GHT DE LA RÉUNION
Groupement Hospitalier de Territoire

CHU
CENTRE HOSPITALIER UNIVERSITAIRE
LA RÉUNION

Charte utilisateur pour l'usage des systèmes d'information et de communication

Tableau des évolutions		
Indice	Date	Motif
1.0	Février 2021	Création

Tableau d'approbation			
Groupe d'élaboration	Avis DSIO	Avis DRH	Approbation
Stéphane Duchesne	Paul Milon	S. BATY	Lionel CALENGE
RSSI GHT	DSI GHT	DRH CHU	Directeur Général du CHU
16/03/2021	16/03/2021	Date 30/03/21	Date 30/03/2021
Signature	Signature	Signature	Signature
			Le Directeur Général, Lionel CALENGE

TABLE DES MATIERES

PREAMBULE

Le Centre Hospitalier Universitaire de La Réunion (ci-après « l'établissement ») met en œuvre des systèmes d'information et de communication nécessaires à son activité, comprenant notamment un réseau informatique et téléphonique, des applications métiers ainsi que des outils technologiques.

Les utilisateurs, qu'ils soient externes ou internes à l'établissement, ont besoin pour l'exercice de leurs fonctions au sein de l'établissement, d'accéder aux systèmes d'information et de communication de l'établissement grâce :

- aux moyens et outils informatiques et de communication qui peuvent être mis à leur disposition par l'établissement ;
- à leurs propres moyens et outils informatiques et de communication.

La présente charte utilisateur pour l'usage des systèmes d'information et de communication a pour objectif de décrire les règles d'utilisation ou d'autorisation d'accès aux systèmes d'information et de communication de l'établissement mis à disposition des utilisateurs par l'établissement. Elle précise les droits et les devoirs de chacun lors de l'usage des systèmes d'Information et de communication et informe les utilisateurs sur les mesures de contrôle en place.

Les règles ainsi définies sont destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance d'usage des systèmes d'information et de communication, en conformité avec les dispositions légales et réglementaires applicables notamment aux établissements de santé, la jurisprudence des Cours et Tribunaux, ainsi que des recommandations de la Commission nationale de l'informatique et des libertés (CNIL), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Direction générale de l'offre de soins (DGOS) du Ministère des solidarités et de la santé, en fonction des besoins métiers, et dans le respect des libertés de chacun.

La présente charte est rédigée dans le souci de concilier les intérêts de chaque utilisateur extérieurs et ceux du l'établissement. Dans un but de transparence à l'égard des utilisateurs, elle manifeste ainsi la volonté de l'établissement d'assurer un usage loyal, respectueux, sécurisé et responsable de ses systèmes d'information et de communication, et de protéger son patrimoine et son image de marque.

La présente charte n'a pas pour objet ou pour objectif de couvrir de façon exhaustive tous les cas de figure susceptibles de se présenter dans le cadre de l'utilisation des systèmes d'information et de communication mis à la disposition des utilisateurs. C'est dans l'esprit des règles ainsi édictées que chaque utilisateur devra se conformer dans des situations non-envisagées.

Il appartient aux utilisateurs externes et internes de veiller au respect des règles énumérées au sein de la présente charte afin de garantir un niveau optimum en termes de sécurité, de traçabilité et de performance dans l'usage des systèmes d'information et de communication, tout en assurant la confidentialité des données et en particulier des données de santé.

La charte s'inscrit dans le prolongement des différentes politiques de sécurité mises en œuvre par l'établissement. Elle pourra évoluer en fonction du contexte légal ou réglementaire et de la politique de sécurité des systèmes d'information du GHT, notamment applicable au sein de l'établissement.

Ainsi, la charte utilisateur pour l'usage des systèmes d'information et de communication a notamment pour objet :

- d'informer les utilisateurs sur les règles d'utilisation des systèmes d'information et de communication mis à leur disposition par l'établissement en cohérence avec les enjeux métiers ;
- de rappeler les droits et obligations de chacun lors de l'emploi des systèmes d'information et de communication conformément aux lois et réglementations en vigueur ;
- de faire connaître les moyens de contrôle mis en place, lorsqu'ils s'avèrent indispensables.

C'est la raison d'être des dispositions suivantes qui s'imposent à tout utilisateur externe ou interne des systèmes d'information et de communication de l'établissement.

ARTICLE 1. DEFINITIONS

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

« Chaine Décisionnelle » : en cas de question ou de difficulté portant sur la présente charte ou en cas de demande d'autorisation en application de la présente charte, l'utilisateur devra contacter le Responsable de la Sécurité des Systèmes d'Information, Direction des Systèmes d'Information et de l'Organisation, et, en parallèle, le Responsable hiérarchique dont il dépend ;

« Données à caractère personnel » : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;

« Données de santé » : désigne les Données à caractère personnel relatives à la santé des personnes comprenant, notamment, les données produites à l'occasion des activités de prévention, de diagnostic ou de soin d'un Professionnel de santé et tout élément de nature à caractériser la santé d'une personne ;

«Equipement Mobile Personnel» : désigne tout équipement (ordinateurs, téléphones, smartphones, tablettes tactiles etc.) propriété de l'utilisateur, et connecté sur site ou à distance, aux systèmes d'information et de communication de l'établissement ;

«Equipement Mobiles Professionnel» : désigne tout équipement mobile (ordinateurs, téléphones, smartphones, tablettes tactiles etc.) mis à disposition des utilisateurs par l'établissement connecté sur site ou à distance, aux systèmes d'information et de communication de l'établissement ;

« Privé » : désigne l'identification par l'utilisateur de tout message électronique, tout fichier ou tout répertoire à des fins autres que relevant de ses activités Professionnelles et/ou syndicales ;

« Professionnel » : désigne tout ce qui concerne l'utilisation des systèmes d'information et de communication de l'établissement à des fins professionnelles, pédagogiques et de recherche ;

« Systèmes d'information et de communication» : désigne les systèmes d'information et de communication de l'établissement dans son ensemble, composé :

- d'éléments physiques tels que notamment des serveurs, , baie de stockage, firewalls, équipements réseaux, interconnexions réseaux (en ce compris les raccordements opérateurs), des ordinateurs (fixes ou portables), Equipement(s) mobile professionnels(s), Equipement(s) mobile personnel(s) des Utilisateurs, tout périphérique et tout autre matériel informatique, connectique ou bureautique en ce compris les plateformes, câbles du réseau, fax, photocopieurs, téléphones (fixes ou portables, Smartphones, etc.), scanners, imprimantes, etc. et ;

- d'éléments logiques tels que notamment les systèmes d'exploitation, logiciels, progiciels, applications, fichiers, données et bases de données, intranet, extranet, système de messagerie, etc.

« Personnel administratifs » : désigne tous les professionnels de l'établissement autres que les Professionnels de santé ;

« Professionnels de santé » : désigne les seuls professionnels médicaux et paramédicaux dont le droit d'exercice et les actes sont réglementés par une disposition législative ou par un texte pris en application de la loi ;

« Utilisateur » : désigne toute personne physique ayant accès aux systèmes d'information et de communication de l'établissement en quelque lieu que ce soit et quel que soit son statut,

« Back up » : centre informatique externe possédant une configuration informatique compatible avec celle de l'Etablissement et prêt à accueillir les applications de ce dernier en cas de défaillance de son centre de traitement habituel ;

« BYOD » : Utilisation, dans un cadre professionnel, d'un matériel personnel tel qu'un téléphone multifonction ou un ordinateur. De l'anglais : bring your own device (BYOD) ;

« Charte » : le présent document et ses annexes, constituant la charte utilisateur pour l'usage des systèmes d'information et de communication ;

« Code malveillant » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keylogger, etc.) ;

« Filtrage » : ensemble d'outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocolaire, etc.) ;

« Matériel nomade » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de l'Etablissement ;

« Moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et pouvant prendre diverses formes : login/mot de passe, biométrie, signature électronique, cartes avec ou sans contact, etc ;

« Scan » : contrôle à travers des outils informatiques de la présence de mots clés dans des contenus (dossiers, documents, courriers électronique, pièces jointes, fichiers, etc.) ;

« Trace informatique » : donnée informatique témoignant de l'existence d'une opération au sein d'une application ou du système d'information ;

ARTICLE 2. CHAMP D'APPLICATION

La présente charte est applicable à l'ensemble des utilisateurs qui utilisent les systèmes d'information et de communication mis à disposition par l'établissement, en quelque lieu que ce soit et quel que soit leur statut.

