Hôpital Cimiez
4, Avenue Reine VICTORIA – CS 91 179
06003 NICE Cedex 1

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

PORM-DSI-CH-017 **VERSION 001**

Mots clés

Rédaction	
Patricia MATTEUCCI (DINSI Délégué à la Protection des Données (DPO))	25/10/2023

Vérification	
Xavier STOPPINI (DINSI Responsable sécurité des systèmes d'information (RSSI))	27/10/2023

Approbation	
Helene LHERBETTE (DINSI Direction)	28/11/2023

Diffusion	
Emetteur :	**Destinataires du document :**
Patricia MATTEUCCI	DINSI Xavier STOPPINI, Helene LHERBETTE, Loriane BAZIRE-DUHEM

Date d'application
28/11/2023

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

Table des matières

PREAMBULE 4
I / DEFINITION ET CHAMP D'APPLICATION DE LA CHARTE 4
1.1 – Cadre réglementaire 4
1.2 - A quoi s'applique la charte 5
1.3 - A qui s'applique la charte 5
II. MODALITES D'ACCES ET D'AFFECTATION DES RESSOURCES DU SI 5
2.1 – Principes 5
2.2 – Octroi des accès 6
2.3 – Conditions d'accès 6
2.4 – Restriction et suppression des accès 7
III. REGLES ET PRINCIPES GENERAUX D'UTILISATION DES RESSOURCES 8
3.1 - Utilisation des ressources informatiques 8
3.2 - Utilisation des outils de communication 9
3.3 – Présomption du caractère professionnel 11
3.4 – Utilisation des ressources professionnelles à des fins privées 12
3.5 – Obligation de sécurité et de confidentialité 13
3.6 – Responsabilité des Utilisateurs 14
3.7 – Respect des droits de propriété intellectuelle 15
3.8 – Recours à des ressources personnelles à des fins professionnelles 15
3.9 – Droit à la déconnexion 15
3.10 – Connexion à distance et nomadisme 15
3.11 – Modalités de connexion au service Wifi Public avec un équipement non délivré par la CHUN 16
IV. REGLES SPECIFIQUES 16
4.1 – Sécurité des échanges de données 16
4.2 – Continuité d'activité (absence, départ, …) 16

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

4.3 – Protection des accès physiques aux sites et locaux 17
4.4 – Protection des données personnelles 17
4.5 – Télétravail 18
V. REGLES RELATIVES A L'ADMINISTRATION DES RESSOURCES SI 18
5.1 – Responsabilité des Administrateurs 18
5.2 – Surveillance et supervision des ressources 18
VI. APPLICATION DE LA CHARTE 19
VII – ENGAGEMENT DE CONFIDENTIALITE DE L'UTILISATEUR 20

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

PREAMBULE

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 Universitaire de Nice et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement et au règlement général de la protection des données (RGPD) en vigueur depuis mai 2018.

En effet, le CHU de Nice (CHUN) met à la disposition de ses utilisateurs des équipements informatiques (serveurs, PC, logiciels…), des moyens de communication (réseau inter-sites, liaisons avec des sites distants, messagerie, …), ainsi que des données et informations qui sont nécessaires à l'accomplissement de leurs missions.
Chaque utilisateur doit être conscient que l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi, de la sécurité du CHUN et du bon usage.

I / DEFINITION ET CHAMP D'APPLICATION DE LA CHARTE

1.1 – Cadre réglementaire

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

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

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

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

1.2 - A quoi s'applique la charte

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

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau ;
- Ordinateurs portables ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- Toutes les applications utilisées sur le système d'information du CHUN

1.3 - A qui s'applique la charte

Cette Charte s'applique à l'ensemble des professionnels de l'établissement de santé rémunérés par le CHUN, tous statuts confondus (titulaire, contractuel, intérimaire, stagiaire, étudiant…) utilisant les moyens informatiques de l'établissement, d'accéder au système d'information à distance, directement ou à partir du réseau administré par l'établissement.

