CHU AMIENS PICARDIE	**Charte d'accès et d'usage du système d'information au CHU AMIENS-PICARDIE** Diffusion : Public	CHUFT2426	Version 03
		Date d'application : 02 oct. 2024	

I. Objet et domaine d'application

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du CHU AMIENS-Picardie 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. Elle constitue une annexe au Règlement Intérieur de l'établissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance.
La Charte est mise à leur disposition sur l'Intranet et la GED.

Cadre règlementaire : Cf. CHUFO2053 « SYSTEME d'INFORMATION : Les règles, les lois, les textes ou les règlements en vigueur au CHU AMIENS PICARDIE »

II. Charte :

1. Introduction

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du CHU d'AMIENS Picardie, 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 portables ;
- Terminaux portables ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- Serveurs ;
- Logiciels.

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 et les personnes auxquelles il est possible 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.

2. Cadre règlementaire

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 de santé à caractère personnel ;
- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données de santé ;
- 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 au regard du droit de la propriété intellectuelle.

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.

Cf. CHUFO2053 « SYSTEME d'INFORMATION : Les règles, les lois, les textes ou les règlements en vigueur au CHU AMIENS PICARDIE »

3. Protection de l'information

La protection du patrimoine d'information du CHU AMIENS PICARDIE vise avant tout à assurer **sa disponibilité, son intégrité, sa confidentialité et son auditabilité**. Même si des dispositions organisationnelles et techniques sont prises au niveau de la structure, elles ne constituent qu'un premier niveau de protection. Chaque collaborateur a un rôle individuel essentiel à jouer.

Notamment, chaque utilisateur doit :

- Signaler à sa hiérarchie ou aux contacts désignés tout événement lui paraissant susceptible de compromettre la sécurité du système d'information ;
- Veiller à préserver la confidentialité des informations qui lui sont confiées ;
- Assurer la disponibilité et la pérennité des informations gérées au niveau de son environnement de travail en utilisant les différents moyens de sauvegarde et de duplication mis à sa disposition, si cette charge lui incombe ;
- Assurer la confidentialité des mots de passe ou codes utilisés pour les dispositifs de contrôle d'accès ;
- Assurer la protection des dispositifs qui participent au contrôle d'accès et qui lui sont confiés à titre strictement personnel (carte de la famille CPX, générateur de mot de passe unique, etc.).

Notamment, chaque utilisateur ne doit pas :

- Faire usage d'informations dont il aurait connaissance sans qu'elles ne lui soient destinées, quand bien même celles-ci ne seraient pas explicitement protégées ;
- Transmettre sans autorisation des informations sensibles à l'extérieur de la structure, par le biais de la messagerie, d'outils en mode « cloud » ou de tout autre support (oral, papier…) ;
- Fournir des informations à une entité tierce (sous-traitant, personne extérieure à la structure) sans l'aval de la hiérarchie ;
- Transmettre des informations d'ordre professionnel sur les réseaux sociaux ;
- Perturber volontairement le fonctionnement du système d'information par l'introduction de programmes malveillants ou par tout autre action ;
- Contourner ou chercher à contourner les règles et restrictions d'utilisation des ressources mises à sa disposition par les services informatiques ou équivalents.

4. Usages des ressources informatiques

Le poste de travail

Dans le cadre de sa mission, un utilisateur 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, chaque 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…).

Notamment, chaque utilisateur ne doit pas :

- Utiliser les équipements pour un usage personnel ;
- Faire usage de postes de travail pour lesquels il n'a pas été explicitement autorisé.

Les logiciels et les applications

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

Chaque utilisateur 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 personnelle, ne sera admise.

Les équipements mobiles de stockage

L'usage de périphérique type clés USB ou disques externes doit rester exceptionnel et exclusivement à titre professionnel.

- Seuls les périphériques de stockage fournis par la structure sont autorisés ;
- Tout périphérique de ce type doit faire l'objet d'un scan par l'antivirus à chaque utilisation par le collaborateur ;
- Si ces périphériques contiennent des données sensibles, elles doivent être cryptées avec les logiciels validés par la DSI et les organismes habilités : l'ASIP Santé, l'ANSSI et la CNIL.

5. Usages des outils de communication

Internet

Dans le cadre de sa mission, un accès à Internet peut être fourni aux utilisateurs.

- Afin de répondre aux exigences légales et de permettre les investigations en cas d'incident de sécurité, la structure trace le trafic internet entrant et sortant de son réseau et peut le faire analyser.
- Toute l'activité Internet du collaborateur peut donc être tracée. Ces traces ont cependant pour seule finalité la sécurité du système d'information et le respect des exigences légales. Leur

accès est restreint aux seules personnes chargées de ces sujets. Elles ne sont en aucun cas disponibles aux autres personnels, ni pour quelque autre utilisation.
- La structure se réserve le droit de bloquer certains contenus et sites web.
- Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la consultation n'excède pas une durée raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

La messagerie

De même, l'utilisation de la messagerie est sujette à certaines bonnes pratiques.

Notamment, chaque utilisateur ne doit pas:

- Répondre à une demande d'informations personnelles ou confidentielles (code confidentiel, mot de passe, etc…)
- Transférer automatiquement ou manuellement les mails professionnels vers des messageries privées externes à la structure ;
- Utiliser une adresse de messagerie professionnelle pour s'inscrire à des forums ou flux d'actualité qui ne sont pas liés aux métiers de la structure ;
- Inscrire, à des forums ou flux d'actualité quel qu'ils soient, une adresse de messagerie correspondant à une liste de diffusion professionnelle ;
- Utiliser la messagerie d'un collaborateur sans son consentement ;
- Relayer des messages de type « chaînes de lettre » ou d'alerte quelle qu'en soit la nature. Si un tel message semble important, il doit être soumis à la DSI qui jugera de sa validité avant toute action.