Les personnes concernées par la présente charte sont :

- les personnels de l'établissement, agents titulaires et contractuels concourant à l'exécution des missions du service public hospitalier, les étudiants rémunérés ou non par l'établissement, les stagiaires et apprentis, les enseignants, les chercheurs ;
- les prestataires ou sous-traitants de l'établissement ;
- les professionnels de santé non-salariés.

La présente charte est complétée par des documents spécifiques pour certaines catégories d'utilisateur tel que les administrateurs des systèmes d'information et de communication.

Les moyens concernés par la présente charte sont :

- l'ensemble des systèmes d'information et de communication qui sont la propriété de l'établissement et/ou utilisé par l'établissement et/ou qui sont mis à la disposition des utilisateurs à des fins professionnelles ;
- l'ensemble des systèmes d'information et de communication qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

La présente charte s'applique à tous les types d'usage qu'ils aient lieu dans les locaux de l'établissement, dans le cadre d'un usage dit « nomade », quel qu'en soit le lien, et dans le cadre d'un accès distant, quel que soit le lieu de cet accès.

La présente charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des systèmes d'information et de communication de l'établissement.

ARTICLE 3. CADRE REGLEMENTAIRE DE LA SECURITE DE L'INFORMATION

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

Le cadre réglementaire de la sécurité de l'information porte notamment 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 de santé.
- Le droit d'accès des patients et des professionnels de santé aux données de santé ;
- Le secret médical et professionnel ;
- Le secret des correspondances ;
- La protection des systèmes d'information ;
- La responsabilité en matière de transmission des informations ;
- La protection des logiciels et des bases de données et le droit d'auteur.

La sécurité de l'information est caractérisée comme étant la préservation de :

- La disponibilité de l'information : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin;
- L'intégrité de l'information : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie ;
- La confidentialité de l'information : l'information ne doit être accessible qu'aux personnes autorisées à y accéder ;
- L'auditabilité de l'information : la traçabilité des informations est assurée au travers d'un dispositif organisationnel et technique de piste d'audit. A ce titre, les systèmes d'information intègrent des outils permettant le traçage des accès et des opérations effectuées sur l'information à des fins de reconstitution et de preuve.

ARTICLE 3. USAGE PROFESSIONNEL ET NON PROFESSIONNEL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Les systèmes d'information et de communication mis à la disposition des utilisateurs de l'établissement sont réservés à l'exercice de leurs activités professionnelles, à savoir notamment : les activités de soins, de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

Les usages sont donc présumés avoir un caractère strictement professionnel, et ce, quelles que soient les conditions effectives d'utilisation par l'utilisateur.

Bien que les systèmes d'information et de communication soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles, pour répondre en cas d'urgence à des obligations socialement admises, est tolérée.

Cette tolérance pourra être suspendue ou limitée en cas d'abus par simple décision de la chaîne décisionnelle de l'établissement. Elle s'inscrit dans le strict respect des règles ci-après exposées :

- L'usage non professionnel doit être exceptionnel et demeurer raisonnable.
- L'usage non professionnel ne doit pas :
  - perturber ou compromettre le bon fonctionnement des systèmes d'information et de communication de l'établissement ;
  - perturber ou compromettre les activités de l'établissement ;
  - porter atteinte ou être susceptible d'engager la responsabilité de l'établissement ;
  - poursuivre un but lucratif ou même ludique ;
  - porter atteinte à l'image ou à la réputation de l'établissement.

L'usage des systèmes d'information et de communication de l'établissement à des fins non professionnelles se traduit dans les faits par :

- la possibilité de créer des répertoires et fichiers informatiques non professionnel sur des postes de travail administratifs ;
- la possibilité d'utiliser de manière résiduelle, à des fins non professionnelles, la messagerie électronique professionnelle ;
- la possibilité d'utiliser de manière résiduelle, à des fins non professionnelles, l'accès internet pour consulter des sites internet dument autorisés par l'établissement ;
- la possibilité d'utiliser de manière résiduelle, à des fins non professionnelles, les services de téléphonie.

L'utilisateur est entièrement responsable de l'usage des systèmes d'information et de communication de l'établissement à des fins non professionnelles et dégage en conséquence l'établissement de toute responsabilité.

Le caractère non professionnel de l'usage des systèmes d'information et de communication interdit, par principe, à l'établissement d'accéder aux contenus ou données créés, émis, reçus ou échangés dans ce cadre.

Cependant le caractère « non professionnel » des répertoires, des fichiers ou des courriers électroniques créés et/ou échangés, ne fait pas obstacle à ce que :

- l'établissement puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'établissement en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;
- ces éléments fassent l'objet de conservation technique dans le cadre des procédures de back up ou de plans de continuité ou reprise d'activité mises en œuvre au sein du l'établissement ;
- en cas de détection ou de suspicion de la présence d'un code malveillant à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;
- un administrateur ou toute personne « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information et de communication, ce notamment dans le cadre d'opération de maintenance ;
- l'établissement puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, CNIL, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.).

ARTICLE 4. ACCES AUX SYSTEMES D'INFORMATION ET DE COMMUNICATION

Article 4.1. Moyens d'authentification

Chaque utilisateur, pour l'exercice de ses missions au sein de l'établissement se voit remettre un ou plusieurs moyens d'authentification, selon ses besoins et missions, permettant l'accès aux systèmes d'information et de communication de l'établissement.

Ces moyens d'authentification sont généralement composés de paramètres de connexion (identifiant logique et mot de passe associé), de dispositifs physiques ou logiques d'authentification, ou tout autre type de moyens d'authentification connus ou à venir mis en œuvre par l'établissement conformément à la politique de sécurité des systèmes d'information, auxquels correspondent des droits d'accès dont l'étendue varie en fonction des besoins, des fonctions, des missions et de la catégorie d'utilisateur.

Les moyens d'authentification sont dans tous les cas personnels, confidentiels et incessibles, étant précisé que chaque utilisateur en est strictement responsable. Ils ne doivent pas être prêtés, communiqués ou partagés avec des tiers, pour quelque raison que ce soit, sauf hypothèses d'absence et de départ mentionnées à l'Article 5.

Il est dès lors interdit à l'utilisateur de :

- procéder à toute divulgation, même intra-service, de ses paramètres de connexion ;
- de prêter à autrui ses dispositifs physiques ou logiques d'authentification ;
- d'utiliser des moyens d'authentification autre que les siens, dans l'hypothèse où il en aurait eu connaissance ;
- de supprimer, masquer ou modifier son identité ou son identifiant ;
- d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.

Sauf à avoir engagé préalablement une demande de suspension ou de suppression de ses accès aux systèmes d'information et de communication, ou à être en mesure de démontrer le contraire, la saisie des paramètres de connexion de l'utilisateur ou l'utilisation de ses dispositifs d'authentification physique ou logique vaut preuve de son accès aux systèmes d'information et de communication. L'utilisateur reconnaît, en conséquence, être responsable de l'utilisation de ses moyens d'authentification.

En termes de sécurité et de confidentialité, l'utilisateur devra suivre toutes les prescriptions complémentaires qui lui seront signifiées par l'établissement.

L'établissement se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie, des moyens d'authentification de tout utilisateur en accord avec la chaîne décisionnelle et conformément à la politique de sécurité des systèmes d'information.

Article 4.2. Perte ou vol des moyens d'authentification

Si ces moyens d'authentification, par nature confidentiels, ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, ou encore s'ils ont été oubliés, l'utilisateur concerné doit, selon la procédure mise en place par l'établissement, renouveler ses moyens d'authentification selon la procédure en vigueur.

L'utilisateur devra aviser, sans délai, la chaîne décisionnelle de la perte ou du vol des moyens d'authentification. Il devra également, selon les cas, soit assister l'établissement, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

Article 4.3. Règles spécifiques de consultation et de partage des données de santé

Les utilisateurs sont informés que les données de santé auxquelles ils ont accès sont des données considérées comme « sensibles » au sens de la loi Informatique et Libertés et du Règlement Général sur la Protection des Données (RGPD), et sont protégées par le secret médical.

Compte-tenu de leur caractère sensible, la consultation et le partage des données de santé sont strictement limités par la loi (Code de la santé publique, Code de la Sécurité Sociale, loi Informatique et Libertés, ….).

Selon l'Article L. 1110-4 alinéa 3 du Code de la santé public, dans le cadre de la prise en charge d'une personne dans un établissement de santé, les destinataires des données de santé sont les membres de l'équipe de soins, à savoir les personnes habilitées à échanger des informations sur le patient afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible .

