CHARTE D'ACCÈS AU SYSTEME D'INFORMATION DU CENTRE HOSPITALIER DE CHAUNY

VERSION 2 – JANVIER 2025

SOMMAIRE

SUIVI DU DOCUMENT

Rédaction	Vérification	Approbation
Mme Lydie Sorton, Informaticienne	Mme Corinne POURRIER, RAQ	M. Joël LOUISY, Directeur du Système d'Information Hospitalier
Date et Signature : 3 Janvier 2025 SIGNE	Date et Signature : 3 Janvier 2025 SIGNE	Date et Signature : 3 Janvier 2025 SIGNE

1. OBJET DU DOCUMENT

La présente charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du Centre Hospitalier de CHAUNY et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

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 et au Règlement Général sur la Protection des Données (RGPD) en vigueur depuis mai 2018.

Cette charte a été validée par la Direction générale de l'établissement. Préalablement à sa mise en œuvre, elle a été notifiée au Comité Local de Coordination, au Comité Social d'Établissement ainsi que la Commission Médicale d'Etablissement. Les membres du personnel et les personnels extérieurs doivent en prendre connaissance. La charte est remise aux membres du personnel au moment de leur embauche, et mise à leur disposition dans le logiciel de gestion documentaire.

Cette charte a fait l'objet de travaux communs au sein du Groupement Hospitalier de Territoire (GHT) auquel appartient l'établissement, afin d'harmoniser les pratiques d'accès et d'usage du SI des établissements et de faciliter l'utilisation des SI hospitaliers par les personnels qui exercent dans plusieurs structures au sein du groupement.

2. CHAMP D'APPLICATION

La présente charte concerne les ressources informatiques, les services Internet et téléphoniques du Centre Hospitalier de CHAUNY, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électroniques interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau ;
- Ordinateurs portables ;
- Terminaux portables ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- Serveurs , Echographes, Radio

Cette charte s'applique à l'ensemble des professionnels de l'établissement de santé, tous statuts confondus, permanents ou temporaires (stagiaires, internes, prestataires, fournisseurs, sous-traitants, bénévoles…) utilisant les moyens informatiques de l'établissement. Elle concerne aussi les personnes ayant accès au système d'information à distance, directement ou à partir du réseau administré par l'établissement.

Dans la présente charte, sont désignés sous les termes suivants :

- **Ressources informatiques** : les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité ;
- **Outils de communication** : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, forum, etc.) ;
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services Internet de l'établissement.

3. CADRE REGLEMENTAIRE

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 ;
- 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.

La présente charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1. Principes

L'établissement de santé héberge des données**,** des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques…), 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 de l'information** est caractérisée comme étant la préservation de :

- **Sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin ;
- **Son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie ;
- **Sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder ;
- **Sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2. Une mission sécurité

La Direction du Système Information et Organisation fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble, c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont bien au service de la production de soins. Elle doit donc caractériser et empêcher les abus.

4.3. Un enjeu technique et organisationnel

Les enjeux majeurs de la sécurité sont la qualité et la continuité des soins, le respect du cadre juridique sur l'usage des données personnelles de santé.

Pour cela La DSIO déploie un ensemble de dispositifs techniques, mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

4.4. Une gestion des risques

L'information médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients. Une information manquante, altérée ou indisponible, peut constituer une perte de chance pour le patient (exemples : erreur dans l'identification d'un patient [homonymie par exemple], perte de données à la suite d'une erreur d'utilisation d'une application informatique…). La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente charte d'accès et d'usage du système d'information s'inscrit dans ce plan de communication.

5. REGLES DE SECURITE

L'accès au système d'information de l'établissement est soumis à autorisation. Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la demande exprimée par l'utilisateur est au préalable validée par le cadre hiérarchique, qui précise les accès nécessaires à son collaborateur, et la transmet par écrit à la DSIO.

Le service informatique attribue alors au demandeur son droit d'accès et lui communique la présente charte d'accès et d'usage du système d'information. Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cessation, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente charte par l'utilisateur.