Une vigilance accrue est nécessaire en ce qui concerne le traitement des pièces jointes.

Notamment, l'utilisateur doit :

- Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.
- Être particulièrement suspicieux en ce qui concerne les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers envoyés habituellement par les contacts ;
- Prévenir immédiatement sa hiérarchie ou les personnes désignées en cas de doute ou d'ouverture de pièces jointes piégées.

La téléphonie fixe et mobile

Un téléphone fixe et un smartphone peuvent avoir été fournis dans le cadre de la mission du collaborateur.

Si un outil de gestion de téléphones mobiles est déployé, il est interdit de tenter de le désinstaller ou de le contourner. Cet outil permet, entre autres, de :
- Maintenir à jour le système d'exploitation du téléphone ;
- Maîtriser le mode de verrouillage et la politique de mot de passe ;
- Gérer les applications.

Chaque collaborateur doit être lui-même acteur de la sécurité du terminal mobile. Pour cela, des règles de bonnes pratiques s'imposent à lui.

Notamment, l'utilisateur doit :

- S'assurer de sa discrétion lors de ses conversations téléphoniques ;
- Veiller à ne pas dépasser les forfaits de l'abonnement fourni par la structure ;
- Connecter le smartphone fourni à des ordinateurs de la structure uniquement ;
- Activer le wifi et le Bluetooth uniquement quand cela est nécessaire, et les désactiver ensuite.

Notamment, l'utilisateur ne doit pas:

- Utiliser la téléphonie de la structure pour un usage personnel, sauf dans les limites raisonnables fixées par la structure si elle l'a autorisé explicitement ;
- Installer des applications qui n'ont pas été autorisées ;
- Utiliser des procédures ou installer des applications qui permettent de contourner la sécurité du système d'exploitation du smartphone fourni (déverrouillage du smartphone avec élévation non autorisée des droits) ;
- Partager la connexion Internet personnelle avec les équipements professionnels ;
- Recharger son smartphone en le connectant à une prise USB d'un ordinateur non géré par la structure ou mise à disposition dans un lieu public. La recharge du smartphone doit être effectuée à l'aide du chargeur fourni par la structure ou sur le port USB du propre poste du collaborateur.

Les dispositions mentionnées plus haut concernant les logiciels, la messagerie ainsi qu'internet s'appliquent également aux smartphones.

6. Usage des moyens d'accès

Chaque collaborateur dispose d'un ou plusieurs comptes nominatifs lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ces comptes sont exclusivement personnels.
Pour utiliser chaque compte nominatif, le collaborateur soit dispose d'un identifiant (« login ») et d'un mot de passe, soit utilise une carte CPS ou CPE (avec un code personnel à 4 chiffres).
Chaque collaborateur est responsable de ses comptes et mots de passe (ou du code personnel associé à la carte), de la carte qui lui a été confiée le cas échéant, et de l'usage qui en est fait. Il doit veiller à conserver secrets ses mots de passe et codes personnels, et à protéger sa carte CPS/CPE ou équivalent contre le vol, afin que personne ne puisse se connecter en usurpant son compte.

Notamment, chaque utilisateur doit:

- Fermer ou verrouiller sa session lorsqu'on quitte son poste ;
- Fermer sa session systématiquement avant de quitter les locaux en fin de service ;
- Signaler toute tentative de violation de son compte personnel.

Notamment, chaque utilisateur ne doit pas:

- 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 ;
- Communiquer son mot de passe 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, ni à son entourage ou personne extérieur au CHU, même pour une situation temporaire ;
- Mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de la structure dont il a l'usage ;
- 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 disponibles dans l'intranet, la GED ou le catalogue d'applications.

7. Informatique et libertés

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du Délégué à la Protection des Données (DPO) de l'établissement de santé, à défaut le Responsable de la Sécurité du Système d'Information (RSSI), qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le DPO procède ensuite aux opérations de déclaration et d'information réglementaires.

Il est rappelé que l'absence de déclaration de fichiers comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement. En cas de non-respect des obligations relatives à la loi Informatique et Libertés, le DPO serait informé et pourrait prendre toute mesure temporaire de nature à mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

8. Surveillance du système d'information

Contrôle

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

Traçabilité

La Direction du Système d'Information 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 est accédé ;
- Le type d'opération réalisée
- Les informations ajoutées, modifiées ou supprimée des bases de données en réseau et/ou des applications de l'hôpital ;
- La durée de la connexion (notamment pour l'accès Internet) ;

Le personnel de la Direction du système d'information respecte la confidentialité des données et des traces auxquelles 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.

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, à défaut, à la centrale d'appels de la DSN.

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.

9. Responsabilités 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, ANS ex ASIP Santé, ANSSI, ...).

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 pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, des moyens informatiques ;
- Un licenciement et éventuellement des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction du CHU AMIENS Picardie est tenue de signaler toutes infractions pénales commises par son personnel au procureur de la République.

10. Entrée en vigueur de la charte

Charte validée en CTE le 21 mars 2018.

Date d'entrée en vigueur

La présente charte entre en vigueur dès sa communication.

Elle pourra faire l'objet d'une revue annuelle ainsi que ses annexes.

Il existe également d'autres chartes spécifiques au sein de l'établissement :

- le BYOD
- Le Hotspot Wifi
- la messagerie instantanée
- le télétravail
- le personnel de la DSN
- la clause de confidentialité

Publicité

Les utilisateurs seront informés du contenu de la présente charte, et de ses modifications, via l'Intranet ECHO de l'organisme, la GED et les notes de services.