Dans ce contexte, seuls les professionnels de santé impliqués dans la prise en charge directe du patient afin d'assurer la continuité des soins peuvent être destinataires de données de santé.

Le personnel administratif peut avoir accès aux informations administratives du dossier patient voir aux données de santé selon le profil métier de l'utilisateur et selon les règles strictement définies par l'établissement.

Les utilisateurs sont informés que seules les personnes désignées et habilitées par la loi peuvent lire et échanger les données de santé des patients.

Les autorisations et habilitations octroyées par l'établissement permettant aux personnes qualifiées d'accéder aux données de santé s'effectuent dans le cadre des dispositions légales et réglementaires encadrant strictement l'accès aux Données de santé.

Les utilisateurs s'interdisent de consulter des informations pour lesquelles ni leur rôle ni leur champ de compétence ne leur donnent de droits particuliers.

Article 4.4. Modalités spécifiques d'accès et de partage des données de santé

Conformément au Décret du 15 mai 2007 définissant les règles relatives à la conservation sur support informatique des données de santé et à leur transmission par voie électronique entre professionnels, les professionnels de santé de l'établissement ont l'obligation d'utiliser la carte de professionnel de santé ou un dispositif équivalent en cas de transmission de données de santé par voie électronique.

La carte de professionnel de santé ou le dispositif équivalent permet ainsi aux Professionnels de santé entre autre de :

- apposer leur signature électronique sur des documents ;
- transmettre les feuilles de soins électroniques aux organismes d'Assurance Maladie obligatoires et complémentaires ;
- créer, alimenter et consulter les données de santé ;
- réaliser des actes médicaux à distance (télémédecine) ;
- utiliser la messagerie sécurisée des Professionnels de santé.

La carte de professionnel de santé ou le dispositif équivalent est un outil obligatoire imposé dans le cadre du partage de l'information médicale.

ARTICLE 5. GESTION DES ABSENCES ET DES DEPARTS

Article 5.1. Absence de l'utilisateur

En cas d'absence de l'utilisateur, celui-ci peut être sollicité par la chaîne décisionnelle de l'établissement afin de lui communiquer ses paramètres de connexion aux systèmes d'information et de communication, lorsque les informations détenues par l'utilisateur sur les équipements, moyens et outils informatiques et de communication mis à disposition par l'établissement sont nécessaires à la poursuite et/ou au bon fonctionnement de l'activité du service auquel appartient l'utilisateur.

Dans une telle hypothèse, l'utilisateur devra expressément autoriser la chaîne décisionnelle de l'établissement à accéder aux équipements, moyens et outils informatiques et de communication en suivant la procédure définie par la chaîne décisionnelle de l'établissement.

En outre, l'établissement se réserve le droit de mettre en place toute solution technologique permettant d'assurer la continuité de l'activité du service auquel appartient l'utilisateur en accord avec la chaîne décisionnelle de l'établissement.

Dans tous les cas qui requièrent l'urgence et en l'absence de possibilité pour l'utilisateur d'autoriser expressément la chaîne décisionnelle de l'établissement à accéder aux équipements, moyens et outils informatiques et de communication mis à disposition par l'établissement, l'utilisateur accepte que ses paramètres de connexion soient automatiquement réinitialisés afin de permettre à l'établissement d'accéder aux équipements, moyens et outils informatiques et de communication mis à disposition par l'établissement dès lors que les informations sont nécessaires à la poursuite et/ou au bon fonctionnement de l'activité du service auquel appartient l'Utilisateur.

L'utilisateur devra impérativement changer son mot de passe dès son retour ou à l'issue du traitement de l'urgence.

Les autorisations d'accès aux systèmes d'information et de communication sont retirées aux agents absents pour longue durée. Les personnes absentes souhaitant maintenir leur connexion doivent adresser une demande de dérogation à la chaîne décisionnelle de l'établissement avec l'accord du responsable hiérarchique.

En cas d'absence prévisible temporaire de l'établissement (congé, RTT, etc.) l'utilisateur doit, le jour de son départ, supprimer de sa messagerie électronique tous les messages reçus ou envoyés et identifiés comme étant « privés » et devra en faire de même avec ses fichiers identifiés comme étant « privés » qui se trouvent sur son poste de travail.

Article 5.2. Départ de l'utilisateur

En cas de départ définitif de l'établissement (départ en retraite, mutation, fin de contrat, démission, licenciement, etc.), l'utilisateur est informé par la présente charte que pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation des systèmes d'information et de communication pourront être modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois (3) mois, les moyens d'authentification et paramètres de connexion de l'utilisateur seront désactivés après son départ dans les meilleurs délais.

Lors de son départ, l'utilisateur doit :

- remettre en bon état général de fonctionnement et restituer, l'ensemble des équipements, moyens et outils informatiques et de communication qui lui ont été remis ;
- restituer les moyens d'authentification et paramètres de connexion qui lui auront été confiés ;
- supprimer les fichiers, répertoires et messages électroniques identifiés comme étant « privés », ainsi que tous les documents de même nature. A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments seront supprimés à l'issue du départ de l'utilisateur de l'établissement, sans être consultés, sans qu'aucune copie ne soit réalisée et sans que la responsabilité de l'établissement ne puisse être recherchée.

L'utilisateur s'interdit de disposer, utiliser, reproduire, copier, télécharger, diffuser ou emmener avec lui tout fichier, répertoire, donnée, information ou document professionnel de l'établissement.

ARTICLE 6. UTILISATION D'INTERNET ET DES SERVICES EN LIGNE

Article 6.1. Internet

En cas de mise à disposition d'un accès à Internet par l'établissement, et sous réserve des tolérances mentionnées à l'Article 3, il est rappelé qu'Internet doit être utilisé à des fins strictement professionnelles, pédagogiques et de recherche.

En conséquence, l'utilisateur est autorisé à utiliser Internet pour les seuls besoins de ses activités professionnelles et dans le respect de la législation en vigueur. Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle de l'utilisateur.

En tant que de besoin, il est rappelé que la consultation et/ou le téléchargement de contenu(s) à caractère pornographique, contraire aux bonnes mœurs, raciste, négationniste, révisionniste, incitant à la commission de crimes, de délits, ou d'infractions à la législation est strictement interdit et susceptible de poursuites pénales.

L'écoute de stations radiophoniques via Internet, le téléchargement de fichiers musicaux, de vidéos, de logiciels de jeux quel qu'en soit le format, à des fins autres que professionnelles, sont strictement prohibés dans la mesure où d'une part, ils peuvent gêner le fonctionnement des systèmes d'information de l'établissement en raison de l'encombrement qu'ils génèrent, tant en termes de volume de flux sur le réseau qu'en termes de place occupée sur les disques et d'autre part, parce que ces téléchargements sont soumis à des régimes juridiques spécifiques pouvant engager la responsabilité de l'établissement en cas de non-respect.

Il en est de même, d'une manière générale, de tous les contenus illicites ou pouvant, pour des raisons de sécurité, porter atteinte à l'image ou aux intérêts de l'établissement.

Pour des raisons de sécurité et de responsabilité ou encore de disponibilité des systèmes d'information, l'accès à certains sites peut être limité ou prohibé par l'établissement. Dans ce cadre, toute autorisation d'utilisation d'Internet peut être suspendu.

Article 6.2. Services en ligne

L'accès à des services en ligne (sites web, blogs, forums, chats, etc.) est strictement réservé à un usage professionnel.

L'utilisation de toutes solutions de stockage et/ou de partage d'information en lien avec l'activité professionnelle de l'utilisateur en mode « cloud » (Google Drive, WeTransfer, Dropbox, OneDrive etc.) est prohibée, sauf autorisation écrite du l'établissement.

L'établissement se réserve la possibilité de mettre à disposition des utilisateurs une solution de stockage et/ou de partage d'information en mode « cloud », de nature à assurer la confidentialité et la protection des données ainsi traitées, conformément aux lois et règlement en vigueur.

ARTICLE 7. UTILISATION DES RESEAUX SOCIAUX

Article 7.1. Les réseaux sociaux pour un usage professionnel

L'accès aux réseaux sociaux pour un usage professionnel est autorisé à condition que soit respectées la législation en vigueur, la jurisprudence et les règles énoncées dans la présente Charte.

L'utilisation et la publication sur les réseaux sociaux pour un usage professionnel engage la responsabilité de l'établissement et peut nuire à son image. Ainsi, lors de la rédaction et de la diffusion de messages sur ces supports, l'utilisateur a, de manière générale, l'obligation de veiller à respecter les règles de bonne conduite, de politesse et de courtoisie.