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

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

II. MODALITES D'ACCES ET D'AFFECTATION DES RESSOURCES DU SI

2.1 – 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, gestion des carrières, 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 :

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

- 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 et immunisée contre les règles extra-européennes ;
- Sa traçabilité : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

2.2 – Octroi des accès

L'accès au poste de travail et à la messagerie est générée de manière automatique par la DRH lors de la création du dossier agent dans le logiciel de gestion des RH.
Les demandes pour les accès aux applications « métier » sont adressées par ticket GLPI par le cadre qui précisera le périmètre des accès nécessaires.
Le service informatique attribue alors au demandeur son droit d'accès.
Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cessation, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente Charte par l'utilisateur.
Ainsi, le compte et l'adresse électronique nominative du salarié seront désactivés de manière automatique au départ de l'agent.
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.

Ces octrois doivent respecter les principes suivants :
- Principe d'identification des Utilisateurs et d'autorisation préalable par la DINSI de tout accès aux ressources IT
- Principe de la proportionnalité des accès et des ressources par rapport au besoin métier de l'Utilisateur
- Principe de séparation des fonctions
- Principe de contrôle/revue régulier des droits et accès en place

Ces règles s'appliquent à toutes les applications du SIH y compris le dossier patient informatisé et notamment pour les accès aux données issues de consultations ou d'hospitalisations.

2.3 – Conditions d'accès

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

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

Pour utiliser ce compte nominatif, l'utilisateur, soit dispose d'un login et d'un mot de passe, soit utilise une carte CPS ou équivalent (avec un code personnel à 4 chiffres).
Le mot de passe initial pour l'ouverture de la session utilisateur est constitué de la manière suivante : Les deux premières lettres du prénom en Majuscule + les deux premières lettres du nom + le jour + le mois de naissance + 4 derniers chiffres du matricule RH+ « ! »

Exemple : JUve1511XXXX!

Le mot de passe sera modifié par l'utilisateur dès la première connexion.
Le mot de passe choisi doit être robuste (pour rappel les recommandations de la CNIL sont les suivantes : 8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner.
Conformément à la Politique de Sécurité du Système d'information, ce mot de passe devra respecter les règles minimales de complexité, à savoir :

- Ne pas comporter une partie de votre nom ou prénom
- Être renouvelé tous les 3 mois
- Avoir une longueur d'au moins 8 caractères
- Comporter au moins 3 types de caractères : minuscules, majuscules, chiffres, symboles : (& »'§)^¨%:/ ;., !?)
- Impossibilité d'utiliser deux fois le même mot de passe

Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.
Chaque utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médicales et 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. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir.

2.4 – Restriction et suppression des accès

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.

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

Il est interdit d'accéder ou de chercher à accéder à une ressource après retrait des accès ou départ de l'utilisateur.

La fermeture du compte utilisateur est générée automatiquement par la fin de contrat de l'agent.

III. REGLES ET PRINCIPES GENERAUX D'UTILISATION DES RESSOURCES

3.1 - Utilisation des ressources informatiques

- **Le poste de travail**

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.

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

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

L'utilisateur ne doit pas :

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

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

- **Les équipements mobiles de stockage**

L'utilisation de périphériques amovibles type clés USB ou disques externes est fortement déconseillée et doit faire l'objet d'un scan par l'antivirus à chaque utilisation par le collaborateur et être crypté.

3.2 - Utilisation des outils de communication

- **Messagerie électronique**

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.
L'accès au compte de l'utilisateur et à l'adresse électronique nominative du personnel seront désactivés de manière automatique 5 jours après la date de départ de l'agent.

Concernant la durée de conservation des courriels deux cas de figure se présentent :

- Pour les messages professionnels, l'employeur peut extraire les courriels professionnels et conserve les données des boites électroniques pendant 5 ans en archivage, après le départ de l'agent.
- Pour les messages personnels, l'établissement veillera à les supprimer. Le salarié devra les récupérer s'il le souhaite.

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

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

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

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

Les envois groupés de mails en masse sont réservés aux seuls services habilités.

L'utilisateur devra être particulièrement vigilant à ne pas cliquer sur des pièces jointes ou liens URL dans les emails douteux.

