Conformément à l'article L.6143-7 du Code de la santé publique, le Directeur Général des HCL a arrêté la présente Charte d'utilisation des Systèmes d'Information Numériques après :

- Soumission pour avis du comité de sécurité du numérique en date du 23 janvier 2019
- Concertation du Directoire du 1er avril 2019
- Information de la commission centrale de soins infirmiers, de rééducation et médicotechniques en date du 11 avril
- Information de la commission médicale d'établissement, lors de la séance du 1er avril 2019
- Information du Comité Technique Central d'Établissement du 2 avril 2019

Direction du Système d'Information et de l'Informatique

TABLE DES MATIÈRES

PRÉAMBULE : GÉNÉRALITÉS ET OBJET DE LA CHARTE

La prise en charge des patients et l'activité des Hospices Civils de Lyon dépendent de la continuité du fonctionnement de son Système d'Information (SI). Les HCL sont soumis aux obligations législatives et réglementaires propres aux informations numérisées et en particulier pour les données à caractère personnel relatives à la santé.

La sécurité, la protection des données et le bon fonctionnement du Système d'Information sont l'affaire de tous et découlent d'une action à la fois collective et individuelle. Chacun doit être conscient de ses droits mais aussi de ses devoirs tant vis-à-vis des patients pris en charge que des HCL et de ses employés.

La Charte de bon usage du Système d'Information des HCL, s'inscrit dans le cadre de la Politique Générale de Sécurité du Système d'Information (PGSSI) des HCL, validée par la Direction Générale. Elle est de ce fait, un document de référence pour l'ensemble des HCL. Tout utilisateur du Système d'Information et de Communication des HCL est invité à en prendre connaissance et à l'appliquer.

ARTICLE 1 : CHAMP D'APPLICATION DE LA CHARTE

1.1 Les utilisateurs concernés

Les règles et obligations figurant dans la présente Charte s'appliquent à tout utilisateur du Système d'Information (SI)et de Communication des HCL, quel que soit son statut (par exemple l'agent des HCL, le personnel en formation, l'étudiant, le stagiaire, le prestataire, le partenaire, l'auditeur, le visiteur occasionnel), son niveau hiérarchique ou son lieu d'accès.

Chaque utilisateur, au moment de la première utilisation de son compte informatique, devra valider avoir pris connaissance de la présente charte et de l'ensemble des termes.

1.2 Système d'Information et de Communication

Le Système d'Information et de Communication des HCL est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques (USB et autres), équipements biomédicaux ou de gestion technique centralisée connectés au réseau, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs et imprimantes multifonctions, téléphones, logiciels et progiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnement à des services interactifs ainsi que toutes les procédures, consignes d'utilisations et modes opératoires.

Les règles édictées dans ce document, s'appliquent également à l'ensemble des équipements informatiques non fournis par les HCL et interagissant avec les ressources interne du SI des HCL. Il s'agit, à titre d'illustration des équipements personnels, ou fournis par des partenaires, et autorisés à être connectés au SI des HCL. Leur utilisation doit être raisonnable et ne pas perturber le bon fonctionnement du système.

1.3 Cadre législatif et règlementaire

L'utilisation du système d'information dans les établissements de santé entre dans le champ d'application de textes législatifs et réglementaires nombreux, qui régissent notamment les principes suivants :

- les droits et libertés reconnus aux utilisateurs du SI des HCL, notamment la liberté d'expression, les libertés syndicales, et la liberté académique reconnue aux universitaires ;
- le traitement numérique des données, et plus précisément le traitement de données à caractère personnel relatives à la santé et le respect de la vie privée ;
- le droit d'accès des patients et des professionnels de santé aux données de santé ;
- l'hébergement de données de santé ;
- le secret professionnel et le secret couvrant les données à caractère personnel relatives à la santé ;
- la signature électronique des documents ;
- le secret des correspondances ;
- la lutte contre la cybercriminalité ;
- la protection des logiciels, des bases de données et le droit d'auteur.