L'utilisateur devra s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'établissement.

Dans ce cadre, sont prohibés tous les messages :

- à caractère calomnieux, outrancier, diffamatoire, ordurier, injurieux, violent, raciste ou pornographique, incitant à la violence, à la haine ou à la discrimination ;
- appelant à commettre un délit ou faisant la propagande d'actes malveillants ;
- portant atteinte aux bonnes mœurs, à l'ordre public, à l'intégrité, à la dignité de la personne, aux droits d'autrui ;
- faisant la propagande de sectes ou incitant de manière directe ou indirecte à rejoindre une secte ;
- assimilables à de la propagande politique ;
- appelant au boycott ;
- diffusant des données à caractère personnel dont les données de santé permettant l'identification de personnes physiques ou morales sans l'autorisation écrite et préalable desdites personnes ;
- diffusant des contenus protégés par des droits de propriété intellectuelle et pour lesquels l'utilisateur n'a pas obtenu une autorisation préalable et explicite du titulaire des droits ;
- ayant pour objet ou pour effet de porter atteinte à la réputation de l'établissement ou à toute personne physique ou morale.

Un contrôle a posteriori des messages publiés sur les réseaux sociaux peut être effectué par l'établissement qui peut demander à l'utilisateur la suppression ou modification de tout ou partie d'un message qui ne remplirait pas les exigences mentionnées ci-dessus.

Article 7.2. Diffusion sur les réseaux sociaux dans un cadre non professionnel

Dans le cadre de la sphère non professionnelle et hors les murs de l'établissement, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux.

Cependant il s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles relatives à l'établissement ou à ses concurrents, des

informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'évènements, à la rémunération, etc.

L'utilisateur n'est aucunement autorisé à faire mention de ses missions au sein de l'établissement que sur les réseaux sociaux à caractère professionnel (par exemple, LinkedIn et Viadeo).

De manière générale, les médecins doivent veiller à respecter les recommandations présentées par le Conseil national de l'ordre des médecins publiées en décembre 2011.

Article 7.3. Signalement

De même, les utilisateurs sont invités à signaler tout message diffusé sur ces réseaux sociaux qui contreviendrait aux règles énoncées ci-dessus.

Qu'il utilise les réseaux sociaux à titre professionnel ou non professionnel, l'utilisateur pourra informer l'établissement d'un agissement de tiers susceptible de porter atteinte à la réputation de l'établissement ou à un droit de l'établissement (notamment de propriété intellectuelle) dont il aurait connaissance.

ARTICLE 8. UTILISATION DE LA MESSAGERIE ELECTRONIQUE

Article 8.1. Mise à disposition d'une adresse de messagerie électronique

En cas de mise à disposition d'une adresse de messagerie électronique par le l'établissement à l'utilisateur, et sous réserve des tolérances mentionnées à l'Article 3, il est rappelé que l'adresse électronique est strictement professionnelle. Elle ne doit donc pas :

- être utilisée dans un autre contexte, et notamment diffusée sur des sites internet (forums, blogs, etc.), sans rapport avec l'activité professionnelle, étant précisé que l'usage du « chat » c'est-à-dire de messageries instantanées est interdite ;
- faire l'objet d'un renvoi sur une boite de messagerie personnelle de l'utilisateur, que ce soit à titre temporaire ou permanent, de manière manuelle ou automatisée ;
- être destinataire d'un renvoi d'une messagerie personnelle que ce soit à titre temporaire ou permanent, de manière automatisée ;
- surcharger les serveurs de messagerie, et l'utilisateur doit veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires.

En l'absence de mise à disposition d'une adresse de messagerie électronique par l'établissement, les utilisateurs ne sont pas autorisés à utiliser une adresse de messagerie personnelle dans le cadre de leur activité professionnelle.

L'attention de l'utilisateur est attirée sur le fait qu'un message électronique laisse des traces et peut notamment être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant. Un message électronique peut constituer un indice, un commencement de preuve par écrit ou une preuve et être susceptible d'engager la responsabilité civile ou pénale de l'établissement et/ou de l'utilisateur. Il est donc recommandé de :

- respecter la plus grande correction dans les échanges électroniques, tant en interne qu'en externe ;
- ne pas émettre d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'établissement ou à des tiers ;
- ne pas usurper l'identité d'une autre personne afin, par exemple, d'intercepter des communications entre tiers.

En cas de réception à tort d'un message électronique interne destiné à une autre personne, l'utilisateur doit le renvoyer à son expéditeur en indiquant l'erreur d'adresse et doit le supprimer de sa boîte de réception, de ses éléments envoyés et de sa corbeille. Si le contenu de ce message était confidentiel, l'utilisateur s'interdit d'en faire état à quiconque, en interne comme en externe.

Il est rappelé aux Utilisateurs qu'Internet n'apporte pas une garantie totale d'acheminement des messages ni des délais d'acheminement de ceux-ci. Le risque de retard, de non remise ou de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes.

Article 8.2. Echange de données de santé

Les utilisateurs habilités à avoir accès aux données de santé des patients sont informés qu'il leur est strictement interdit d'échanger des données de santé avec un tiers de l'établissement par le biais de leur messagerie. Le transfert de données de santé en dehors de l'établissement ne peut se faire que par le bais d'une messagerie sécurisée ou toutes mesures de sécurité particulières autorisées par l'établissement.

Article 8.3. Utilisation à des fins personnelles

L'utilisation de la messagerie électronique à des fins personnelles, sous réserve des tolérances mentionnées à l'Article 3, doit respecter la législation en vigueur, la jurisprudence et les principes posés dans la présente charte d'utilisation des systèmes d'information. Dans ce cadre, les dispositions suivantes doivent être respectées :

- les messages doivent être signalés par la mention « privé » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « privé » ;
- les messages reçus doivent être classés, dès réception, dans un dossier dénommé « Privé » ;

A défaut d'avoir été identifié comme étant « privé », le message est réputé entré dans le cadre des activités professionnelles de l'utilisateur.

Article 8.4. Accès aux messages par l'établissement

Selon la jurisprudence, sont présumés avoir un caractère professionnel les messages électroniques reçus ou créés par un utilisateur grâce à des systèmes d'information et de communication de l'établissement ou de ses moyens ou ressources, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant « privés ».

Conformément à l'Article 3 de la présente charte, il en résulte que :

- l'établissement peut y accéder librement, sans autorisation et hors de la présence de l'utilisateur ;
- les messages identifiés comme étant « privés » ne sont accessibles qu'en présence de l'utilisateur et avec son accord, sauf en cas de risque ou d'évènement particulier, si l'utilisateur a été prévenu.

En tant que de besoin, il est rappelé que l'utilisateur ne saurait transformer des messages relevant de ses activités professionnelles en correspondance qualifiée de « privée ». Toute démarche qui consisterait à qualifier de « privé » un message dans le seul but de le soustraire à la lecture de l'établissement caractériserait un manquement de l'utilisateur à ses obligations et constituerait une faute susceptible d'entrainer des sanctions disciplinaires.

ARTICLE 9. UTILISATION DES SERVICES DE TELEPHONIE

Les postes téléphoniques fixes ou mobiles mis à la disposition de certains utilisateurs le sont à des fins professionnelles.

L'utilisation des postes téléphoniques à des fins personnelles est tolérée à condition qu'une telle utilisation soit raisonnable, qu'elle n'affecte pas l'exercice de ses fonctions par l'utilisateur, n'entrave pas la sécurité des Systèmes d'information de l'établissement, ni ne gêne la bonne marche de son activité.

Les Utilisateurs sont informés que le système de téléphonie enregistre les numéros de téléphones entrants et sortants, et que des relevés téléphoniques sont établis.

Les Utilisateurs sont informés que les données relatives à l'utilisation des services de téléphonie ne sont conservées, en principe, que pour une durée maximale d'un (1) an, conformément à la législation.

Les Utilisateurs sont informés qu'une consommation excessive des services de téléphonie à des fins personnelles pourra faire l'objet de sanctions disciplinaires, s'il y a lieu.

ARTICLE 10. FICHIERS ET REPERTOIRES CREES PAR L'UTILISATEUR

Article 10.1. Utilisation des espaces de stockage professionnels

L'utilisateur doit créer et stocker les fichiers et répertoires dans les emplacements prévus à cet effet mis à disposition par l'établissement.

A la demande de l'utilisateur, et sous réserve de nécessité, l'établissement mettra à disposition des environnements sauvegardés pour le stockage des répertoires et des fichiers.

