CENTRE HOSPITALIER d'Ardèche Nord	**CHARTE DU SYSTEME D'INFORMATION**		*SI/DOC/0001* *Version n°1*
			Date de diffusion : 06/01/2020
Rédaction MERLE J.M. INGENIEUR 19/12/2019 TANCHE P. DIRECTEUR ADJOINT 20/12/2019	**Validation** GUAY C. DIRECTEUR 31/12/2019	**Approbation** BARBATO C. DSQGR 06/01/2020	**Date de revue :** 03/07/2023

Table des matières

1. Objet de la Charte 4
2. Champ d'application 5
3. Cadre règlementaire 6
4. Acteurs et responsabilités 7
5. Propriété des données et des ressources informatiques 8
6. Critères fondamentaux de sécurité 9
6.1. Principes 9
6.2. Une mission sécurité 9
6.3. Un enjeu technique et organisationnel 9
6.4. Une gestion des risques 9
7. Règles d'usage du système d'information 11
7.1 Usage général 11
7.2 Etre un utilisateur responsable 11
7.3 Ne pas mettre en difficulté l'établissement 11
7.4 Confidentialité de l'information et obligation de discrétion 12
7.5 Protection de l'information 12
7.6 Usage des ressources informatiques 13
7.7 Utilisation d'équipement personnel 13
7.8 Usage des outils de communication 13
7.9 Usage des login et des mots de passe (ou de cartes CPS ou équivalents) 15
7.10 Image de l'établissement 16
8. Protection des données personnelles 17
9. Surveillance du système d'information 18

9.1 Surveillance de la messagerie 18
9.2 Surveillance de l'Internet 18
9.3 Gestion et usage de la téléphonie 18
9.4 Contrôle 18
9.5 Traçabilité 19
10. Alertes 19
11. Responsabilités et sanctions 20
12. Modifications 20
13. Entrée en vigueur 20

Date	Version	Auteur	Evolution du document
2016	1.0	J COMBET, JM MERLE	creation
September 2019	2.0	P.TANCHE, JM MERLE	modification, integration RGPD

1. OBJET DE LA CHARTE

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du centre hospitalier d'Ardèche nord et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

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

Cette Charte a été validée par la Direction générale de l'établissement. Préalablement, elle a été notifiée à sa mise en œuvre au Comité d'Etablissement et à la Commission médicale d'Etablissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance de la présente charte.

La Charte est mise à leur disposition sur l'Intranet.

« L'informatique doit être au service de

chacun. Elle ne doit pas porter atteinte à la

vie privée,

Ni aux libertés individuelles et publiques. »

Article 1 de la loi du 06/01/1978

2. CHAMP D'APPLICATION

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du Centre hospitalier d'Ardèche Nord ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau;
- Ordinateurs mobiles;
- Terminaux ;
- Terminaux mobiles;
- Imprimantes simples ou multifonctions;
- Serveurs
- Equipements réseaux locaux et étendus
- Applications et données associées
- Logiciels et infrastructures informatiques associés aux dispositifs médicaux (DM) et dispositifs médicaux de diagnostic in vitro (DMDIV)

Cette Charte s'applique à l'ensemble du personnel de l'établissement de santé, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (stagiaires, internes, doctorants, prestataires, fournisseurs, sous-traitants, …) utilisant les moyens informatiques de l'établissement ainsi que les personnes ayant accès au système d'information à distance directement ou à partir du réseau administré par l'établissement.

Chaque utilisateur, en tant qu'usager des ressources informatiques, s'engage à connaître et à appliquer l'ensemble des dispositions de la présente charte.

L'établissement s'engage, pour sa part, à mettre en œuvre la meilleure politique de sécurité possible, afin de garantir les exigences de sécurité liées à son activité. Ceci pour préserver les ressources informatiques mises à la disposition des utilisateurs.

Cette charte concerne la totalité des utilisateurs. A ce titre, elle doit être communiquée à tout utilisateur, interne ou externe (chartes prestataires) à L'établissement.

Les contrats entre L'établissement et tout tiers (personne morale) donnant accès aux ressources informatiques de l'établissement devront stipuler que les utilisateurs s'engagent à respecter la présente charte. Les responsables des utilisateurs extérieurs s'engagent à faire respecter la présente charte par leurs propres salariés et éventuel établissement sous-traitant.