La présente Charte est en conformité avec la réglementation sur la sécurité de l'information en vigueur.

ARTICLE 2 : RÈGLES GÉNÉRALES D'UTILISATION DES RESSOURCES

Il est de la responsabilité de chaque utilisateur d'adopter un comportement professionnel lors de l'utilisation du Système d'Information, en se conformant aux règles suivantes.

2.1 Respect des lois, des règlementations et de la déontologie

Les utilisateurs sont responsables des ressources qui leur sont confiées dans le cadre de l'exercice de leurs fonctions. Ils doivent concourir à la protection des dites ressources.

Leur usage du système d'information des HCL doit être conforme vis-à-vis des lois et des règlementations en vigueur.

Il est notamment interdit :

- de diffuser des informations relatives aux HCL, à ses agents, à ses patients (violation du secret médical) ou à ses partenaires, par le biais des outils numériques fournis par les HCL, sauf si la conduite des activités le nécessite ;
- d'accéder aux données à caractère personnel relatives à la santé sans justification professionnelle ;
- de diffuser des images et films pris au sein des HCL des agents et des patients sans leur autorisation explicite et celle des HCL ;
- de diffuser ou de télécharger des informations protégées par le droit d'auteur, qu'il s'agisse notamment d'écrits, d'images, de logiciels ou de bases de données ;
- de porter atteinte à la vie privée des patients et des personnels;
- de publier tout propos contraire à la loi et aux règles de déontologie ;
- de participer à tout acte relevant de la fraude informatique (falsification, modification, suppression et introduction d'informations avec l'intention de nuire) ;
- de participer à tout acte portant atteinte au non-respect des réglementations édictées en matière de traitement des informations à caractère personnel, dont la Loi Informatique et liberté et le RGPD (Règlement Général sur la Protection des données) ;
- d'interrompre le fonctionnement du réseau ou d'un système connecté au réseau ;
- de connecter un équipement sur le réseau sans autorisation ;

- d'installer des logiciels, copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein des HCL ;
- de neutraliser ou contourner les dispositifs de sécurité installés sur les postes de travail qui lui sont confiés (en particulier l'anti-virus et les dispositifs de filtrage) ;
- d'utiliser la messagerie des HCL pour diffuser en masse des messages sans autorisation préalable de la Direction Générale ;
- de diffuser des messages à vocation syndicale à partir d'une adresse de messagerie non dédiée à cet effet ;
- de confier son identifiant / mot de passe ;
- de demander son identifiant / mot de passe à un collègue ;
- d'usurper l'identité d'autrui ;
- d'utiliser le réseau HCL et les moyens mis à sa disposition par les HCL pour créer, envoyer, recevoir, transmettre, télécharger, enregistrer, ouvrir ou afficher tout contenu illicite, et en particulier qui pourrait être constitutif, sans que ce qui suit soit limitatif :
    - d'apologie de crimes contre l'humanité ou de crimes de guerre;
    - d'incitation à la violence ou la haine raciale ;
    - de discrimination ;
    - de pédophilie ;
    - de diffamation, d'injure, d'atteinte à la vie privée ;
    - de harcèlement sexuel ou de harcèlement moral ;
    - d'atteintes aux mineurs ;
    - de pornographie.

2.2 Protection des données à caractère personnel

Les traitements de données à caractères personnel doivent faire l'objet d'une formalité interne. Les utilisateurs souhaitant réaliser des traitements relevant de la Loi Informatique et Liberté (LIL) et du Règlement européen à la protection des données (RGPD) doivent prendre contact avec le référent à la protection des données de leur direction, avant d'y procéder.