L'obtention d'un droit d'accès au système d'information de l'établissement de santé entraîne pour l'utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

Tout utilisateur est responsable à titre personnel de l'usage qu'il fait des ressources informatiques. Il doit particulièrement veiller à ne pas détourner les moyens informatiques de l'usage professionnel pour lequel ils sont mis à disposition.

5.1. Confidentialité de l'information et obligation de discrétion

Les personnels de l'établissement sont soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels doivent 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.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux qui sont publics ou partagés. 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 électronique dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.

Les données financières et les informations liées au personnel appartiennent à l'établissement et ne doivent être utilisées que dans le cadre strict des usages prévus lors de leur constitution. L'utilisateur doit veiller à la discrétion et à la non diffusion de ces données.

5.2. Protection de l'information

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Les bases de données associées aux applications sont implantées sur des serveurs centraux situés dans des salles protégées. De même, les documents bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smartphone…) ne doivent pas le mettre en évidence pendant un déplacement ni exposer son contenu à la vue d'un voisin de train… ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, clé USB, disque dur USB…). Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les médias de stockage amovibles (exemples : clés 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 faire l'objet d'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 connaîtrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement.

5.3. Usages des ressources informatiques

Seules des personnes habilitées de l'établissement de santé (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et, plus globalement, d'installer de nouveaux matériels informatiques.

L'utilisateur s'engage à ne pas modifier la configuration des ressources mises à sa disposition (matériels, réseaux…)

L'établissement prend toutes dispositions techniques pour protéger son réseau et son SIH des intrusions ou malveillances externes. L'utilisateur est tenu de ne pas mettre en péril ces dispositifs par l'introduction de matériels de communication sans un accord préalable express du Service Informatique. En particulier, la connexion de modems ou de dispositifs de réseau sans fil (Wifi, Bluetooth) permettant un accès externe est interdite.

Il est interdit d'apporter, volontairement ou non, des perturbations au bon fonctionnement des postes de travail, des réseaux et des systèmes, que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques, logiciels d'écoute du réseau, etc.) ou par le contournement de règles de sécurité (exemple : arrêt de l'antivirus).

Les logiciels commerciaux acquis par l'établissement ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement.

- **Le poste de travail**

Dans le cadre de sa mission, un collaborateur peut se voir fournir un ou plusieurs postes de travail, fixes ou nomades. Il est de son devoir d'appliquer les règles de bonne pratique liées à ce type de matériel. Notamment,

Le collaborateur doit :

- Veiller à conserver en bon état de fonctionnement le matériel et les logiciels mis à sa disposition ;
- Veiller à ce que les règles de verrouillage de session soient bien appliquées sur son matériel ;
- Signaler tout dysfonctionnement ou anomalie sur le matériel ;
- S'engager à sécuriser son matériel avec les moyens mis à disposition par la structure (système antivol, etc.).

Le collaborateur ne doit pas :

- Utiliser les équipements pour un usage personnel, sauf dans les limites fixées par la structure si elle l'a autorisé explicitement ;
- Faire usage de postes de travail pour lesquels il n'a pas été explicitement autorisé.

- **Les logiciels et les applications**

L'utilisation de logiciels du commerce est soumise au respect du code de la propriété intellectuelle défini par le législateur.

Chaque collaborateur doit avoir conscience :

- Que l'utilisation de logiciels est soumise à l'acquisition par l'entreprise de licences d'utilisation ;
- Que la loi protège les logiciels contre la copie ;
- Que sa responsabilité civile et pénale sera engagée en cas de copie non autorisée ou de piratage de logiciel ;
- Qu'aucune installation de logiciel piraté sur le poste de travail, même pour utilisation à titre personnel, ne sera admise.

- **Les équipements mobiles de stockage**

L'usage de périphériques type clés USB ou disques externes doit rester exceptionnel. Seuls les périphériques de stockage fournis par la structure sont autorisés.

5.4. Usages des outils de communication

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 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.

- **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 de 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'établissement en vigueur.