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

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

3. CADRE REGLEMENTAIRE

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

- Le traitement numérique des données, et plus précisément:
  - Le traitement de données à caractère personnel et le respect de la vie privée ;
  - Le traitement de données personnelles de santé : Les données relatives à la santé sont considérées par la loi Informatique et Libertés (article 8) comme des données sensibles;

- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données médicales ;
- Le secret professionnel et le secret médical;

- La protection des données personnelles :
  - Les utilisateurs du système d'information de l'établissement de santé sont soumis à plusieurs obligations en ce qui concerne les modalités de mise en œuvre du traitement des données à caractère personnel. De façon générale, les utilisateurs doivent respecter les principes de protection des données de santé et des données à caractère personnel (finalité, pertinence et proportionnalité, conservation limitée, sécurité et confidentialité et respect des droits des personnes).

- La signature électronique des documents;
  - Conformément au Référentiel Général de Sécurité (RGS).

- Le secret des correspondances :
  - Les utilisateurs doivent s'abstenir de toute tentative d'intercepter les communications privées, qu'il s'agisse de courrier électronique ou de dialogue direct.
  - De lourdes sanctions pénales (un an d'emprisonnement et 45 000 € d'amende) frappent celui qui porte atteinte au secret de la correspondance.

- La lutte contre la cybercriminalité;

- La fraude informatique ;
  - L'utilisateur s'engage à ne pas effectuer des opérations pouvant nuire au bon fonctionnement du réseau informatique, à l'intégrité de l'outil informatique et aux relations internes et externes de L'établissement.
  - La simple accession à un système d'information sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système.

- Les actes consistant à empêcher un système de fonctionner par exemple par l'introduction de « virus » ainsi que l'introduction ou la modification frauduleuse de données sont visés et sanctionnés par le nouveau code pénal.
- Les sanctions peuvent aller jusqu'à 3 ans d'emprisonnement et 45 000 € d'amende.

- La protection des logiciels et des bases de données et le droit d'auteur :
  - La législation interdit à tout utilisateur de faire des copies de logiciels pour quelque usage que ce soit. Les copies de sauvegarde sont les seules exceptions à la règle. La copie d'un logiciel constitue en effet le délit de contrefaçon sanctionné pénalement. L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux répressifs et civils, la personne morale qui l'emploie peut également être poursuivie.

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

4. ACTEURS ET RESPONSABILITES

Les responsabilités des différents acteurs, sont en particulier :

- Le responsable informatique fait office de Responsable Sécurité. Il est le contact privilégié sur les aspects de sécurité des systèmes d'information de L'établissement.

- Le Comité de Direction est habilité à demander des mesures de surveillance dans le respect des recommandations de la CNIL;

- L'équipe informatique gère ces moyens de surveillance et manipule les informations recueillies en toute confidentialité;

- Le contrôle et la vérification de la conformité des mesures de sécurité sont placés sous la responsabilité de la Direction Générale ;

- L'utilisateur final fera remonter les incidents ou phénomènes anormaux qu'il constate auprès du responsable de la sécurité des systèmes d'information qui aura reçu des consignes particulières.

5. PROPRIETE DES DONNEES ET DES RESSOURCES INFORMATIQUES

Toutes les données et ressources informatiques mises à la disposition de l'utilisateur sont la propriété intégrale et exclusive de L'établissement.

Tous les fichiers/répertoires/courriers électroniques utilisateurs, hors ceux marqués « privé » ou « personnel » et conformément aux règles telles qu'indiquées à l'article 7.1 de la présente charte, appartiennent à L'établissement. Les données dites « privées » ou « personnel » sont du domaine de la vie privée de chacun.

Les utilisateurs s'engagent à ne divulguer à des tiers non autorisés, ni transmettre, directement ou indirectement, d'une façon délibérée ou non, et sous quelque forme que ce soit, tout ou partie des informations appartenant à L'établissement mises à sa disposition.

Il en est de même pour toutes les données dont les prestataires pourraient avoir connaissance à l'occasion de l'exécution de leur contrat.

6. CRITERES FONDAMENTAUX DE SECURITE

6.1. PRINCIPES

L'établissement de santé héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques, …), et sur les personnels (paie, gestion du temps, évaluations, accès à Internet et à la messagerie, …).