Il devra être vigilant à tout contact :

- De personnes qu'il ne connait pas, surtout si elles vous invitent à cliquer sur des liens ou à ouvrir un fichier ;
- D'une personne connue envoyant une communication inhabituelle *;*
- De personnes cherchant à créer un sentiment d'urgence ou de danger.

En cas de doute, vous pouvez demander de l'aide directement à la DINSI par mail à .DINSI.Signalements Attaques CHU Nice *<signalements-attaques@chu-nice.fr>.*

- **Accès, navigation et utilisation 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, la traçabilité est conservée et leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et de ne pas mettre en danger l'image ou les intérêts de l'établissement de santé.
Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur…) peuvent être enregistrées par des tiers, analysées et utilisées à des fins, notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle ni aucune coordonnée professionnelle, sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.
Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.
Tous les accès Internet sont tracés, enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.
Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment les

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

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.

Le téléchargement de contenu illicite depuis Internet est formellement interdit.

- **Téléphone et fax**

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.
Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l'identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou de professionnels.

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

- **Espaces de discussion en ligne**

L'utilisateur doit faire respecter les règles de discrétion, loyauté, confidentialité et sécurité y compris sur les réseaux sociaux.

3.3 – Présomption du caractère professionnel

- **Utilisation des ressources à des fins professionnelles**

Tout utilisateur s'engage à n'utiliser les moyens informatiques mis à sa disposition que dans le cadre exclusif de son activité au CHUN et donc à titre professionnel.
Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente un intérêt au regard des fonctions exercées ou des missions à mener.

- **Autorisation de la DINSI d'en contrôler l'utilisation à ce titre**

En vue d'assurer le bon fonctionnement, la sécurité et la qualité de service des systèmes informatiques, le CHUN met en place des administrateurs du système, qui ont accès aux informations relatives aux utilisateurs (fichiers, courriers électroniques, connexions à Internet…), y compris celles qui sont enregistrées sur le disque dur du poste de travail. Ces personnes sont tenues au secret professionnel.

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

Le CHUN dispose :

- d'outils de contrôle de stockage et d'archivage des données et messages ;
- d'un système de journalisation des connexions, destiné à identifier et enregistrer toutes les connexions ou tentatives de connexion, avec conservation des données ne pouvant excéder un an à l'exception des logs concernant les logiciels métiers (RH, comptabilité, messagerie) pour lesquels la durée de conservation est de 5 ans maximum ;
- d'une traçabilité des actions (consultation, création, modification, suppression) dans les applications métiers mises en œuvre ;
- de la possibilité de prise de contrôle à distance des postes de travail pour des dépannages et installations.

Le CHUN utilise différents moyens techniques (consultation de la mémoire cache, contrôle des flux, installation de limites d'accès au serveur proxy, utilisation de pares-feux) pour procéder à des contrôles d'utilisation, conformes à la présente Charte, des ressources informatiques mises à disposition.

Le CHUN se réserve le droit d'utiliser des logiciels de filtrage afin d'interdire l'accès à certains sites Internet dont le contenu lui semble illicite ou en contradiction avec les objectifs de la présente charte ainsi que tout outil de prise en main à distance autre que ceux autorisés par le CHUN.
Le CHUN ne garantit pas que ce filtrage sera totalement efficace, ni exempt de toute interruption, faille ou erreur.

L'utilisateur accepte que le CHUN puisse :

- avoir connaissance des informations nécessaires à l'administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper la perturbation du service ;
- contrôler a posteriori l'utilisation de sa messagerie en analysant des indications générales de fréquence, de volume, de taille des messages, de format des pièces jointes, sans qu'il y ait aucun contrôle sur le contenu des messages échangés.
- contrôler a posteriori les données de connexion à Internet par service et par utilisateur ainsi que les sites les plus visités.

Sur demande du Directeur Général, du RSSI ou sur requête judiciaire, le CHUN peut procéder à des contrôles individuels de bonne utilisation de la Messagerie et d'Internet.