Aucun utilisateur ne peut collecter et/ou traiter des données à caractère personnel (ou nominatives), sans autorisation des HCL et sans s'assurer préalablement du strict respect des lois et règlements en vigueur et notamment de la loi informatique et liberté (LIL), du règlement européen à la protection des données (RGPD), mais également de la politique général de protection des données à caractère personnel (PGPD) des HCL

Constitue un traitement de données à caractère personnel, toute opération ou tout ensemble d'opérations portant sur des données identifiantes (directement ou indirectement), quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

2.3 Usage à des fins professionnelles

Les ressources informatiques (applications, messagerie, accès Internet…) et les moyens mis à disposition par les HCL (postes de travail informatiques fixes ou portables, téléphones, fax…) sont à usage strictement professionnel.

Par principe, tous les fichiers créés par l'utilisateur ainsi que tous les messages envoyés, reçus et stockés seront considérés comme professionnels.

Un usage à des fins personnelles est toutefois toléré à condition qu'il soit licite, raisonnable et ponctuel, et dans les conditions prévues notamment aux articles 4, 5 et 6 de la présente charte. Pour ne pas être considérés comme professionnels, les fichiers créés à ce titre ainsi que les messages envoyés ou reçus doivent être identifiés et stockés, expressément, sous un répertoire nommé « mes données personnelles ». Ce répertoire doit être situé sur le disque dur de l'ordinateur, afin de ne pas encombrer les serveurs des HCL. Les ressources informatiques des HCL n'ont pas vocation à assurer ni sauvegarde, ni restauration de ces répertoires « mes données personnelles ».

2.4 Fin de mission

Lors de son départ, l'utilisateur doit restituer au service les matériels et logiciels mis à sa disposition. Il doit au préalable y effacer ses fichiers et données personnelles. Il ne doit pas copier de document professionnel.

ARTICLE 3 : SÉCURITÉ DES ÉQUIPEMENTS MIS À DISPOSITION

3.1 Sécurité du poste de travail

La configuration initiale du poste de travail doit être respectée

La configuration du matériel des HCL a été étudiée afin de garantir le bon fonctionnement et la sécurité du Système d'Information. De ce fait, elle ne doit jamais être modifiée et doit être conservée telle qu'elle a été définie par la Direction des Systèmes d'Information et de l'Informatique (DSII) des HCL.

De même, afin de limiter tout risque de propagation de virus à travers le réseau informatique, l'utilisateur ne doit jamais désactiver les outils de sécurité, tel que l'antivirus et les dispositifs de filtrage, ou modifier leur paramétrage.

Afin de limiter le risque d'intrusion, les postes de travail informatiques, quand ils sont connectés au réseau des HCL, ne doivent pas être connectés simultanément à un autre réseau.

Dans le cadre du respect de la propriété intellectuelle et des règles d'usage des licences, la copie des logiciels mis à disposition par les HCL est interdite, hormis les copies de sauvegarde. Chaque utilisateur doit se conformer aux restrictions d'utilisation des logiciels fournis par les HCL.

Les ordinateurs doivent être protégés physiquement.

Chacun doit veiller à utiliser les moyens de protection fournis par les HCL tels que les câbles antivol, les armoires à clé, afin d'éviter les vols ou la dégradation des équipements.

Par ailleurs, les postes de travail fixes ne doivent pas être déménagés d'un local à l'autre sans autorisation des équipes DSII.

Les sessions des ordinateurs doivent être verrouillées en cas d'absence.

Afin d'empêcher tout risque d'intrusion dans le Système d'Information pouvant mener à des incidents de sécurité, telle que la fuite d'informations, chaque utilisateur doit s'assurer d'avoir verrouillé sa session, s'il est amené à laisser sa station de travail sans surveillance ou à quitter son bureau.

Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les répertoires réseaux mis à disposition.

Les HCL mettent à la disposition des utilisateurs des espaces de stockage afin qu'ils puissent sauvegarder et partager des informations. Les utilisateurs doivent être vigilants quant à l'usage qu'ils font de ces répertoires partagés, et sont responsables des informations stockées.

