Centre Hospitalier
PAUL CABANIS

CHARTE UTILISATEURS DU SYSTEME D'INFORMATION DU CENTRE HOSPITALIER PAUL CABANIS

Version 2.0
2018

CYCLE DE VIE DU DOCUMENT

AUTEUR(S)

Fonction	Nom	Date
Responsable Informatique	Arnaud BROCHOT	09/2018

RELECTEURS

Fonction	Nom	Date
Directrice déléguée	Béatrice Cornefert	12/09/2018

VALIDATION

Fonction	Nom	Date
Directrice déléguée	Béatrice Cornefert	

HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
1.0	02/2010	Version initiale	
2.0	09/2018	Version amendée (Règles, Droit)	

Table des matières

1 Objet du document

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 Paul Cabanis et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du Système d'Information (SI).

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 de l'établissement. Préalablement, elle a été notifiée à sa mise en œuvre au directoire et présentée pour information 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.

2 Champ d'application de la Charte

La présente Charte concerne les ressources informatiques, les services Internet et téléphoniques du Centre Hospitalier Paul Cabanis, 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 et ordinateurs portables, tablettes, smartphones ;
- ✓ Imprimantes simples ou multifonctions, Fax ;
- ✓ Support mobile de données (exemples : CD, disquette, clé USB, disque dur, ...)
- ✓ Téléphones fixes, DECTs et téléphones portables ;
- ✓ Serveurs.

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, intérimaires, 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.

3 Définition

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

Utilisateur

Toute personne, quel que soit son statut, ayant accès ou utilisant les ressources informatiques dans le cadre de son emploi, d'une prestation ou d'un stage rémunéré ou non au sein de l'Établissement de Santé.

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 divers (web, messagerie, forum, etc.) ;

Moyens informatiques

Ce sont les moyens matériels (ordinateurs, serveurs, imprimantes, tablettes, smartphones) et logiciels mis à disposition dans le cadre des fonctions occupées.

Système d'information

Ensemble des éléments et règles participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein de l'Établissement et vers ses partenaires externes.

Le système d'information (SI) ne se réduit pas à l'informatique ; il regroupe l'ensemble des moyens humains, techniques et organisationnels visant à assurer le traitement, le stockage et l'échange d'informations nécessaires aux activités de l'établissement.

Donnée à caractère personnel

«Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. » (Article 2 alinéa 2 de la loi informatique et liberté).

Traitement de données à caractère personnel

« Constitue un traitement à caractère personnel toute opération ou tout ensemble

d'opérations portant sur de telles données, que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. » (Article 2 alinéa 3 de la loi informatique et liberté).

Responsable des traitements

Le responsable du traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités (à quoi il va servir) et ses moyens (selon quelles modalités). En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

4 Cadre réglementaire

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 :
  - o Le traitement de données à caractère personnel et le respect de la vie privée;
  - o 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, du plan sécurité de l'établissement.

5 Critères fondamentaux de la sécurité

5.1 Principes

Le Centre Hospitalier Paul Cabanis héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médicotechniques, ...), 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.

5.2 Une mission sécurité

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

5.3 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 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.

5.4 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 des 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.

6 Règles de sécurité

6.1 Article 1 : Accès aux systèmes d'information

L'accès au système d'information de l'établissement est soumis à autorisation. Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la demande est exprimée par le responsable de l'utilisateur, qui précise les accès nécessaires à son agent et la transmet par écrit au service Informatique.

En fonction de la demande, le service informatique et/ou les responsables métiers auront la charge de créer un ou des comptes pour le nouvel utilisateur.

Concernant l'accès au SI de l'établissement par des administrateurs systèmes et/ou logiciel ou par des intervenants extérieurs, la demande doit être faite directement auprès du service informatique. Ce dernier est en charge :

- ✓ de remettre l'intégrité de cette présente charte mais aussi celle destinée aux administrateurs,
- ✓ de leur faire signer l'engagement personnel pour le respect de ces deux chartes,
- ✓ éventuellement, de donner les droits nécessaires pour l'accès au SI. Des comptes nominatifs leur seront ainsi affectés.

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.

6.2 Article 2 : Confidentialité de l'information et obligation de discrétion

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, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.

L'accès aux données de santé à caractère personnel des patients par les professionnels de santé habilités se fait à l'aide d'un identifiant et d'un mot de passe strictement personnels, ou d'une carte CPS ou CPE.

6.3 Article 3 : 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 important de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux implantés 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 (ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'autrui ; 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.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les medias 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. 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.

6.4 Article 4 : Usage des ressources informatiques

Seules des personnes habilitées par le Centre Hospitalier Paul Cabanis (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 (matériels, réseaux, ...) mises à sa disposition, 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).

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.

6.5 Article 5 : Utilisation des matériels et des espaces de stockage

Poste de travail : l'utilisateur s'interdit d'installer des programmes, des matériels ou autres outils informatiques sans l'accord de sa hiérarchie. Le poste professionnel ne peut être utilisé que par le salarié (ou parfois le Service) auquel il a été affecté, pour les finalités professionnelles définies.