- **Usage d'Internet**

L'accès à l'Internet a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.

Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur l'Internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et de ne pas mettre en danger l'image ou les intérêts de l'établissement de santé.

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 recommandé à chaque utilisateur de ne pas 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.

Il est également interdit de participer à des jeux de hasard, d'argent, ou de s'impliquer dans le blanchiment d'argent au moyen d'Internet.

Tous les accès Internet sont tracés, enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment les 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.

- **Usage de la messagerie électronique**

L'ensemble des principes et règles édictés par la présente charte s'applique à l'utilisation de la messagerie électronique « Outlook ».

La messagerie permet de faciliter les échanges entre les professionnels de l'établissement ainsi qu'entre les professionnels et des tiers. Dans le cadre de leur activité professionnelle, ces derniers se voient attribuer une messagerie électronique.

Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant. Cela pourait constituer une preuve ou un commencement de preuve valant 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. À 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 porter atteinte à son image. Selon les droits et obligations de la fonction publique, les utilisateurs sont tenus par leurs devoir de confidentialité et de loyauté contractuelles qui encadrent le contenu des informations qu'ils peuvent transmettre par email.

Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs doivent 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.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer le service informatique des dysfonctionnements qu'ils peuvent être amenés à rencontrer dans le dispositif de filtrage.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message, leur qualité à recevoir la communication des informations transmises ainsi que le contenu de ces messages. En cas d'envoi à un nombre important de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi massif de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

Les risques de retard, de non remise, et de suppression automatique des messages électroniques doivent être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception.

- **Usage de la messagerie sécurisée de santé (MSS)**

Ce service assure les échanges entre utilisateurs par voie électronique en garantissant la sécurité, la traçabilité et la confidentialité des données de santé à caractère personnel.

Les utilisateurs s'engagent à respecter les dispositions figurant à l'article L. 1110-4 du code de la santé publique relatives aux conditions d'échange de données de santé entre deux ou plusieurs professionnels de santé.

Le service de messagerie sécurisée ne se substitue en aucun cas au dossier médical, sanitaire ou médico-social des personnes concernées (les patients) que doivent tenir les professionnels habilités en vertu des obligations légales et règlementaires qui leur incombent. Il constitue uniquement un outil professionnel d'échange sécurisé de données de santé, et non un nouvel espace de stockage.

Le fonctionnement de ce service repose sur l'utilisation d'annuaires qui permettent d'authentifier et identifier les utilisateurs habilités. Ils permettent également aux utilisateurs de retrouver des correspondants.

L'utilisateur s'engage à utiliser les données contenues dans les annuaires dans le strict respect du cadre de ses fonctions et dans un but exclusivement professionnel. Ceci exclut tout particulièrement toute démarche commerciale ou publicitaire, politique ou religieuse.

L'utilisateur est informé qu'en utilisant le service MSSanté, s'il n'est pas déclaré en liste rouge, il accepte de figurer dans les Annuaires et que soient inscrites dans ceux-ci des informations le concernant (Nom, Qualité, Adresse, Téléphone, Adresse mail, Profession, Spécialité, Numéro ADELI, Identifiant RPPS, Structure de rattachement) permettant aux autres utilisateurs de la messagerie de l'identifier et d'échanger des messages sécurisés avec lui.
Également, l'utilisateur est informé qu'il conserve la possibilité de modifier, supprimer ou rectifier des informations le concernant. L'utilisateur accepte également que ces informations soient accessibles aux autres utilisateurs par le moyen des annuaires.

Ce service de messagerie réservé aux professionnels de santé et aux professionnels médico-sociaux est accessible uniquement après vérification de la qualité professionnelle de l'utilisateur. L'accès à la messagerie se fait au moyen d'une authentification forte de type carte CPS ou équivalent. Les identifiants de connexion sont strictement personnels et placés sous la seule responsabilité de l'utilisateur. Il appartient à chaque utilisateur de mettre en œuvre toutes les mesures de sécurités nécessaires à la protection de ces identifiants et à ne les divulguer sous aucun prétexte et à quelque titre que ce soit.