Article 10.2. Utilisation à des fins personnelles

Les fichiers ou répertoires créés par l'utilisateur grâce aux équipements, moyens et outils informatiques et de communication mis à sa disposition pour l'exercice de ses activités sont présumés, sauf si l'utilisateur les identifie expressément comme étant « privés », entré dans le cadre de ses activités professionnelles.

Tout fichier ou répertoire qui n'est pas identifié comme « privé » est réputé relever des activités professionnelles de l'utilisateur de sorte que l'établissement peut y accéder librement, sans autorisation de l'utilisateur et hors la présence de ce dernier.

En revanche, si un fichier ou répertoire est identifié comme étant « privé », l'établissement ne peut y avoir accès qu'en présence de l'utilisateur ou si celui-ci a été prévenu, sauf en cas de risque ou d'évènement particulier et selon les règles définies dans l'Article 3.

Un fichier ou répertoire identifié avec les initiales ou le nom d'un utilisateur ne sera pas considéré comme « privé ».

L'établissement ne saurait être tenu pour responsable de la destruction ou l'altération de ces fichiers « privés ».

Article 10.3. Accès aux fichiers et répertoires par l'établissement

Selon la jurisprudence, sont présumés avoir un caractère professionnel :

- les fichiers créés par un utilisateur grâce à des systèmes d'information et de communication de l'établissement ou de ses moyens ou ressources, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant « privés » ;
- les supports de stockage externes dès lors qu'ils sont connectées à un outil informatique mis à la disposition de l'utilisateur par l'établissement dans le cadre de son activité professionnelle.

Conformément à l'Article 3 de la présente charte, il en résulte que :

- l'établissement peut y accéder librement, sans autorisation et hors de la présence de l'utilisateur ;

- aucune information à caractère professionnel ne peut être ni stockée dans un répertoire informatique utilisé à des fins non professionnelles, ni stockée sur un support de stockage externe non dument autorisé ;
- les fichiers identifiés comme étant « privés » ne sont accessibles qu'en présence de l'utilisateur ou si celui-ci a été prévenu, sauf en cas de risque ou d'évènement particulier.

En tant que de besoin, il est rappelé que l'utilisateur ne saurait enregistrer des informations ou documents relevant de ses activités professionnelles, dans des fichiers, répertoires ou tout support de stockage identifiés comme étant « privés ». Toute démarche qui consisterait à qualifier de « privé » un fichier ou un répertoire dans le seul but de le soustraire à la lecture de l'établissement caractériserait un manquement de l'utilisateur à ses obligations et constituerait une faute susceptible d'entrainer des sanctions disciplinaires.

ARTICLE 11. UTILISATION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION A DES FINS DE TELEMEDECINE

L'établissement permet aux professionnels de santé d'effectuer des actes de télémédecine via les systèmes d'information et de communication dès lors que cette activité a été organisée par l'établissement.

L'Article L. 6316-1 du Code de la santé publique définit la télémédecine comme :

« Une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs Professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient ».

La télémédecine permet aux Professionnels de santé d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients.

Les actes de télémédecine pouvant être effectués par les utilisateurs professionnels de santé sont les suivants :

- la téléconsultation ;
- la télé expertise ;
- la télésurveillance médicale ;
- la téléassistance médicale ;
- la régulation médicale.

Il est rappelé aux utilisateurs que seules les personnes désignées et habilitées par la loi peuvent effectuer des actes de télémédecine.

Les utilisateurs habilités à effectuer des actes de télémédecine s'engagent à respecter les dispositions légales et réglementaires relatives à l'exercice de la profession médicale telles que notamment les articles du Code de la santé publique et du Code de déontologie médicale.

En particuliers, selon les articles R. 4127-76 et R. 5132-3 du Code de la Santé Publique, les prescriptions doivent être conformes aux constatations médicales faites par les médecins et sont liées à un examen médical du patient. Elles sont rédigées, datées et signées par leurs auteurs.

Les utilisateurs sont informés que les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne concernée, sauf cas particuliers (par ex : coma ou autre impossibilité de donner son consentement…). La personne doit notamment être informée de son état de santé, des traitements et actions envisagés ainsi que des risques.

Les professionnels participant à un acte de télémédecine peuvent, sauf opposition du patient dûment informé, échanger des informations le concernant.

Compte tenu des risques que comporterait la transmission d'informations dégradées ou la divulgation de celles-ci à des tiers, il incombe aux utilisateurs effectuant des actes de télémédecine de respecter les règles de sécurité informatique énumérées au sein de la présente charte et de la politique de sécurité des systèmes d'information du GHT.

ARTICLE 12. EQUIPEMENTS MIS A LA DISPOSITION DES UTILISATEURS

Article 12.1. Périphériques mobiles

Les téléphones mobiles, smartphone, ordinateur portable ou tout autre périphérique mobile mis à la disposition de l'utilisateur, par l'établissement, le sont à des fins professionnelles, pédagogiques et de recherche.

L'utilisateur veille à utiliser son ordinateur portable ou tout autre périphérique mobile dans un espace dans lequel il est à même d'assurer la confidentialité des échanges. Il doit également veiller à ce que des tiers non autorisés ne puissent accéder aux systèmes d'information et de communication, les utiliser ou accéder à leurs contenus.

L'utilisateur n'est autorisé à les utiliser à des fins personnelles qu'à titre résiduel et dans le respect des règles édictées par la présente charte.

L'utilisateur s'interdit de conserver ou de stocker des informations confidentielles ou sensibles, relatives aux patients sur un ordinateur portable ou tout périphérique mobiles mis à sa disposition dans la mesure où ceux-ci ne sont pas sécurisés.

En cas de doute, l'utilisateur s'adressera à la chaine décisionnelle afin de mettre en œuvre les mesures de protection édictées par l'établissement pour préserver la sécurité et la confidentialité des informations stockées.

En cas non seulement d'incident avéré mais également de doute, l'utilisateur doit immédiatement en aviser le l'établissement.

Article 12.2. Badges

Des badges (cartes magnétiques ou à puce) sont remis aux utilisateurs le jour de leur entrée en fonction dans les locaux de l'établissement ou lors de demandes d'accès spécifiques.

Ces badges peuvent avoir plusieurs fonctionnalités telles que le contrôle de l'accès physique et/ou logique, la gestion des temps de travail ainsi que la gestion de la restauration de l'établissement.

Ces badges sont personnels et incessibles. Ils ne doivent pas être prêtés, partagés, loués ou cédés à qui que ce soit, pour quelque raison que ce soit.

L'enregistrement du badge d'un utilisateur sur une badgeuse vaut preuve de l'accès physique ou logique de celui-ci. L'utilisateur reconnaît, en conséquence, être responsable de l'utilisation de son badge.

Le jour de son départ, l'utilisateur est tenu de restituer son badge au service en charge de la gestion des badges.

ARTICLE 13. CONNEXION DES EQUIPEMENTS MOBILES PERSONNELS AUX SYSTEMES D'INFORMATION ET DE COMMUNICATION DE L'ETABLISSEMENT

Article 13.1. L'accès aux systèmes d'information et de communication

L'utilisateur ne peut utiliser à des fins professionnelles des systèmes d'information et de communication qui sont sa propriété personnelle ou qu'il détient à titre personnel, sauf autorisation explicite de l'établissement et sous réserve du respect des prescriptions techniques exigées par la Direction des Systèmes d'Information et de l'Organisation (DSIO).

La connexion par les utilisateurs de leurs équipements mobiles personnels (ordinateurs, téléphones, smartphones, tablettes tactiles etc.), sur site ou à distance, au système d'information de l'établissement est autorisée dans la mesure où l'utilisation de ce matériel est en conformité avec les stipulations de la présente charte et de la politique de sécurité propre aux équipements mobiles personnels de l'établissement.

L'établissement est libre de refuser la connexion d'un équipement mobile personnel sur ses systèmes d'information si l'équipement en question n'est pas conforme aux contraintes de sécurité de l'établissement.

L''utilisateur s'engage à toujours disposer d'un équipement mobile personnel en état de fonctionnement et à télécharger régulièrement les mises à jour proposées par les éditeurs des logiciels et applications de sécurité utilisée.

L'utilisateur doit faire l'acquisition d'outils tels que notamment des logiciels antivirus et de chiffrement des données permettant de limiter les risques d'atteinte à la sécurité des systèmes d'information de l'établissement.

L'utilisateur s'engage à protéger son Equipement mobile personnel par un identifiant et un mot de passe afin d'empêcher les tiers d'avoir accès aux systèmes d'information et de communication de l'établissement.