3.4 – Utilisation des ressources professionnelles à des fins privées

Une utilisation des ressources professionnelles à des fins privées n'est par principe pas autorisée.
Une consultation ponctuelle et dans des limites raisonnables du web, pour un motif personnel, des

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

sites Internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne met pas en cause l'intérêt et la réputation du CHUN est tolérée. La plupart des sites gardent une trace des passages et notamment de l'identifiant du visiteur, qui apparaît sous le nom du CHUN.

Un usage raisonnable de la messagerie, dans le cadre des nécessités de la vie courante et familiale, est toléré, à condition que cela n'affecte pas le trafic normal des messages professionnels. L'envoi en masse, tout comme le fait de faire suivre vers d'autres utilisateurs des messages à caractère non professionnel sont interdits.
L'utilisateur doit différencier ses emails personnels par une qualification privée ou personnelle dans l'objet et/ou le classement dans un répertoire spécifique dédié au contenu privé distinguable par son nom. Sinon tous les messages ne respectant pas ces conditions sont présumés être à caractère professionnel.
Les mêmes principes sont appliqués pour distinguer les fichiers professionnels et privés.
Si le salarié souhaite conserver ces messages, il lui appartient d'en prendre copie.

Le CHUN ne peut prendre connaissance des messages ou des fichiers « personnels » d'un utilisateur que dans le cadre d'une instruction pénale ou par une décision de justice.

3.5 – Obligation de sécurité et de confidentialité

Les personnels de l'établissement sont soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels doivent faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.
L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux qui sont publics ou partagés.
Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électronique dont l'utilisateur n'est ni directement destinataire, ni en copie.
L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.

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

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

Il est formellement interdit d'utiliser des logiciels espions, de désactiver les paramétrages de sécurité (antivirus…)

Tout constat de vol de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou, de façon plus générale, toute suspicion d'atteinte à la sécurité ou tout manquement substantiel à cette charte, doit être signalé au RSSI et au DPO à l'adresse mail suivante : dpo@chu-nice.fr.
En cas de perte et/ou de vol, la direction du service informatique activera un outil qui lui permet de localiser le matériel et le rendre inutilisable.

3.6 – Responsabilité des Utilisateurs

Il est interdit de détourner les finalités d'utilisation des ressources.
L'utilisateur s'engage au respect du secret professionnel, à ne pas agir pour nuire et à respecter les données des autres.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques du CHUN mises à sa disposition.
Il est tenu à l'obligation de discrétion professionnelle pour les données et informations auxquelles il a accès dans le cadre de ses activités professionnelles. Le corps médical est tenu au secret médical et à la déontologie médicale.
Il lui appartient de protéger ses données en utilisant des moyens de sauvegarde mis à sa disposition.

L'utilisateur s'engage au respect des lois et règles relatives notamment :
- à la protection de la vie privée : le droit à la vie privée, le droit à l'image et le droit de représentation implique qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans un consentement de la personne intéressée ;
- à l'interdiction de messages de nature diffamatoire, injurieux, discriminatoire, politique, religieux, d'incitation à la violence, à caractère raciste, pornographique, etc…
- à la confidentialité des données personnelles.

Il s'engage à ne pas perturber volontairement le fonctionnement du système d'information du CHUN et notamment :
- à ne pas interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ;
- ne pas introduire des programmes virus ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, ou saturer les ressources ;
- ne pas modifier les configurations des matériels du CHUN ;
- ne pas installer ou désinstaller de logiciels sur ces matériels ;
- ne pas déplacer les matériels ;
- ne pas installer de programme pirate (licence d'utilisation non acquise) ;
- etc…

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

3.7 – Respect des droits de propriété intellectuelle

L'utilisateur s'engage également au respect de la propriété littéraire et artistique :

- ✓ Droit de propriété sur les logiciels créés
- ✓ Respect des droits des tiers (droit d'auteur, brevets …)

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.