La préservation de la sécurité des données à caractère personnel et des données de santé engage chaque utilisateur à :

- Ne jamais communiquer de données de santé par messagerie non sécurisée ;
- Garder strictement confidentiels ses éléments d'authentification et ne pas les dévoiler à un tiers.

5.5. Usages des logins et des mots de passe (ou de cartes CPS ou équivalents)

Chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant, ou en tentant d'utiliser, le compte d'un autre utilisateur, ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur, soit dispose d'un login et d'un mot de passe, soit utilise une carte CPS ou équivalent (avec un code personnel à 4 chiffres)

Le mot de passe choisi doit être robuste (12 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé tous les 6 mois. Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.

Chaque utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médicales et médicotechniques, les applications administratives, le réseau, la messagerie, l'Internet… Il est ainsi possible pour l'établissement de vérifier *a posteriori* l'identité de l'utilisateur ayant accédé ou tenter d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir.

Il est interdit de contourner, ou de tenter de contourner, les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.

En cas d'oubli du mot de passe, ou de difficulté de connexion, le Service Informatique fournit la marche à suivre pour que l'utilisateur puisse à nouveau se connecter en toute sécurité.

L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

5.6. Image de marque de l'établissement

Les utilisateurs ne doivent pas nuire à l'image de marque de l'établissement à travers la communication d'informations à l'extérieur, via les moyens informatiques auxquels ils ont accès, en interne ou en externe, ou du fait de leur accès à Internet.

Le personnel de l'établissement, soumis en toutes circonstances au respect des règles de secret professionnel, de discrétion professionnelle et de devoir de réserve, doit redoubler de vigilance dans l'utilisation des réseaux sociaux dont la finalité reste du domaine exclusivement privé (article 9 du Code civil).

5.7. Dispositions spécifiques à l'usage des internes en médecine en dehors de l'activité professionnelle

La présente charte s'applique dans les mêmes termes, pour les internes, en dehors de leur temps de travail et dans le cadre de l'utilisation personnelle des outils mis à leur disposition par l'établissement.

L'utilisation de la connexion internet à partir de leurs ordinateurs personnels leur permet d'accéder aux sites de leur libre choix conformément au paragraphe 5.4 de la présente charte et aux dispositions des codes civil et pénal.

6. PROTECTION DES DONNEES PERSONNELLES

L'établissement doit se conformer aux procédures liées à l'entrée en vigueur du règlement général de la protection des données (RGPD), et notamment :

- **Désigner un délégué à la protection des données (DPO/DPD**)
- **Informer les personnes concernées par un traitement de données** (patients, personnes participant à une recherche, etc.) : l'information doit être délivrée de façon concise, transparente, compréhensible et aisément accessible. Elle doit pouvoir être abordable par le « grand public ».
- **Tenir un registre décrivant les traitements** mis en œuvre et les mesures de mise en conformité de ces traitements. Dans certains cas (notamment les traitements de recherche), il doit solliciter l'autorisation de la CNIL avant de mettre en œuvre son traitement de données personnelles : il doit dans ce cas en informer préalablement le DPO ;
- **Réaliser une analyse de l'impact du traitement de données,** portant tant sur les risques sécurité et techniques que sur les risques juridiques pour les personnes, avant de mettre en œuvre certains traitements, notamment ceux portant sur des données de santé à grande échelle (dispositifs de télémédecine, traitements portant sur les dossiers des résidents pris en charge par un EPHAD, etc.). La liste des types de traitements pour lesquels une analyse d'impact est requise est disponible sur le site de la CNIL.

6.1. Devoirs des utilisateurs

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit « RGPD ».

Les utilisateurs du système d'information de l'établissement de santé sont soumis à plusieurs obligations en ce qui concerne les modalités de mise en œuvre du traitement des données à caractère personnel. De façon générale, les utilisateurs doivent respecter les principes de protection des données de santé et des données à caractère personnel suivants :

- Le respect des finalités initiales du traitement ;
- La pertinence et l'exactitude des données au regard des finalités poursuivies ;
- L'information des personnes concernées ;
- Les droits des personnes concernées ;
- La protection adaptée aux risques présentés par le traitement sur les plans technique et organisationnel ;
- Le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs.