L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone,...

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

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

6.2. UNE MISSION SECURITE

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

6.3. UN ENJEU TECHNIQUE ET ORGANISATIONNEL

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

Pour cela, le service informatique déploie un ensemble de dispositifs techniques mais aussi organisationnels en accord avec les besoins en sécurité définis par les métiers. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle

pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information. A contrario une personne sensibilisée à la sécurité de l'information peut être la première ligne de défense (respect de la charte).

6.4. UNE GESTION DES RISQUES

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

7. REGLES D'USAGE DU SYSTEME D'INFORMATION

L'accès au système d'information de l'établissement est soumis à autorisation. Une demande préalable informatique est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la demande exprimée par l'utilisateur est transmise par son cadre (ou la direction des ressources humaines), qui précise les accès nécessaires à son agent en remplissant un formulaire à destination du service informatique sur l'intranet.

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

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

Lorsqu'ils utilisent les ressources informatiques ou qu'ils y accèdent, les utilisateurs doivent respecter les dispositions suivantes :

7.1 USAGE GENERAL

Les ressources informatiques sont la propriété de L'établissement et doivent uniquement être utilisées pour répondre à des besoins professionnels légitimes. Les utilisateurs sont responsables de l'usage qu'ils font des ressources informatiques de L'établissement dans l'exercice de leurs fonctions et sont autorisés à avoir accès aux ressources informatiques pour les aider à s'acquitter de leurs tâches. Ils doivent donc réserver l'usage de ces ressources exclusivement au cadre de leurs activités professionnelles. Un usage personnel des moyens de communication est toutefois exceptionnellement admis dans la mesure où il reste modéré et n'affecte pas de manière significative les performances ou la sécurité du système d'information ou s'il est justifié par l'urgence.

7.2 ETRE UN UTILISATEUR RESPONSABLE

Dans le cadre d'un usage loyal et responsable, l'utilisateur doit respecter les autres acteurs et ne pas transgresser la loi. Attentif aux ressources auxquelles il a accès, qui sont la propriété de L'établissement, il a la charge de la sécurité à son niveau et applique les consignes de sécurité définies par les instances de L'établissement.

L'utilisateur doit s'abstenir de modifier les paramètres des systèmes, en lieu et place des personnes autorisées, d'adjoindre ou d'utiliser des dispositifs logiciels ou matériels sans accord préalable de la Direction informatique (modems, web mail, Peer-to-Peer, « chat », jeux, clé USB personnelle etc.…).
Les anomalies de fonctionnement et les problèmes inexpliqués seront signalés au service informatique.
Il incombe à tout utilisateur propriétaire d'une information de la protéger en fonction de sa sensibilité. Un propriétaire d'information peut être le créateur de cette information et/ou la personne consciente des risques liés à celle-ci en fonction d'un contexte donné à un instant donné. Dans ce cas une demande de protection (contrôle d'accès, chiffrement…) sera faite auprès du service informatique.

7.3 NE PAS METTRE EN DIFFICULTE L'ETABLISSEMENT

L'utilisateur doit se garder de toute expression pouvant être pénalement sanctionnée ou de prise de position non habilitée engageant l'établissement. Il ne doit pas se faire le relais de rumeurs ou d'informations mal fondées. Il ne doit pas utiliser son adresse mail professionnelle à des fins privées et réciproquement.

7.4 CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION

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

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, quelque en soit le moyen (messagerie, cloud, papier…), des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

7.5 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est recommandé de ne stocker aucune donnée ni aucun document sensible non protégés sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux dans des salles protégées. De même, les documents

bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement.

Le stockage de données privées sur des disques réseau est interdit.

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

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail ou lieu de résidence (hôtel, habitation…).

Les médias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données ou de support. Leur usage doit être fait avec une très grande vigilance. L'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement.

7.6 USAGE DES RESSOURCES INFORMATIQUES

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

L'utilisateur s'engage à ne pas modifier la configuration des ressources (applications, matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes autorisés et compétentes de l'établissement (ou par son intermédiaire la société avec laquelle il a contracté).