Les utilisateurs ne doivent jamais effacer, supprimer ou modifier des informations pouvant être nécessaires au bon déroulement des activités et des services rendus par les HCL.

Ils doivent procéder à des sauvegardes régulières des informations professionnelles, stockées localement sur leur ordinateur, sur les répertoires réseaux et ce, afin d'éviter tout risque de perte d'informations (en cas de défaillance de l'ordinateur par exemple).

Pour les informations sensibles, l'utilisateur veillera à les stocker dans des répertoires avec des droits réservés aux seules personnes légitimes à y accéder (tels que les répertoires partagés entre les membres d'un service par exemple). En cas de doute, il pourra se renseigner auprès du support DSII.

Les informations sauvegardées sur les répertoires, y compris les répertoires personnels, doivent être conformes aux lois et règlements en vigueur (interdiction, entre autres, de stocker des informations à caractère pédopornographique, raciste, diffamatoires ou des copies illégales de logiciels, de films, de musique ou d'images).

3.2 Sécurité des ordinateurs portables

Une vigilance particulière est demandée aux utilisateurs d'ordinateurs portables, dans la mesure où les mises à jour des outils de sécurité ne s'effectuent qu'en connexion au seul réseau HCL et que l'usage de ces ordinateurs est limité au seul usage professionnel. Il est donc expressément demandé à ces utilisateurs de se connecter au minimum une heure par semaine au réseau des HCL, hors congés, afin de permettre les mises à jour régulières.

3.3 Sécurité des autres moyens du SI

Les supports amovibles doivent être évités

Les supports amovibles personnels, tels que les clés USB, les appareils photos, les lecteurs MP3, les téléphones portables, les smartphones ou les disques externes sont susceptibles d'héberger des programmes informatiques pouvant porter atteinte à l'intégrité du Système d'Information (par exemple des virus, des vers, ou des chevaux de Troie) et par conséquent, menacer sa sécurité, et ce, parfois à l'insu de l'utilisateur. Leur installation est à proscrire.

Ainsi, il est demandé à chaque personne de privilégier l'usage de matériels fournis par les HCL, et de ne les connecter qu'à des postes de travail sécurisés (pourvus d'un antivirus). De plus, chaque utilisateur doit veiller à ne pas connecter des supports amovibles dont l'origine lui paraît suspecte.

En cas de doute sur la fiabilité d'un support amovible, l'utilisateur doit se rapprocher du support de la DSII, qui pourra lui indiquer comment procéder à son analyse.

Les documents sensibles doivent être rapidement récupérés des imprimantes

Les imprimantes sont souvent partagées, de ce fait, tout document confidentiel (contenant par exemple, des données à caractère personnel relatives aux patients ou aux agents, ou des informations financières) doit être récupéré immédiatement après son impression et classé dans un endroit approprié.

Les moyens de télécommunication sont à usage professionnel prioritairement.

Les HCL mettent à disposition des utilisateurs des moyens de télécommunication tels que les télécopieurs (fax) ou les téléphones. Ces moyens de télécommunication sont réservés à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel est toléré à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur ou à la bonne conduite des activités des HCL.

En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services de télécommunication mis à la disposition des utilisateurs.

Les téléphones portables et smartphones doivent être protégés par un code.

Les téléphones portables et les smartphones, permettant de stocker et/ou d'accéder aux informations parfois confidentielles des HCL, doivent être protégés. Lorsque cela est techniquement possible, l'utilisateur doit définir un code PIN et un code de déverrouillage en prenant soin de choisir un code suffisamment complexe (en évitant les codes de type « 0000 » ou « 1234 »).

ARTICLE 4 : DROITS D'ACCÈS

L'accès à tout ou partie du Système d'Information (comme la messagerie, Internet, les sessions sur les postes de travail, le réseau…) repose sur un compte d'accès strictement personnel composé d'un identifiant (par exemple le code HCL ou le code prestataire) et d'un authentifiant, tel que le mot de passe. Ces moyens d'authentification sont strictement personnels et confidentiels et ne doivent en aucun cas être communiqués à une tierce personne. En cas de corruption de l'authentifiant, l'utilisateur a le devoir de procéder à son changement sans délai. En cas d'intervention du support de la DSII nécessitant la communication de l'authentifiant, celui-ci devra être changé.