Périphériques USB : les périphériques de type clés USB ou disques durs externes doivent être utilisés qu'à des fins professionnelles. Seul le matériel appartenant à l'Etablissement peut être connecté sur le réseau.

Imprimantes : l'utilisateur est responsable du bon usage des imprimantes et responsable des données qu'il imprime. Il doit être attentif à l'imprimante sélectionnée et doit s'assurer de ne pas laisser à la vue de tous les documents sensibles imprimés.

Téléphones : les téléphones sont limités à un usage strictement professionnel.

Toute connexion sans autorisation de périphériques (Téléphone portable, Clé USB, WEBCAM...) ou d'ordinateur personnel est interdite.

Espaces de stockage : l'utilisateur doit, dans la mesure du possible, maîtriser ses espaces de stockage (pas de doublons, organisation efficace et lisible). Il doit veiller à n'y stocker que des données ayant une valeur professionnelle. Une tolérance est acceptée en ce qui concerne les disques durs des ordinateurs, où l'utilisateur peut définir un espace personnel explicite.

Afin de ne pas saturer les espaces de stockage, il convient d'y faire régulièrement le tri et de réévaluer la pertinence des données conservées.

Enfin, il est rappelé que l'ensemble des documents professionnels doit être stockés sur les espaces réseau dédiés, sécurisés et sauvegardés, et non pas sur les disques durs des postes de travail, non sécurisés et non sauvegardés.

Objets connectés de santé et applications smartphones : les objets connectés de santé (Google glass, pilulier numérique, implant intelligent...) et les applications pour Smartphone liée à la santé ne peuvent être testés, utilisés et déployés que sous le contrôle du service informatique et du référent Sécurité du SI. Ces objets et applications pouvant servir d'aide à la décision et embarquer des données de santé patients, il convient de cadrer leur usage.

Utilisation de services Cloud :

L'accès à des services, particulièrement en mode Cloud, non préalablement approuvés par le service informatique (exemple : services de stockage et d'échange de fichiers en ligne de type Dropbox, Google Drive, etc., applications en mode SaaS de type Skype, WhatsApp, messageries diverses, etc.) est strictement interdit.

6.6 Article 6 : Usage du téléphone 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.

6.7 Article 7 : 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.

Conformément aux exigences légales de traçabilité, 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 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.

6.8 Article 8 : 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» ou «PERSONNEL» dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

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.

Toute correspondance contenant des données de santé à caractère personnel doit se faire obligatoirement avec une messagerie sécurisée compatible MS-Santé.

L'espace de confiance défini par le système de messageries sécurisées MS-Santé est le seul système d'échange électronique de données personnelles de santé conforme aux exigences de la loi Informatique et Libertés (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée le 6 août 2004) et du Code de la santé publique (art. L.1110-4 et art. L.1111-8).

6.9 Article 9 : Verrouillage des postes de travail

Qu'il s'agisse d'un poste fixe ou d'un portable, l'utilisateur ne doit pas quitter son poste de travail sans se déconnecter, en laissant des ressources ou services accessibles, même pour une courte durée.

En règle générale, l'utilisateur verrouillera son poste de travail en cas d'absence.

Un mécanisme de verrouillage automatique et/ou de déconnexion automatique sera activé.

6.10 Article 10 : Usage des logins et des mots de passe (ou de cartes CPS ou équivalent)

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, soit utiliser 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 tous les 3 mois. 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 de 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 médicotechniques, 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. 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...

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.

6.11 Article 11 : Propriété intellectuelle

Les clauses énoncées dans les licences des différents logiciels doivent être respectées.

Il est interdit d'effectuer des copies de logiciel pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

6.12 Article 12 : Protection de l'image de l'Etablissement

Le droit à l'image concerne les faits et informations de l'Etablissement dans son fonctionnement quotidien, qui n'ont pas à être rendus publiques. Aucun fichier, quelle que soit sa nature, ne doit être diffusé vers l'extérieur et notamment sur l'Internet, sans motif professionnel autorisé.

L'utilisateur doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, pédophile, négationniste ou portant atteinte d'une quelconque façon à la dignité humaine.

L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs lors de ses échanges électroniques par courrier ou par publication sur des forums professionnels. Il n'émettra pas d'opinions étrangères à son activité professionnelle susceptibles de porter préjudice à l'Etablissement.

6.13 Article 13 : Existence d'une tolérance d'un usage privé

Au sein du rapport de 2004 sur la « Cyber surveillance », la CNIL a invité les entreprises à tolérer l'utilisation d'Internet et de la messagerie à des fins personnelles sur le lieu de travail, tout en précisant que cette utilisation devait être « raisonnable ».