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

7.7 UTILISATION D'EQUIPEMENT PERSONNEL.

L'utilisation d'équipements personnels (BYOD : Bring Your Own Device) dans le cadre professionnel n'est pas autorisée, sauf exception et sous contrôle du service informatique.
Dans ce cas aucune donnée sensible ne sera stockée ni échangée non chiffrée.
En ce qui concerne les données de l'établissement, l'utilisateur est responsable de l'application de la politique de sécurité en vigueur.
En ce qui concerne les données personnelles, l'établissement est responsable de leur sécurité, conformément aux recommandations de la CNIL.

7.8 USAGE DES OUTILS DE COMMUNICATION

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

USAGE DU TELEPHONE ET DU FAX

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

Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l'identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou professionnels.

La communication d'informations médicales (exemples : résultats d'examens, …) aux patients et aux professionnels extérieurs est strictement réglementée. Les utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'établissement en vigueur.

USAGE D'INTERNET

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

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

Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur, …) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.

USAGE DE LA MESSAGERIE

L'usage de la messagerie est autorisé à l'ensemble du personnel. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement. Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre l'hôpital et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

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

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

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou de porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.

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

l'information de bout en bout, les informations médicales doivent être rendues anonymes.

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

TELECHARGEMENT SUR L'INTERNET

Les utilisateurs ne doivent pas télécharger des exécutables (fichier.exe) sans accord du service informatique et les installer sur les systèmes, et à plus forte raison, se livrer à différentes « expériences » (risques de virus, failles de sécurité…).
Les utilisateurs doivent également planifier le téléchargement de fichiers de taille importante, durant les heures de faible activité (avant 8h00 et après 17h00 du lundi au vendredi), en particulier à partir de sites distants pour éviter la saturation des moyens de communication.
Tout téléchargement de fichier concernera des activités strictement professionnelles, répondant aux missions confiées par l'établissement à l'utilisateur.

GROUPES DE DISCUSSION ET RESEAUX SOCIAUX SUR INTERNET.

Ce sont des tribunes publiques où il est interdit de révéler les informations confidentielles de l'établissement.

Seuls les utilisateurs qui ont été dûment autorisés par leur hiérarchie sont habilités à parler / écrire au nom de L'établissement pour communiquer sur des sujets de discussion bien précis. Par conséquent, ces personnes doivent faire tout ce qui est en leur pouvoir pour être professionnels dans les commentaires qu'ils font en ligne.

En ce qui concerne les réseaux sociaux (type Viadeo, Facebook…), l'utilisateur ne doit pas faire référence à son employeur actuel sur des sujets professionnels sensibles et doit éviter de donner des informations privées pouvant être utilisées comme mots de passe dans les systèmes de L'établissement (nom de jeune fille de la mère…). Ce type d'information est utilisé par les pirates pour s'introduire dans les systèmes.

7.9 USAGE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENTS)

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

Pour utiliser ce compte nominatif, l'utilisateur soit dispose d'un login et d'un mot de passe, ou utilise une carte CPS ou équivalent (avec un code personnel à 4 chiffres). Le mot de passe choisi doit être robuste (**8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé régulièrement**. Le mot de passe est strictement confidentiel et personnel (sauf exception pour des raisons d'organisation des services et avec les mesures de sécurité adaptées). Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en

charge de la sécurité des systèmes d'information, même pour une situation temporaire.

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

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

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

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

7.10 IMAGE DE L'ETABLISSEMENT

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de 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 leurs accès à Internet.

8. PROTECTION DES DONNEES PERSONNELLES

Les utilisateurs du système d'information de l'établissement de santé sont soumis à plusieurs obligations en ce qui concerne les modalités de mise en œuvre du traitement des données à caractère personnel. De façon générale, les utilisateurs doivent respecter les principes de protection des données de santé et des données à caractère personnel (finalité, pertinence et proportionnalité, conservation limitée, sécurité et confidentialité et respect des droits des personnes).
L'établissement doit par ailleurs se conformer aux procédures liées à l'entrée en vigueur du règlement général de la protection des données (RGPD), et notamment :

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

Dans ce cadre, les utilisateurs doivent notamment :

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

9. SURVEILLANCE DU SYSTEME D'INFORMATION

Il est rappelé que toute information circulant et/ou stockée sur les systèmes informatiques de L'établissement est considérée comme ayant un caractère professionnel et est toujours censée être mise à la disposition de L'établissement par l'utilisateur. De ce fait, L'établissement se réserve le droit d'examiner, à tout moment, les données informatiques, le courrier électronique (hors du domaine privé) et l'utilisation d'Internet des utilisateurs.