L'utilisation de logiciels du commerce est soumise au respect du code de la propriété intellectuelle défini par le législateur.
Chaque collaborateur doit avoir conscience :

- Que l'utilisation de logiciels est soumise à l'acquisition par l'entreprise de licences d'utilisation ;
- Que la loi protège les logiciels contre la copie ;
- Que sa responsabilité civile et pénale sera engagée en cas de copie non autorisée ou de piratage de logiciel ;
- Qu'un logiciel utilisé sans licence, qu'il soit gratuit ou non, est une contrefaçon ou une source d'infection virale, voire d'intrusion par un tiers ;
- Qu'aucune installation de logiciel piraté sur le poste de travail, même pour utilisation à titre personnel, ne sera admise.

3.8 – Recours à des ressources personnelles à des fins professionnelles

Le recours à des ressources personnelles à des fins professionnelles est par défaut interdit sauf autorisation spécifique.

3.9 – Droit à la déconnexion

L'utilisateur est en droit de ne pas être connecté aux outils numériques professionnels (téléphone portable, courriels, etc.) hors des horaires de travail (temps de transport travail-domicile, congés, temps de repos, week-end, soirée, etc.…).

3.10 – Connexion à distance et nomadisme

Dans le cadre de connexions à distance au CHUN, l'utilisateur s'engage à respecter les règles de la

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

sécurité informatique et notamment :

- De se connecter à partir d'un poste informatique fourni par le CHUN, bénéficiant d'un antivirus à jour et des mises à jour des patchs correctifs de sécurité.
- L'utilisateur doit veiller à ce qu'à l'issue de chaque connexion à distance, les données résiduelles (fichiers temporaires ou zones de mémoire vive) en provenance du SIH soient effacées de son poste.

Tout vol ou perte de matériel doit être signalé et déclaré via la création d'un ticket GLPI (cf procédure de vol ou perte).

3.11 – Modalités de connexion au service Wifi Public avec un équipement non délivré par la CHUN

(Instituts de formation des professions paramédicales du CHU de Nice...)
L'utilisation du service Wifi Public du CHUN est gratuit et accessible à partir de la saisie du mot de passe Wifi renouvelé tous les jours.
Dans le cadre de l'utilisation d'équipement personnel sur le réseau Wifi Public, il appartient à l'utilisateur de vérifier qu'il dispose des équipements matériels, logiciels, navigateurs lui permettant d'utiliser le service et il s'engage à avoir un antivirus fonctionnel et à jour.
L'utilisateur respecte toutes les règles de la Nétiquette en s'interdisant notamment tout comportement et tout usage contraire à l'ordre public et aux bonnes mœurs. La présente charte s'applique en totalité.

IV. REGLES SPECIFIQUES

4.1 – Sécurité des échanges de données

Tout envoi et réception de documents avec l'extérieur ne pourra se faire que par la boite mail du CHU et de préférence via MS Santé pour les professionnels de santé.

L'utilisation de googledrive, we transfer, dropbox, GAFAM etc. est interdite.
L'usage d'un container sécurisé est conseillé (container Zed).

4.2 – Continuité d'activité (absence, départ, …)

En cas d'absence ou de départ, les agents dont la fonction le nécessite devront organiser avec leur équipe la passation d'activité et signifier leur absence avec un message automatique d'absence.
Il est formellement interdit d'accéder au poste ou messagerie d'un collègue absent sans son accord.

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

4.3 – Protection des accès physiques aux sites et locaux

Les cartes d'accès sont nominatives, leur port est obligatoire et il est interdit de les prêter.
Il est interdit de donner accès à un local sans vérifier la légitimité de la demande.

Les locaux « sensibles » sont équipés de système de surveillance pour assurer la sécurité des matériels (salle machine, local LTZ..).

4.4 – 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).

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 :

- Désigner un Délégué à la protection des données (DPO/DPD). Un DPO a été nommé pour l'ensemble du GHT06 dont le CHU de Nice est l'établissement support. Ses coordonnées sont les suivantes : dpo@chu-nicefr
- 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 le cas échéant 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 (DPO);

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

- **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 ;
- **S'assurer auprès du RSSI que l'encadrement des mesures techniques et opérationnelles de sécurité des règles obligatoires et recommandées** sont conformes au PAS (Plan d'assurance sécurité) lorsqu'il y a 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 RSSI et du DPO les incidents de sécurité** impliquant des données personnelles.