Les utilisateurs sont seuls responsables des actions réalisées depuis leurs comptes d'accès.

L'encadrement s'assure que les droits d'accès accordés aux utilisateurs sous sa responsabilité correspondent à leur mission. Il s'assure également du retrait de ces droits en fin de mission.

Les droits d'accès associés à ces comptes feront l'objet d'une revue régulière afin de corriger toutes les anomalies (droits non adéquats au regard des activités des utilisateurs par exemple). De plus, en cas de mobilité d'un utilisateur, ses droits d'accès seront modifiés ou désactivés.

En cas de départ définitif :

- le compte de l'utilisateur sera désactivé ;
- les traces relatives aux accès de l'utilisateur seront conservées 1 an.

Il appartient à l'utilisateur de récupérer ou d'effacer les données identifiées comme « mes données personnelles », dans le respect de la Charte, avant son départ. Il lui appartient également d'anticiper la transition au niveau de la messagerie par exemple vis-à-vis de ces correspondants. Les données professionnelles seront conservées dans le respect du secret professionnel.

L'utilisation de comptes non personnels (par exemple des comptes génériques ou partagés) doit rester exceptionnelle. Dans le cas où l'utilisateur y a accès, il est responsable de l'usage qu'il fait de ces derniers, et doit respecter les règles de sécurité du présent document, au même titre que pour son compte personnel.

Les mots de passe doivent respecter les règles de bonne pratique de la CNIL

L'utilisateur doit définir un mot de passe complexe, difficile à deviner par un tiers et doit veiller à le modifier régulièrement afin d'éviter toute usurpation de son identité, en application des mécanismes mis en place aux HCL sur la définition des mots de passe Windows qui imposent le respect de ces règles.

L'accès aux informations se fait au regard des nécessités professionnelles.

Les personnels des HCL sont soumis au secret professionnel dont le secret médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données à caractère personnel relatives à la santé. Les personnels doivent faire preuve d'une discrétion absolue dans l'exercice de leur mission de service public. 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.

Afin de garantir la qualité des services rendus par les HCL et l'intégrité de son SI, chaque utilisateur ne doit accéder qu'aux seules informations nécessaires à la réalisation de son activité professionnelle et dans le respect des principes de confidentialité. Les informations consultées dans le cadre de tâches professionnelles ne doivent être utilisés qu'à ce titre.

Lorsqu'une personne estime qu'elle ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles, elle doit s'adresser à son responsable hiérarchique afin de les faire modifier.

ARTICLE 5 : UTILISATION D'INTERNET

Internet est à usage professionnel prioritairement.

Les HCL mettent à disposition des utilisateurs l'accès à Internet. Cet accès est réservé à des fins strictement professionnelles. Cependant, dans le cadre de nécessités de vie courante, un usage personnel est toléré, à

condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur ou à la bonne conduite des activités des HCL.

En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services Internet, mis à disposition des utilisateurs.

La consultation de sites Internet ou le téléchargement de fichiers illégaux sont interdits, sauf si cela est expressément requis dans le cadre des activités professionnelles des utilisateurs.

L'accès à des sites, initialement bloqués par les HCL, est interdit sauf cas dérogatoire.

Les HCL se réservent le droit de bloquer l'accès à tout site Internet non indispensable aux activités professionnelles et interférant avec le déroulement normal des activités des HCL (par exemple : problèmes de débit Internet et de saturation réseau) ou présentant un risque d'incident de sécurité. Par ailleurs, les sites contenant des éléments pornographiques, indécents, incitant à la haine, insultants ou relatifs au piratage informatique sont bloqués par des règles de filtrage.