Une utilisation à titre privée est tolérée durant les temps de pause si :

- ✓ Elle ne perturbe pas la bonne exécution du travail de l'utilisateur ;
- ✓ Elle n'impacte pas les performances des systèmes ;
- ✓ Elle est conforme à la réglementation en vigueur et à la présente Charte ;
- ✓ L'utilisateur n'utilise pas les moyens informatiques pour diffuser des informations sans rapport avec l'activité ou à caractère illégal ;
- ✓ L'utilisateur n'implique pas le Centre Hospitalier Paul Cabanis dans cet usage personnel des ressources.

6.14 Article 14 : Dispositions en cas d'absence d'un salarié

Au cas où les procédures dites de « doublonnage » ne soient pas applicables et pour assurer une continuité de l'activité professionnelle, l'employeur peut être amené à accéder à l'espace réseau ou à la messagerie d'un salarié absent.

Afin de ne pas porter atteinte à la vie privée des salariés, l'employeur applique la jurisprudence. Celle-ci considère que : « tout message reçu ou envoyé depuis le poste de travail mis à disposition par l'employeur a par principe un caractère professionnel. Dans ce cas, l'employeur peut le consulter. Toutefois, si un dossier, un document ou un message est clairement identifié comme étant personnel, l'employeur ne doit pas en prendre connaissance. »

6.15 Article 15 : Preuve

L'utilisateur reconnaît et accepte que les registres informatisés, conservés dans le système d'information de l'Etablissement dans des conditions raisonnables de sécurité, soient considérés comme les preuves irréfragables de l'utilisation des moyens informatiques de l'Etablissement et des communications.

7 Informatique et libertés

7.1 Article 16 : Déclaration de fichier comportant des données nominatives

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

L'établissement a désigné M. Jean-Pierre VOISIN comme Délégué à la Protection des Données (DPO) à caractère personnel pour l'établissement. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.

Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel des établissements du GHT dont celui de Paul Cabanis au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le délégué veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPO M. Jean-Pierre VOISIN du Centre Hospitalier Régional d'Orléans ou le référent de l'établissement.

8 Surveillance du système d'information

8.1 Article 17 : 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.

8.2 Article 18 : Traçabilité

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 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'établissement ;
- ✓ La durée de la connexion (notamment pour l'accès Internet) ;

Les personnels du service informatique respectent 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.

8.3 Article 19 : 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 référent de la Sécurité du Système d'Information (rSSI) ou à défaut au Responsable Informatique ou au Service Informatique.

De même tout incident grave de sécurité mentionné à l'article L. 1111-8-2 du code de la santé publique doit être signalé au référent de la Sécurité du Système d'Information (rSSI) ou à défaut au Responsable Informatique ou au Service Informatique afin que cet incident puisse être déclaré sur le portail de signalement des évènements sanitaires indésirables prévu par l'arrêté du 27 février 2017.

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 résidents 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 du Centre Hospitalier Paul Cabanis dans le respect des dispositions législatives et réglementaires applicables (CNIL, ASIP Santé, ...).

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 Centre Hospitalier Paul Cabanis est tenu de signaler toutes infractions pénales commises par son personnel au Procureur de la République.

10 Textes de référence

Code Pénal

- ✓ Article 226-13 : « *La révélation d'une information à caractère secret par une personne dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende.* »

- ✓ Articles 226-13, -15, -16, -17, -21 et -22 modifiés par la loi du 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- ✓ Articles 227-23 et 227-24 modifiés par la loi du 5 mars 2007 relative à la prévention de la délinquance.
- ✓ Articles 323-1, -2, -3 et 323-5 (Loi Godfrain), modifiés par la loi du 21 juin 2004 pour la confiance dans l'économie numérique.
- ✓ Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, modifiée le 6 août 2004.
- ✓ Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
- ✓ Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Code de la Propriété intellectuelle

- ✓ Articles L335-1 à L335-8 modifiés par les lois du 1er Août 2006 relatives au droit d'auteur et aux droits voisins dans la société de l'information, du 28 octobre 2009 relative à la protection de la propriété littéraire et artistique sur Internet, du 29 octobre 2007 de lutte contre la contrefaçon, du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet.
- ✓ Articles L342-1 à L342-5 et L343-1 et L343-2 relatifs à la protection des bases de données.

Code de la Santé Publique

- ✓ Article L 1110.4
- ✓ Article L 1111.7
- ✓ Article L 1111.8

Ces textes encadrent un corpus réglementaire portant sur les thèmes suivants :

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

Journal Officiel

- ✓ Arrêté du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information

Parlement européen

- ✓ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Mme Béatrice CORNEFERT, Directrice déléguée du Centre Hospitalier Paul Cabanis

Monsieur Arnaud BROCHOT, responsable Informatique du Centre Hospitalier Paul Cabanis

11 Engagement personnel

L'Utilisateur du Système d'Information du Centre Hospitalier Paul Cabanis, par sa signature de la présente charte, reconnaît avoir lu et déclare avoir compris la présente charte et les règles auxquelles il est soumis.

Nom : .....

Prénom : .....

Fonction : .....

Déclare avoir pris connaissance de la présente charte et m'engage à m'y conformer strictement.

Date : .....

Signature :