4.5 – Télétravail

Les utilisateurs concernés par ce dispositif devront prendre connaissance et appliquer rigoureusement la charte du télétravail du CHU de Nice.

Une formation en ligne aux règles de base liées à la sécurité informatique sera obligatoire avant toute mise en place du dispositif de télétravail.

V. REGLES RELATIVES A L'ADMINISTRATION DES RESSOURCES SI

5.1 – Responsabilité des Administrateurs

Il est interdit d'utiliser les données pour d'autres finalités que la supervision du fonctionnement et sécurité des ressources.
Les administrateurs doivent être équipés de matériel sécurisé et ils devront séparer les usages professionnels courants des usages administrateurs.
Il est interdit d'exercer une pression sur un Administrateur.
L'obligation de sécurité et de confidentialité est renforcée pour les administrateurs.

5.2 – Surveillance et supervision des ressources

Une supervision automatisée globale et régulière à des fins de sécurité et de contrôle des connexions et flux réseau, de la messagerie est réalisée par les services de la DINSI et les sociétés extérieures habilitées à la demande du CHU en 24h/24 et 7j/7.
Des analyses et investigations spécifiques peuvent être réalisées en cas de nécessité (menace, incident, …).

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

VI. APPLICATION DE LA CHARTE

- Les règles définies dans la présente Charte ont été fixées dans le respect des dispositions législatives et réglementaires applicables (CNIL, ASIP Santé...).
- L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services Internet décrites dans la Charte.
- En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions pouvant être :
    - Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, de l'accès aux moyens informatiques ;
    - Une sanction disciplinaire pouvant aller jusqu'au licenciement en fonction de la gravité des faits reprochés et de leurs conséquences pour le CHUN
    - Eventuellement, des actions civiles ou pénales, selon la gravité du manquement
    - Outre ces sanctions, la Direction du CHU de Nice est tenue de signaler toute infraction pénale commise par son personnel au procureur de la République.
    - Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou évènement particulier.
- La présente charte pourra être revue à la demande du RSSI et/ou du DPO.

POUR RAPPEL – PREMIERE OUVERTURE DE SESSION

Comme précisé ci-dessus en page 6 de la présente charte, le mot de passe initial pour l'ouverture de la session utilisateur est constitué de la manière suivante : Les deux premières lettres du prénom en Majuscule + les deux premières lettres du nom + le jour + le mois de naissance + 4 derniers chiffres du matricule RH+ « ! »

Exemple :
Jean ROBERT, né le 29/11/1970 matricule 1007662
Le mot de passe sera le suivant : JEro2911766!

Le mot de passe sera modifié par l'utilisateur dès la première connexion.

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION DU CHU DE NICE A DESTINATION DES SALARIES

VII – ENGAGEMENT DE CONFIDENTIALITE DE L'UTILISATEUR

Je soussigné/e
Nom :
Prénom :
~~Numéro de matricule~~ :
Fonction : Etudiant/Elève **~~Téléphone~~ :**

Etant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je déclare avoir pris connaissance de la charte d'accès et d'usage du système d'information du CHU de Nice et m'engage à la respecter.

Je m'engage par conséquent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à……, le …/…../…….

Signature :

POUR RAPPEL – PREMIERE OUVERTURE DE SESSION

Comme précisé ci-dessus en pages 6 et 18 de la présente charte, le mot de passe initial pour l'ouverture de la session utilisateur est constitué de la manière suivante : Les deux premières lettres du prénom en Majuscule + les deux premières lettres du nom + le jour + le mois de naissance + 4 derniers chiffres du matricule RH+ « ! »

Exemple :
Jean ROBERT, né le 29/11/1970 matricule 1007662
Le mot de passe sera le suivant : JEro2911766!

Le mot de passe sera modifié par l'utilisateur dès la première connexion.

Ce document est la propriété du CHU de Nice. Toute utilisation, reproduction, modification est soumise à un accord du propriétaire.