Enfin, l'utilisateur ne pourra, en aucun cas, faire valoir l'absence de blocage technique des accès vers de tels sites, pour justifier une autorisation implicite d'un usage légalement prohibé.

Les sites de stockage en ligne sont également bloqués. Seule une nécessité professionnelle dûment justifiée et valable permettra un déblocage individuel.

La publication depuis le Système d'Information des HCL doit se faire dans le respect de la loi et des codes de déontologie professionnelle.

La publication de contenu professionnel et/ou personnel, depuis le Système d'Information des HCL, sur les blogs, forums, réseaux sociaux, ou sites non professionnels, c'est-à-dire non partenaires ou non administrés par les HCL, engage la responsabilité de l'utilisateur et l'image des HCL. Cette publication doit donc se faire dans le respect des principes énumérés à l'article 2 et des codes de déontologie professionnelle pour les professions qui en disposent.

Les outils de communication audiovisuelle par Internet utilisés pour l'échange d'informations confidentielles sont à éviter

Les outils de communication audiovisuelle par Internet (téléphone, visio-conférence) peuvent comporter des failles pouvant constituer une menace pour la sécurité du Système d'Information et des informations échangées (possibilité d'interception des échanges par une tierce personne ou contournement des moyens de protection tels que les pare-feu par exemple). Ces outils de communication sont à proscrire dès lors que des informations confidentielles sont concernées.

ARTICLE 6 : UTILISATION DE LA MESSAGERIE ÉLECTRONIQUE

La messagerie électronique est à usage professionnel avant tout.

Les HCL mettent à disposition des utilisateurs une messagerie électronique. Cet accès est réservé à des fins strictement professionnelles. Cependant, dans le cadre de nécessités de vie courante, un usage personnel est toléré, à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur ou à la bonne conduite des activités des HCL.

En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité du service de messagerie électronique, mis à disposition des utilisateurs.

L'utilisation d'une liste de diffusion est assujettie à l'accord du responsable gestionnaire de la liste et doit respecter le cadre strictement professionnel. Tout autre usage de la liste de diffusion, y compris syndical, nécessite un accord explicite de chacun des agents constituant la liste.

Les messages reçus depuis l'extérieur des HCL sont contrôlés par un anti-virus avant d'être remis. L'accès aux pièces jointes est donc susceptible d'être empêché a priori.

L'utilisation de smartphones pour relever la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est à proscrire.

Les agents peuvent consulter leur messagerie à distance, à l'aide d'un navigateur. Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

ARTICLE 7 : REMONTÉE DES INCIDENTS PAR LES UTILISATEURS DU SI

Toute anomalie suspectée ou avérée concernant le SI (par exemple les vols ou pertes de matériels, les vols ou pertes d'informations, ou les dysfonctionnements du poste de travail, une alerte de détection virale sur un poste de travail, un incident sur une application), ou toute violation des règles décrites dans le présent document, doivent être signalées au support de la DSII qui traitera.

En outre, en cas d'accès accidentel à un site internet illicite ou potentiellement dangereux (site corrompu ou susceptible d'être vecteur d'une infection virale), l'utilisateur doit se déconnecter immédiatement du site et informer le support de la DSII.

Une fois déclarés, les incidents sont traités par les services compétents en fonction de leur nature.

ARTICLE 8 : MESURES D'ACCÈS ET DE CONTRÔLE

Les HCL se réservent la possibilité d'effectuer, à tout moment, des vérifications et des contrôles sur la validité des accès et le respect des stipulations de la Charte, notamment par le biais de logiciels d'analyse des journaux de sécurité sur les systèmes et d'un logiciel de filtrage pour les accès WEB. Les échanges vis-à-vis de l'extérieur (Internet) donnent lieu à des traces nominatives systématiques qui sont conservées pendant 1 an.

