet a pour objectif d'aider les utilisateurs à trouver des informations nécessaires à leur mission usuelle.
Il est rappelé à l'utilisateur que, lorsqu'il « navigue » sur l'Internet, son identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et à ne pas mettre en danger l'image ou les intérêts du CHM.
Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur, ...) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc interdit à l'utilisateur de fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.
Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.
Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque utilisateur, le détail de son activité sur l'Internet.
Selon l'article 6 de la loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 et la loi relative à la lutte contre le terrorisme, ces traces sont conservées pour une durée de un an.
Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.
La Direction du Système d'Information est habilitée à consulter les fichiers journaux individuels dans la mesure où la sécurité, le bon fonctionnement du Système d'information est remis en cause.
D'autre part en référence au cas de jurisprudence Martin Cass. Soc. Du 09-07-2008 précisant que « les connexions établies par un salarié sur des sites internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de *les identifier, hors de sa présence* », la Direction du Système d'Information peut communiquer sur demande, ces informations à la Direction du CHM ou à la Direction du Prestataire Externe pour lequel travaille l'utilisateur concerné.

Article 22 : usage de la messagerie

Une messagerie électronique peut être mise à disposition d'un Prestataire Externe pour mener au mieux son activité professionnelle.

L'utilisateur doit garder à l'esprit que ses messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre l'hôpital et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

L'usage des listes de diffusion doit être strictement professionnel.

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou de porter atteinte à son image. L'utilisateur est tenu par les clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'il transmet par courriel.

La diffusion de tract par messagerie est interdite, le SPAM est interdit, L'ouverture de courriels assimilés à du SPAM est à proscrire.

Afin de ne pas surcharger les serveurs de messagerie, l'utilisateur doit veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé. Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

L'usage des forums de discussions répond aux mêmes règles de bon usage que la messagerie électronique.

Article 23: usage des photocopieurs

Dans le cas où le Prestataire Externe, ou son personnel utiliserait les moyens de reprographie du CHM, il devra s'assurer de ne laisser aucune trace/document sur les disques des photocopieurs ou sur les ressources de stockage réseau.

6.6 *Protection Antivirale*

Article 24

En cas d'utilisation d'équipement appartenant au Prestataire Externe, la station avec laquelle celui-ci ou ses personnels intervient doit être exempte de virus et à jour des divers correctifs de sécurité.

Article 25

Aucun logiciel de prise en main à distance (exemples Logmein ou Teamviewer) ne doit être installé et/ou utilisé par le Prestataire Externe sans que celui-ci n'y ait été autorisé explicitement (autorisation écrite) par la Direction du Système d'Information du CHM.
Le Prestataire Externe et ses personnels n'installeront aucune porte dérobée ou ouverte sur les postes, encore moins sur les serveurs.

6.7 *Authentification*

Article 26

Les identifiants des comptes d'accès utilisés pour se connecter au Système d'information du CHM, par le Prestataire Externe ou son personnel sont nominatifs.

Article 27

Le Prestataire Externe s'engage à ne pas céder à d'autres personnes que celles déclarées les codes d'accès et à faire appliquer cette règle à son personnel;

Article 28

Le Prestataire Externe s'engage à ce que son personnel intervienne uniquement sur les ressources déclarées.

Article 29

Le Prestataire Externe devra veiller à ce que son personnel ne configure pas les applications logicielles utilisées pour se connecter sur le Système d'Information du CHM, afin qu'elles permettent d'enregistrer les mots de passe.

Article 30

Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels.
L'utilisateur s'engage à signaler toute tentative de violation de son compte personnel.
De même, le Prestataire Externe s'engage à signaler tous cas de compromission ou suspicion de compromission des comptes d'accès fournis pour accéder au SIH du CHM.

6.8 Mises à jour et correctifs

Article 31

Le Prestataire Externe ne peut modifier le paramétrage ni prendre de décisions d'exploitation des logiciels, applications ou matériels en production sans en avertir son interlocuteur au Centre Hospitalier du Mans et sans son accord.

Article 32

Le Prestataire Externe ne peut modifier des données sans en avoir préalablement informé la ou les personnes du Centre Hospitalier du Mans qui lui ont été désignées pour l'accompagner dans ses actions et sans leur accord.

Article 33

Le Prestataire Externe s'engage à informer le CHM des risques d'une opération envisagée, des incidents éventuels et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Le Prestataire Externe s'engage à informer préalablement le CHM de toute opération susceptible de provoquer l'indisponibilité ou la dégradation des performances du système.

6.9 Traçabilité, imputabilité

Article 34

Le Prestataire Externe ne peut effacer les fichiers traces ou log (fichiers générés en standard par exemple par une application) sans autorisation de la ou les personnes du Centre Hospitalier du Mans qui lui ont été désignée(s) pour l'accompagner dans ses actions.

Article 35

Concernant le journal des connexions à distance exigé [**reference**] dans le référentiel de sécurité du système d'information :

- Le Prestataire Externe devra conserver ces traces de connexions sur une période d'au moins 18 mois glissants à partir de la première connexion.
- La demande de ce journal de connexion sera effectuée par tous moyens jugés adéquats par le CHM. Cette demande pourra être effectuée par le Directeur général du CHM, le Directeur du Système d'Information ou le Responsable Sécurité du Système d'Information.

7 Acceptation de la Charte de bon usage du Système d'Information à destination des prestataires externes du CH du Mans

- A remplir par le représentant légal de la société prestataire -

Si votre société dispose d'un Responsable Sécurité du Système d'Information merci d'indiquer ses coordonnées : **Nom/Prénom :** **Téléphone :** **Adresse Courriel :**
Merci d'indiquer les coordonnées de l'interlocuteur responsable de la sécurité de la prestation et celles de son suppléant : **Nom/Prénom :** **Nom/Prénom :** **Téléphone :** **Téléphone :** **Adresse Courriel :** **Adresse Courriel :**
Lu et approuvé **Pour la Société :** **Nom/Prénom :** **Fonction :**
Date : **Signature et tampon.**

8 Glossaire :

ARS : Agence Régionale de Santé

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

ASIP Santé : Agence des Systèmes d'Information Partagés de Santé

CNIL : Commission Nationale Informatique et Liberté

DGOS : Direction Générale de l'Offre des Soins

DSI : Direction du Système d'Information

HAS : Haute Autorité de Santé

LESSIS : Fédération des Entreprises des Systèmes d'Information Sanitaires et Sociaux

MCAS : Ministères Chargés des Affaires Sociales (dans le cadre de la PSSI-MCAS comprendre les ministères des affaires sociales, de la santé et des droits des femmes, du travail, de l'emploi, de la formation professionnelle et du dialogue social, de la ville, de la jeunesse et des sports

PAS : Plan d'Assurance Sécurité

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

PSSIE : Politique de Sécurité des Systèmes d'Information de l'Etat

RGS : Référentiel Général de Sécurité

SIH : Système d'Information Hospitalier

SIS : Systèmes d'Information de Santé