9.1 SURVEILLANCE DE LA MESSAGERIE

Afin de respecter la liberté individuelle et la vie privée de chacun, l'utilisateur qui souhaite faire usage de la faculté d'utiliser, à titre exceptionnel, la messagerie électronique à des fins privées est tenu d'indiquer clairement, dans l'objet du message, que celui-ci a un caractère privé ou personnel:

L'établissement considèrera donc comme personnel et non professionnel le seul courrier électronique indiquant « privé » ou « personnel » dans l'objet du message ou stocké dans un dossier de la messagerie intitulé « privé » ou « personnel ».
Le même principe est applicable aux répertoires et fichiers « privé » ou « personnel » dans l'Explorateur Windows ou tout autre type de stockage de données.

9.2 SURVEILLANCE DE L'INTERNET

L'établissement se réserve également le droit d'examiner l'activité sur Internet et d'analyser les habitudes d'utilisation, de façon non nominative et à des fins statistiques (dans le respect des recommandations de la CNIL), pour veiller à ce que les ressources informatiques soient utilisées conformément aux dispositions de cette charte.

L'établissement dispose, en effet, de logiciels et de systèmes qui sont en mesure de surveiller et d'enregistrer toutes les utilisations d'Internet. Pour chaque utilisateur, ces mesures de sécurité sont susceptibles d'enregistrer chaque site Web visité, ou message de courrier électronique hors webmail, ainsi que chaque transfert de fichier vers et depuis les réseaux de L'établissement.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

9.3 GESTION ET USAGE DE LA TELEPHONIE

Les contrôles ont pour objet de s'assurer du caractère non abusif de l'usage privé du téléphone mis à disposition par l'établissement dans le cadre de l'activité professionnelle.
Les relevés de facturations détaillés ne font pas apparaître les quatre derniers chiffres des numéros appelés.
D'autre part, l'établissement s'interdit tout enregistrement de conversation téléphonique à l'insu des utilisateurs.

9.4 CONTROLE

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

Le contrôle de ces informations ne peut être réalisé que par l'équipe informatique (tenue au secret professionnel), conformément et dans le cadre de leur définition de fonction. Ces informations ne seront utilisées qu'à des fins statistiques et à la demande de la direction de l'établissement.

Modalité d'accès aux données utilisateur en son absence par sa hiérarchie : seules les données professionnelles peuvent être accédées par nécessité de la poursuite de l'activité de l'établissement. L'utilisateur en sera informé systématiquement dès son retour.

9.5 TRAÇABILITE

Le service informatique assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

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

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il a accédé ;
- Le type d'opération réalisée
- La durée de la connexion (notamment pour l'accès Internet) ;

Le personnel de la Direction du système d'information respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs ou dysfonctionnements.

10. ALERTES

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

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains.
Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle des personnels soient respectées.

11. RESPONSABILITES ET SANCTIONS

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

L'établissement ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrites dans la Charte.

En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions prévues dans les textes selon la gravité du manquement. (Rappel, avertissement, retrait des moyens informatiques, licenciement et éventuellement des actions civiles ou pénales)

- Pour les agents titulaires, l'échelle des sanctions est prévue dans la : loi n° 86-33 du 9 janvier 1986 - article 81 ;
- Pour les agents stagiaires, les sanctions sont prévues dans le décret n°97-487 du 12 mai 1997 ; article 16,
- Pour les non titulaires, les sanctions sont prévues : décret N°91-155 du 6 février 1991, article 39.

Outre ces sanctions, la Direction du Centre hospitalier d'Ardèche nord est tenu de signaler toutes infractions pénales commises par son personnel au procureur de la République.

12. MODIFICATIONS

Cette charte pourra faire l'objet de modifications par L'établissement après acceptation de la Direction et des Partenaires Sociaux.

La charte modifiée ou des avenants seront accessibles aux utilisateurs sur l'Intranet.

13. ENTREE EN VIGUEUR

La présente charte a été soumise pour avis au comité d'établissement et intégrée au règlement intérieur suite à sa modification le 26/09/2019

M. Guay Cyril, Directeur de l'établissement de santé

M. Jean-Michel Merle, Responsable de la sécurité du système d'information de l'établissement de santé