Par ailleurs, les administrateurs de la DSII ayant accès aux données techniques s'engagent à respecter les règles de confidentialité applicables aux contenus des journaux. Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaitre dans le cadre de leurs fonctions. Ils ne pourront répondre à aucune autre sollicitation que celles provenant du Directeur de la DSII dans le cadre de procédures définies, dont notamment :

- de requêtes émanant de la Direction du Personnel et des Affaires Sociales, de la Direction des Affaires Médicales pour ce qui concerne les personnels HCL ;
- de requêtes émanant de la Direction Organisation, Qualité, Risques et Usagers pour ce qui concerne les patients (y compris les personnels pris en charge par les HCL) ;
- de requêtes de justice ;
- de missions d'audit (Cour des comptes, HAS, CNIL, audits internes, etc.).

8.1 Accès aux données à caractère professionnel de l'utilisateur

En cas d'absence ou de départ de l'utilisateur, quel qu'en soit le motif, l'utilisateur doit s'organiser pour permettre aux HCL d'accéder à tous les fichiers non classés sous les répertoires « mes données personnelles », ceux-ci étant présumés à caractère professionnel, qu'il a enregistré sur son poste ou sur le serveur des HCL.

8.2 Accès aux données à caractère personnel (ou privées) de l'utilisateur

Sauf en cas d'événement, de risque particulier susceptible de porter préjudice aux HCL, à l'un de ses agents ou à un tiers, ou dans l'un du non-respect d'une obligation de l'article 3, les HCL s'engagent à n'accéder aux données et communications électroniques ayant été identifiées et classées comme personnelles par un utilisateur, émises, reçues, transmises, téléchargées ou enregistrées par un utilisateur, sur un poste ou sur le serveur des HCL, qu'en présence de l'utilisateur concerné ou qu'après l'avoir dûment informé. La mise en œuvre de cette disposition relève de la seule responsabilité du directeur de l'établissement.

Dans le cadre d'une enquête, ou sur commission rogatoire d'un juge, les données et communications électroniques identifiées et classée comme personnelles par un utilisateur peuvent être saisies par un officier de police judiciaire. La mise en œuvre de cette disposition relève de la seule autorité judiciaire.

8.3 Contrôle des accès aux dossiers des patients

La Commission du Système d'Information de la CME (CSI-CME) en relation avec la Direction du Système d'Information et de l'Informatique a précisé le cadre des accès aux dossiers des patients dans le dossier patient informatisé. Ces habilitations ont été progressivement déployées dans les services de soins et sur les services transversaux.

La Direction Générale, la Commission Médicale d'Établissement et la Direction Centrale des Soins ont décidé de mettre en place une sous-commission afin de procéder à des vérifications régulières du bon usage des habilitations.

Le fonctionnement de cette sous-commission est cadré par la « Charte de fonctionnement de la sous-commission de la Commission du Système d'Information de la CME en charge du contrôle des accès aux dossiers des patients », disponible auprès de la Commission Système d'Information de la CME.

ARTICLE 9 : LES SANCTIONS

Le manquement aux règles et mesures de sécurité de la présente Charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des limitations ou suspensions d'utiliser tout ou partie du Système d'Information et de Communication, des sanctions disciplinaires, après éventuellement une mise en demeure et/ ou une plainte pénale, selon la gravité des faits.

ARTICLE 10 : APPLICATION DE LA CHARTE

La présente charte entre en vigueur à compter de la date de publication mentionnée sur la page de garde.

Elle est publiée sur le site Intranet des HCL. Elle est rappelée à la première connexion sur un ordinateur des HCL.

Elle sera révisée en cas de modification du cadre législatif et/ou réglementaire.

Toute modification du présent document sera notifiée aux utilisateurs par le biais du mailing et de la publication intranet et par une information (modification non substantielle) des instances représentatives centrales.

Pour toutes questions relatives au document, l'officier de sécurité du système d'information et la Direction du Système d'Information et de l'Informatique peuvent être consultés.