Dans le cadre de l'utilisation des systèmes d'informations couverts par la présente charte, les utilisateurs devront se conformer à l'ensemble des procédures et politiques de l'établissement, disponibles sur le logiciel de gestion documentaire, portant sur la mise en œuvre d'un traitement de données à caractère personnel. Il s'agit en particulier de la politique interne de protection des données à caractère personnel de l'établissement, de la procédure de gestion des violations de données, de la politique de gestion des droits des personnes, le dossier générique de spécifications fonctionnelles des durées de conservation et de la procédure de protection des données dès la conception et par défaut.

Il est rappelé que l'absence de déclaration de traitements/fichiers comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement.

Les utilisateurs s'engagent à n'utiliser que les moyens et outils informatiques mis à leur disposition par l'établissement et couverts par la présente charte.

Dans ce cadre, les utilisateurs doivent notamment :

- **Déclarer les nouveaux et toutes modifications de traitements de données à caractère personnel** auprès du référent à la protection des données de l'établissement ou à défaut au délégué à la protection des données (DPD ou DPO) du GHT ;
- **S'assurer auprès** du référent à la protection des données de l'établissement ou à défaut auprès du délégué à la protection des données (DPD ou DPO) du GHT **que l'encadrement contractuel des prestations des tiers fournisseurs** est conforme au RGPD lorsqu'il est chargé du recours à un prestataire de service ;
- **Se conformer aux règles de sécurité et de confidentialité des données** définies au sein de l'établissement, dans le respect de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), et aux obligations liées à la conservation des données ;
- **Signaler auprès du DPO les incidents de sécurité** impliquant des données personnelles.

Les utilisateurs, lors de l'utilisation des moyens et outils informatiques mis à disposition par l'établissement, peuvent, dans le cadre de l'exercice de leurs fonctions, traiter des données concernant la santé des patients.

Ces données sont des données dites particulières, leurs traitements répondent alors à des conditions de licéité plus strictes et sont soumis à des mesures de sécurité adaptées aux risques encourus par les personnes concernées. Ces données doivent faire l'objet d'une vigilance accrue de la part des utilisateurs.

Les utilisateurs professionnels de santé sont en outre soumis au secret professionnel.

Quoiqu'il en soit, chaque utilisateur s'engage à n'accéder aux données que lorsque c'est strictement nécessaire à l'exercice de ses fonctions et à ne traiter les données concernant la santé des patients via les moyens et outils informatiques mis à sa disposition par l'établissement que dans le respect de règles de confidentialité et des mesures de sécurité prévues notamment par :

- Les dispositions applicables de la politique générale de sécurité des systèmes d'information de santé
- La présente charte ;
- La politique de sécurité des systèmes d'information (PSSI) de l'établissement ;
- Les politiques et procédures sur la protection des données à caractère personnel susvisées.

6.2. Droits des utilisateurs

L'établissement met en œuvre des traitements de données à caractère personnel en relation avec l'usage des moyens informatiques et outils numériques couverts par la présente charte et pour assurer leur sécurité. L'établissement s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

Un DPO/DPD a été désigné au niveau du GHT. Il pilote la gouvernance des données à caractère personnel des établissements membres du GHT.

Les catégories suivantes de données sont traitées :

- Informations professionnelles ;
- Informations relatives à l'identité ;
- Journaux de connexion et autres traces informatiques ;
- Informations sur l'utilisation des moyens informatiques et outils numériques.

Ces catégories de données proviennent essentiellement des moyens informatiques et outils numériques ainsi que des annuaires informatiques et de la Direction Ressources Humaines.