En cas de vol, perte, ou constat quelconque d'intrusion frauduleuse sur l'équipement personnel, l'Utilisateur devra immédiatement prévenir la chaine décisionnelle afin que des mesures nécessaires soient prises pour protéger les systèmes d'information et de communication de l'établissement et les données y étant stockées.

Les accès aux systèmes d'information et de communication de l'établissement par des équipements personnels en dehors des horaires de travail peuvent être directement bloqués à distance par les personnes habilitées de l'établissement.

Article 13.2. La propriété et le contrôle des données accessibles via l'équipement mobile personnel

L'utilisateur est informé que toutes données relevant de ses activités professionnelles stockées ou accessibles via un équipement mobile personnel demeureront la propriété exclusive de l'établissement.

L'établissement se réserve le droit d'accéder et de contrôler les données relevant de ses activités professionnelles stockées sur l'équipement personnel de l'utilisateur.

En cas de départ de l'établissement, l'utilisateur s'engage à transférer à l'établissement l'ensemble des données relevant de ses activités professionnelles éventuellement stockées sur son équipement personnel.

Article 13.3. Responsabilité en cas de vol ou de dommages matériels causés à l'équipement mobile personnel

L'utilisation de l'équipement mobile personnel reste sous l'entière responsabilité des utilisateurs. Il appartient notamment aux utilisateurs de prendre toutes les mesures appropriées de façon à protéger leurs propres données et/ou logiciels, notamment de la contamination par d'éventuels virus circulant sur le réseau internet ou de l'intrusion d'un tiers dans le système de son terminal (ordinateur PC portable, smartphone…) à quelque fin que ce soit.

L'établissement ne saurait être responsable des éventuels dommages causés à l'équipement mobile personnel de l'utilisateur résultant notamment d'une utilisation de son équipement non conforme aux règles de sécurité énumérées au sein de la présente charte et de la dernière version de la politique de sécurité propre aux équipements mobiles personnels de l'établissement.

Article 13.4. Utilisations prohibées de l'équipement mobile personnel

L'utilisateur est informé que les règles d'utilisation prohibées des systèmes d'information et de communication de l'établissement s'étendent à son équipement mobile personnel lorsqu'il se connecte aux systèmes d'information et de communication de l'établissement (atteinte à la vie privée ou à l'image d'un tiers, diffamation, injure, discrimination, dénigrement de l'établissement, l'atteinte à l'image de marque, à sa réputation ou à ses droits…).

De même, sont prohibés les téléchargements de contenus portant atteinte au droit de propriété intellectuelle effectués par l'utilisateur via les systèmes d'information et de communication de l'établissement avec son équipement mobile personnel.

ARTICLE 14. CONNEXIONS A DISTANCE AUX SYSTEMES D'INFORMATION ET DE COMMUNICATION

Article 14.1. Accès à distance

L'établissement met à disposition des utilisateurs, un accès à distance de ses systèmes d'information et de communication au travers d'une connexion sécurisée personnelle, sous réserve de la nécessité de service et en fonction des besoins métier :

- accès applicatifs ;
- bureau à distance ;
- accès à la messagerie ;
- accès aux fichiers partagés sur les disques et sites intranet dédiés.

L'utilisation des systèmes d'information et de communication de l'établissement l'accès à distance implique le respect de la présente charte par les Utilisateurs.

L'utilisateur est responsable de l'usage qu'il fait des systèmes d'information et de communication, et s'engage à respecter les règles de sécurité informatique prévues à cet effet. Notamment, à ne pas effectuer intentionnellement des opérations pouvant avoir pour conséquences :

- de masquer sa véritable identité ou de s'approprier des moyens d'authentification d'un autre utilisateur ;
- d'intercepter des communications entre tiers ;
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants.

L'utilisateur s'engage à ne pas effectuer d'opérations pouvant nuire au bon fonctionnement du réseau et à l'intégrité des systèmes d'information et de communication de l'établissement. Il s'engage à clore sa session informatique en cas d'éloignement de son poste informatique.

L'utilisateur est informé que l'ensemble des services utilisés génère « des fichiers de traces » essentiels à l'administration des systèmes.

Dans le cadre d'une enquête interne ou d'une réquisition judiciaire et après accord de la chaîne décisionnelle, ces fichiers peuvent être transmis aux autorités compétentes.

Article 14.2. Utilisation à des fins médicales

Il est rappelé aux professionnels de santé que les diagnostics à distance doivent être réalisés uniquement dans le cadre de la télémédecine. Les professionnels de santé ne pourront effectuer à distance que des actions de contrôle, de suivi et d'avis, à l'exclusion des actes visés dans le cadre légal applicable à la télémédecine.

Article 14.3. Cas du télétravail

L'établissement se réserve la possibilité de mettre en œuvre du télétravail selon la législation en vigueur.

Le cas échéant, l'utilisation autorisée au télétravail devra suivre les dispositions de la charte ainsi que l'ensemble des procédures et instructions données par le l'établissement pour l'utilisation des systèmes d'information et de communication.

ARTICLE 15. PROTECTION DE LA PROPRIETE INTELLECTUELLE ET DE L'IMAGE

L'utilisation des systèmes d'information et de communication de l'établissement implique le respect des droits de propriété intellectuelle, ainsi que de l'image de marque de l'établissement.

A ce titre, il est rappelé que les logiciels, bases de données, documents techniques ou commerciaux et les éventuelles créations graphiques du l'établissement sont des actifs immatériels qui lui appartiennent et qui bénéficient d'une protection particulière.

Les utilisateurs s'engagent donc à ne pas procéder, par quelque moyen que ce soit, à des actes de contrefaçon sur ces actifs.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'établissement, c'est-à-dire dans le respect des indications données par l'établissement ;
- ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, de tenter d'installer des logiciels ou applications pour lesquels l'établissement ne possèderait pas un droit d'usage ;
- ne pas reproduire, copier, utiliser, remettre à des tiers ou diffuser, les éléments appartenant au l'établissement ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles ;
- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des personnels ou de tiers au l'établissement ;
- ne pas nuire à l'image de marque du l'établissement en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de l'établissement ou du fait de leur accès par internet ou toute autre moyen de communication.

ARTICLE 16. PRESERVATION DE LA CONFIDENTIALITE ET DU SECRET

Article 16.1. Confidentialité des données

Le respect de la confidentialité des données est une exigence essentielle du l'établissement. L'utilisateur s'engage donc à une stricte obligation de confidentialité à l'égard des informations qu'il peut être amené à connaître dans le cadre de ses activités.

L'utilisateur s'engage à ne pas divulguer d'informations confidentielles ou sensibles relatives aux patients, aux personnels ou à l'établissement et de manière générale, toute information dont la divulgation pourrait porter préjudice à l'établissement ou à des tiers.

Il veille à ce que les informations qu'il exploite ne puissent pas être consultées, modifiées ou reproduites par un tiers.

Le respect de cette obligation de confidentialité implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres utilisateurs ;
- ne pas extraire ces informations et données confidentielles et ne pas les reproduire sans l'accord préalable de l'établissement et/ou de les détourner de leur utilisation normale à des fins non professionnelles ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein du l'établissement.

Il est rappelé que l'obligation de confidentialité subsiste au-delà de la durée du contrat de travail, de la convention de stage ou de tout autre type de relation professionnelle que l'utilisateur peut avoir avec le l'établissement.

Article 16.2. Secret médical et professionnel

Le secret médical et professionnel réside dans l'obligation de ne pas révéler à des tiers des informations d'ordre médical ou privé concernant la personne soignée.

Les utilisateurs sont informés que le secret médical et professionnel couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé ou du personnel administratif, c'est à dire tout ce qui lui a été confié, mais aussi tout ce qu'il a vu, lu, entendu, constaté ou compris.

Sont ainsi protégés par le secret les déclarations et confidences du patient et de son entourage, les faits découverts au cours de soins, les faits ou circonstances en rapport avec l'état du patient, les éléments du traitement (prescriptions, médicaments, pronostics, diagnostics...) mais aussi tout élément de la vie privée du patient (conflit familial, difficultés matérielles...).

L'article L 1110-4 alinéa 1er du Code de la santé publique énonce que :

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

L'utilisateur ayant accès à des informations soumises au secret médical et professionnel s'engage à 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'utilisateur s'engage à ne pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ ou confidentielles couvertes par le secret médical et professionnel.

La violation du secret médical et professionnel peut donner lieu à des sanctions pénales, civiles et ordinales.

L'article 226-13 du Code pénal sanctionne les personnes portant atteinte à une information à caractère secret d'une peine pouvant aller jusqu'à un an d'emprisonnement et 15 000 euros d'amende.

Sur le plan civil, le patient qui subit un préjudice en raison de la révélation d'informations couvertes par le secret peut obtenir des dommages et intérêts.

Enfin, sur le plan disciplinaire, les ordres professionnels peuvent infliger aux Professionnels de santé une peine disciplinaire (avertissement, blâme, suspension temporaire d'exercice, radiation du tableau de l'Ordre).

De surcroît, l'utilisateur est informé qu'une atteinte au secret médical et professionnel pourra faire l'objet de sanctions disciplinaires par l'établissement, s'il y a lieu.

ARTICLE 17. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 17.1. Devoirs de l'utilisateur

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel. Ces dispositions figurent pour l'essentiel dans le Règlement Général sur la Protection des Données (loi n° 2018-493 du 20 juin 2018) et la loi Informatique et Libertés (loi n° 78-17).

Dans ce cadre, les utilisateurs devront se conformer à la procédure en cas de mise en œuvre d'un traitement de données à caractère personnel.

Toute nouvelle constitution de fichiers ou de bases de données comprenant des données à caractère personnel doit faire l'objet de formalités préalables auprès du Délégué à la Protection des Données (DPO), sauf dérogations légales ou réglementaires. Dans ce cadre, l'utilisateur doit respecter les finalités des traitements de données à caractère personnel objets de ces formalités préalables et aucun utilisateur ne peut de son propre chef mettre en œuvre un tel traitement automatisé.

Conformément au Règlement Général sur la Protection des Données et à la loi Informatique et Libertés, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un tel traitement impliquent que les données à caractère personnel doivent être :

- traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1 du Règlement Général sur la Protection des Données, comme incompatible avec les finalités initiales (limitation des finalités) ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1 du Règlement Général sur la Protection des Données, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises

par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Article 17.2. Droits de l'utilisateur

L'établissement met en œuvre des traitements de données à caractère personnel concernant les utilisateurs. 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. Ces données sont destinées aux personnes habilitées au sein de l'établissement ainsi qu'aux autorités habilitées.

Les traitements opérés dans le cadre de la présente charte ont pour finalité :

- le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- la gestion des annuaires 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 systèmes d'information et de communication, notamment la conservation des logs de connexion et des données de toute nature ;
- la gestion de la messagerie électronique ;
- 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 agenda des personnes répertoriées dans ces réseaux ;
- le respect de la présente charte.

A toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion et d'organisation des systèmes d'information et de communication électronique.

Conformément au Règlement Général sur la Protection des Données et à la loi Informatique et Libertés, l'utilisateur est informé, en particulier, qu'il dispose d'un droit d'interrogation, d'accès, de rectification et d'opposition pour motif légitime au traitement des données le concernant et qui s'exerce auprès du Délégué à la Protection des Données (DPO).

ARTICLE 18. PROTECTION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Article 18.1. Mise en œuvre

L'établissement met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité physique et logique des systèmes d'information et de communication tels que définis et détaillés au sein de sa politique de sécurité des systèmes d'information.

A ce titre, il lui appartient de limiter, selon les besoins dictés par les missions de chacun, les accès aux systèmes d'information et de communication, et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation desdits systèmes d'information et de communication mis à la disposition de l'utilisateur.

Les systèmes d'information et de communication sont exclusivement installés, configurés, paramétrés et gérés par le personnel habilité par l'établissement.

Si un risque est identifié ou en cas d'évènement particulier, l'établissement peut décider de :

- accéder aux équipements, moyens et outils informatiques et de communication mis à disposition de l'utilisateur, y compris à tous les fichiers et données identifiés comme « privés » par celui-ci, sans toutefois pouvoir en divulguer le contenu ;
- suspendre tout ou partie de l'accès aux systèmes d'information ou de communication, sans préavis.

Article 18.2. Devoirs de l'utilisateur

L'utilisateur doit, quant à lui, dans l'exercice de ses fonctions, concourir à la protection desdits systèmes d'information et de communication, en faisant preuve de prudence, en toutes circonstances. En cas de doute sur l'attitude à tenir, il doit interroger préalablement la chaîne décisionnelle.

L'utilisateur doit, à ce titre, se conformer notamment mais non limitativement aux règles de conduite suivantes :

- en cas d'absence, même temporaire et de courte durée, verrouiller l'accès au matériel qui lui est confié ou à son équipement personnel, dès lors que celui-ci contient des informations relatives à ses activités professionnelles ;
- effectuer des enregistrements réguliers des fichiers et données de l'établissement dont il dispose sur le matériel mis à sa disposition. A ce titre, l'utilisateur doit s'assurer que les fichiers et données qu'il stocke le sont sur des espaces régulièrement sauvegardés par l'établissement. Ces enregistrements réguliers doivent impérativement être effectués systèmes de sauvegarde de l'établissement.
- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du courrier électronique est inconnu ou douteux ;

- ne pas transmettre de fichiers ou données sensibles à une personne qui en ferait la demande et dont il ne se serait pas assuré au préalable de l'identité, même si cette demande émane d'une adresse électronique interne à l'établissement ;
- avant tout envoi ou communication, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir la communication des informations transmises ;
- en cas d'envoi à une pluralité de destinataires, l'utilisateur doit 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 ;
- en cas d'envoi à une liste de diffusion, il est important de vérifier la liste des destinataires de celle-ci ;
- détruire les messages du type « chaîne de solidarité » ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la Direction des systèmes d'information et de l'organisation (DSIO) ;
- prendre toutes précautions nécessaires en cas d'utilisation d'un matériel nomade, incluant de ne pas le mettre en évidence pendant un déplacement, de ne pas exposer son contenu à la vue d'un voisin, de le ranger dans un lieu sûr, de même que les supports mobiles de données (exemples : CD, disquettes, clé USB, etc…) dont l'usage doit être fait avec une très grande vigilance ; l'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces matériels nomades et supports mobiles, notamment en bloquant les ports de connexion des outils informatique ;
- mettre sous clé tout dossier ou document confidentiel et verrouiller son ordinateur ou terminal lorsque l'utilisateur quitte son espace de travail.

L'utilisateur ne doit pas porter atteinte à la sécurité de l'établissement et/ou à la propriété intellectuelle des tiers. Il ne doit notamment pas :

- installer des logiciels en dehors des licences, copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein de l'établissement et ce, même si l'utilisateur est, pour les besoins de ses fonctions, administrateur des équipements mis à sa disposition et peuvent techniquement le faire ;
- sans autorisation expresse, décompiler, désassembler, altérer les systèmes et les données issues des systèmes d'information et de communication de l'établissement, pratiquer l'ingénierie inverse ou tenter de découvrir ou reconstituer le code source des logiciels/progiciels, les idées qui en sont la base, les algorithmes, les formats de fichier ou les interfaces de programmation ou d'interopérabilité, à moins que cela ne relève de ses fonctions ou de son contrat de travail ;
- sans autorisation expresse, traduire, adapter, arranger, modifier les équipements, moyens et outils informatiques et de communication mis à disposition de l'utilisateur à moins que cela ne relèvent de ses fonctions telles qu'elles sont prévues par son contrat de travail ;
- sans autorisation expresse, procéder seul ou avec l'aide d'un tiers à la correction des éventuelles erreurs, dysfonctionnements des systèmes d'information et de communication de l'établissement pour les rendre conforme à sa destination à moins que cela ne relèvent de ses fonctions telles qu'elles sont prévues par son contrat de travail ;

- utiliser les équipements, moyens et outils informatiques et de communication mis à disposition de l'utilisateur pour un usage autre que conforme à sa destination et/ou qui serait de nature à créer un risque pour l'établissement ou qui nuirait aux intérêts de l'établissement ;
- détourner les réseaux de communication ou en faire un usage autre que conforme à leur destination et/ou qui serait de nature à créer un risque pour l'établissement ou qui nuirait aux intérêts de l'établissement.

Articles 18.3. Mesures d'urgence et plan de continuité d'activité

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, l'établissement peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande de l'établissement à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des systèmes d'information et de communication (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources des systèmes d'information et de communication (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

ARTICLE 19. OUTILS DE CONTROLE MIS EN PLACE PAR L'ETABLISSEMENT

Article 19.1. Contrôle et audit

Pour des raisons de sécurité et de bon fonctionnement des systèmes d'information et de communication, et en particulier pour des raisons de confidentialité des données sensibles, l'utilisateur est informé que l'établissement met en œuvre un certain nombre d'outils lui permettant de contrôler et d'auditer l'utilisation de ses systèmes d'information et de communication par les utilisateurs.