Ces données sont conservées pour les durées suivantes :

- Les informations professionnelles ainsi que les informations relatives à l'identité sont conservées le temps de présence du personnel dans l'établissement augmentée des délais de prescription et de conservation obligatoire ;
- Les informations sur l'utilisation des moyens informatiques et outils numériques ainsi que les logs de connexion et autres traces sont conservées selon les systèmes pendant une durée allant de 6 mois à un an ;

- Les images des systèmes de vidéosurveillance/vidéoprotection sont conservées pendant une durée d'un mois sauf incident.

Ces données sont destinées aux personnes habilitées au sein de l'établissement et aux autorités habilitées.

Les traitements concernés par la charte ont pour finalité :

- Le suivi et la maintenance des moyens informatiques et outils numériques, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- La gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;
- La mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des moyens informatiques et outils numériques, notamment la conservation des journaux de connexion, des traces informatiques et des données de toute nature notamment à des fins d'historisation et de preuve de l'utilisation des moyens informatiques et outils numériques ;
- La gestion de la messagerie électronique et messagerie sécurisée de santé (MSSanté);
- Le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
- Le contrôle du respect de la charte et les audits ;
- Les statistiques, investigations et enquêtes.

Ces finalités permettent à l'établissement de poursuivre des intérêts légitimes liés à la bonne utilisation et à la sécurité de ses moyens informatiques et outils numériques dans le respect des droits des utilisateurs.

A toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion, d'organisation et de sécurité des moyens informatiques et outils numériques.

Conformément à la loi Informatique et libertés, les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'interrogation, d'accès, de limitation, d'effacement, de rectification et d'opposition au traitement des données les concernant et qui s'exerce auprès du délégué à la protection des données ou directement auprès du directeur de l'établissement:

Par courrier électronique : dpo@ch-stquentin.fr ou par courrier postal à l'attention du délégué à la protection des données (DGRQC) à l'adresse suivante : 1, avenue Michel de l'Hospital BP 608 Saint-Quentin 02321 Saint-Quentin, accompagné d'une copie d'un titre d'identité

Par courrier électronique direction@ch-chauny.fr ou par courrier postal à l'attention du Directeur délégué de l'établissement, à l'adresse suivante : 94 rue des anciens combattants 02300 CHAUNY, accompagné d'une copie d'un titre d'identité.

Chaque utilisateur peut également donner des directives relatives à la conservation, à l'effacement et à la communication de ses données après son décès. Une personne peut être désignée pour exécuter ces directives et elle aura alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement en cas de décès.

7. SURVEILLANCE DU SYSTEME D'INFORMATION

7.1. Contrôle

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment du RGPD et de la loi Informatique et Libertés.

7.2. Traçabilité

La direction des systèmes d'information assure la traçabilité de l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition, pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération;
- L'heure de la connexion;
- Le système auquel il est accédé;
- Le type d'opération réalisée;
- Les informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ou des applications de l'hôpital;
- La durée de la connexion (notamment pour l'accès Internet).

Le personnel de la Direction du système d'information respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

7.3. Alertes

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 ou tout manquement substantiel à cette charte, doit être signalé au Responsable de la Sécurité du Système d'Information.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. 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, soit respectée.

8. RESPONSABILITES ET SANCTIONS

Les règles définies dans la présente charte ont été fixées par la Direction de l'établissement de santé dans le respect des dispositions législatives et réglementaires applicables (CNIL, ASIP Santé...).

Toute utilisation pour motifs personnels et en dehors de tout usage professionnel, met à la charge de l'utilisateur l'entière responsabilité de cette utilisation et des conséquences qui s'en suivent.

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services Internet décrites dans la charte. En cas de manquement aux règles de la présente charte, la personne responsable de ce manquement est passible de sanctions pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, de l'accès aux moyens informatiques;
- Pour les contractuels, un licenciement et, éventuellement, des actions civiles ou pénales, selon la gravité du manquement.
- Pour les Titulaires de la fonction publique, une radiation et, éventuellement, des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction du Centre Hospitalier de CHAUNY est tenue de signaler toute infraction pénale commise par son personnel au procureur de la République.

Contact HOTLINE : 7371