Les opérations de contrôle et d'audit portent sur la régularité de l'utilisation des systèmes d'information et de communication. Elles se justifient par les obligations incombant à l'établissement.

De par son activité, l'établissement est soumis à une obligation générale de sécurité, en application, entre autre et de manière non exhaustive, des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E) et sa déclinaison sectorielle, du Règlement Général pour la Protection des Données, et de la loi dite « Informatique et libertés ».

L'utilisation des systèmes d'information et de communication pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

L'établissement se réserve ainsi le droit, notamment, que ce soit de manière automatique ou manuelle :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources des systèmes d'information et de communication ;
- de contrôler l'origine licite des logiciels installés ;
- de conserver des fichiers de journalisation des traces informatiques en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, l'établissement se réserve le droit de, que ce soit de manière automatique ou manuelle :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu des équipements, moyens et outils informatiques et de communication mis à disposition ;
- procéder à toutes copies utiles pour faire valoir ses droits.

Ces opérations de contrôle et d'audit relèvent des fonctions de la Direction des Systèmes d'Information et de l'Organisation de l'établissement, sous le contrôle du Responsable de la Sécurité des Systèmes d'Information (RSSI) du GHT.

En particulier, dans le cadre de ses fonctions, elle peut exercer un contrôle notamment des durées de connexion et des sites les plus visités. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, elle est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

Le Responsable de la Sécurité des Systèmes d'Information et tout intervenant de la Direction des systèmes d'information et de l'organisation doivent impérativement respecter la confidentialité des échanges électroniques et des fichiers de l'utilisateur.

En cas de faisceau d'indices laissant supposer qu'un utilisateur interne de l'établissement met en cause les intérêts et la sécurité de l'établissement, en ne respectant pas les règles instituées par la présente charte, la Direction des systèmes d'information et de l'organisation, sous le contrôle du Responsable de la Sécurité des Systèmes d'Information , se réserve le droit de fournir à la Direction des ressources humaines, sur sa demande écrite et motivée, les traces informatiques individuelles des connexions incriminées.

En cas de non-respect avéré de la présente charte par un utilisateur externe de l'établissement, la Direction des systèmes d'information et de l'organisation, sous le contrôle du Responsable de la Sécurité des Systèmes d'Information, se verra dans l'obligation d'avertir la direction de la société ou de l'organisme d'appartenance de l'utilisateur pour que celle-ci décide de la suite à donner.

Suivant la gravité des faits, les droits d'accès et habilitations de l'utilisateur concerné pourront être suspendus temporairement ou définitivement.

Article 19.2. Traçabilité

Pour satisfaire aux obligations légales et réglementaires qui lui incombent (exigence de traçabilité), et notamment pour s'assurer de sa capacité à apporter la preuve, le cas échéant, du bon usage des ressources et moyens informatiques et de communication électronique mis à la disposition de l'utilisateur, l'établissement met en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des moyens informatiques et de communication électronique.

Le cas échéant, les traces informatiques sont conservées pour une durée limitée en conformité avec la politique de sécurité des systèmes d'information, le Règlement Général pour la Protection des Données et la loi Informatique et Libertés.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

Article 19.3. Filtrage

Pour satisfaire aux obligations légales et réglementaires qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de de ses systèmes d'information et de communication, le l'établissement procède à la mise en place d'outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet.

Il est précisé que ces outils, en ce qu'ils portent entre autre et non limitativement sur l'accès à internet, et permettent notamment un contrôle des connexions des utilisateurs, leur identifiant, du système auquel il est accédé, du type d'opération réalise, des informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ou des applications de l'Etablissement, la durée de connexion, etc.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

Article 19.4. Scan informatique

Le scannage informatique consiste à contrôler à travers des outils informatiques la présence de mots clés dans des contenus professionnels des moyens informatiques et de communication électronique de l'Etablissement.

L'établissement se réserve le droit de mettre en œuvre des opérations de scan des moyens informatiques et de communication électronique tels que le scan des éléments professionnels de l'utilisateur, et notamment des documents, des dossiers, des courriers électroniques, pièces jointes, fichiers.

Les documents, dossiers, courriers électroniques, pièces jointes, etc. identifiés comme « privé », par l'utilisateur, ne seront pas consultés par le l'établissement, sauf respect des dispositions légales particulières en la matière.

Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés. Ils permettent à l'établissement de disposer d'un dispositif d'alerte prudentiel et rapide de ses moyens informatiques et de communication électronique.

Article 19.5. Vidéosurveillance

Les Utilisateurs sont informés qu'à des fins de sécurité et de contrôle, l'accès aux locaux de l'établissement est protégé par des caméras de vidéosurveillance.

Ces caméras fonctionnent 24h/24, 7 jours/7. Elles n'enregistrent que les images et non le son associé aux images.

Des panneaux affichés dans les locaux sous vidéosurveillance précisent également à l'utilisateur la présence de caméras.

Ces images ne sont visionnées que par les personnes habilitées à cet effet de l'établissement.

Les images sont conservées pour une durée maximale de un (1) mois, conformément à la législation.

Il est rappelé que le système de vidéosurveillance mis en place n'a pas pour objet la surveillance spécifique d'un utilisateur ou d'un groupe d'utilisateurs déterminé.

L'enlèvement ou la neutralisation des caméras de surveillance sans justificatif est strictement interdit.

ARTICLE 20. NON-RESPECT DE LA CHARTE

Les règles définies dans la présente charte ont été fixées par la direction de l'établissement dans le respect des dispositions législatives et réglementaires applicables.

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conforme aux règles d'accès et d'usage des systèmes d'information et de communication décrites dans la charte.

Toute mauvaise utilisation ou utilisation non conforme aux conditions et limites définies par cette charte est constitutive d'une faute. En conséquence, le non-respect des dispositions légales et règlementaires ainsi que de la présente charte expose l'utilisateur en cause à des sanctions :

- l'utilisateur s'expose à des sanctions concernant son droit d'utiliser les systèmes d'information et de communication notamment : le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie des systèmes d'information et de communication. ;
- l'utilisateur peut faire l'objet de sanctions disciplinaires ;
- l'utilisateur est susceptible d'engager sa responsabilité personnelle, tant sur le plan civil que sur le plan pénal.

L'utilisateur est informé que la direction de l'établissement est tenue de signaler toutes infractions pénales commises par son personnel au procureur de la République.

L'établissement, pour sa part, déclare mettre en œuvre, par le biais notamment de la charte, tous les efforts nécessaires à un bon usage des systèmes d'information et de communication et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

ARTICLE 21. DEROGATIONS AUX REGLES DEFINIES DANS LA PRESENTE CHARTE

Les demandes spécifiques de l'utilisateur relatives à l'utilisation des systèmes d'information en dehors du périmètre de la présente charte ou en contradiction avec les règles définies dans la charte doivent être adressées directement au supérieur hiérarchique de l'utilisateur ainsi qu'au Responsable de la Sécurité des Systèmes d'Information dans un document écrit et signé par le demandeur.

Responsable de la Sécurité des Systèmes d'Information communiquera à la direction de l'établissement les demandes de dérogation au respect des règles définies dans la présente charte.

L'autorisation exceptionnelle ou le refus de la direction de l'établissement de déroger aux règles de la présente charte sera formalisé dans un document signé et daté.

ARTICLE 22. ENTREE EN VIGUEUR ET INFORMATION DE L'UTILISATEUR

La présente charte est :

- pour les personnels de l'établissement, agents titulaires et contractuels concourant à l'exécution des missions du service public hospitalier, les étudiants rémunérés ou non par l'établissement, les stagiaires et apprentis, les enseignants, les chercheurs : annexée au règlement intérieur ;
- pour les prestataires ou sous-traitants de l'établissement : annexée au contrat de prestation ou de sous-traitance conclu avec le l'établissement ;
- pour les professionnels de santé non-salariés : toute validation d'accès au système d'information et de communication de l'établissement emporte l'acceptation sans réserve de la présente charte. Si l'utilisateur ne souhaite pas être lié par les termes des présentes, il ne peut pas être connecté au système d'information et de communication du l'établissement.

En conséquence, l'utilisateur quel qu'il soit, est supposé en avoir pris connaissance.

Les instances représentatives du personnel sont informées de l'entrée en vigueur de la présente charte.

La présente charte annule et remplace, en toutes ses stipulations, la précédente charte.

Elle est applicable à compter de la date d'approbation par le directeur d'établissement.