CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques mis à la disposition du personnel du centre hospitalier du Rouvray et ainsi de permettre de :

- Respecter les dispositions législatives et réglementaires en vigueur, concernant notamment la protection des libertés individuelles, la confidentialité des données à caractère nominatif, la protection des logiciels, la répression de la contrefaçon, la protection du droit des auteurs et de la propriété intellectuelle,.
- Assurer la sécurité du système d'information
- Maintenir les performances du système et assurer à chacun un environnement de travail de qualité

Cette charte expose les principales règles que tout utilisateur doit respecter, qu'il s'agisse de règles générales d'utilisation, de règles de sécurité, d'interdictions posées par les dispositions législatives et réglementaires en vigueur ou de règles de bonnes pratiques permettant un partage équitable des ressources entre l'ensemble des utilisateurs. Une annexe à cette charte précise les règles s'appliquant spécifiquement à l'utilisation d'Internet et de la messagerie électronique.

L'attention des utilisateurs est appelée sur le caractère non limitatif des règles posées à la présente charte, qui s'appliquent sans préjudice du respect de l'ensemble des dispositions législatives et réglementaires en vigueur.

DEFINITIONS

Le terme « utilisateur » désigne toute personne utilisant les ressources informatiques de l'établissement, qu'il s'agisse de personnels titulaires et stagiaires, d'agents contractuels de droit public ou privé, de stagiaires, d'étudiants en soins infirmiers de l'IFSI, de prestataires publics ou privés intervenant dans la maintenance ou l'installation du système.

Le terme « ressources informatiques » désigne tout moyen matériel (serveurs, ordinateurs, imprimantes et autres équipements informatiques) et logiciels, mis à disposition par l'établissement.

PERIMETRE D'APPLICATION

La charte s'applique à tout utilisateur des ressources informatiques mises à disposition par l'établissement dans ses structures intra et extra hospitalières ainsi que tout autre moyen de connexion à distance afin d'accéder via le réseau informatique de l'établissement, à tout service de communication et de traitement électronique interne ou externe, y compris l'accès sur l'internet. Le respect des règles définies par la présente charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'établissement, systèmes accessibles par l'intermédiaire des réseaux de l'établissement.

SANCTIONS

La violation des dispositions précisées par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions :

- Disciplinaires, conformes au régime dont relève l'utilisateur.
- Pénales, en fonction de la législation en vigueur.

REGLES GENERALES D'UTILISATION, D'ACCES ET DE SECURITE

1) Règles générales

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques de l'établissement à partir des comptes qui lui ont été ouverts ou des matériels mis à disposition. Il doit contribuer à la sécurité générale du système d'information et réserver l'usage de ces ressources au cadre de son activité professionnelle.
L'établissement met à la disposition des utilisateurs les ressources matérielles et logicielles nécessaires à l'exercice de l'activité professionnelle. L'ajout ou l'utilisation de matériels personnels ou l'installation de logiciels autres que ceux autorisés et installés par l'établissement sont interdits. L'utilisation des logiciels et plus généralement de tout document doit se faire dans le respect des dispositions légales et réglementaires liées à la propriété intellectuelle, des recommandations fixées par les détenteurs de droits et des engagements pris par le Centre Hospitalier du Rouvray (dans les contrats de licences par exemple)
Toute demande d'installation doit être formulée auprès de la Direction de l'Evaluation et de l'Informatique (DEI) (service informatique) (cf. I/DEI/02/A).

Sur les sites de l'établissement, tout utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication internes et externes telles qu'elles sont fixées par la DEI. Ces raccordements ne peuvent être modifiés qu'avec son autorisation préalable. Ces modalités couvrent à la fois des aspects matériels (connexion physique) et logiciel (connexion logique)

L'utilisateur doit veiller à respecter les règles techniques applicables et les procédures ou protocoles d'usage du matériel et des logiciels (gestion documentaire de l'établissement). Il assure en outre, la protection de ses données et de ses informations en utilisant les moyens de sauvegarde les plus adaptés.

2) Conditions d'accès de l'utilisateur

L'établissement ne peut faire bénéficier l'Utilisateur d'un accès aux ressources informatiques qu'après acceptation de la présente Charte.

L'utilisation des ressources informatiques du Centre Hospitalier du Rouvray est soumise à autorisation préalable. Cette autorisation doit être demandée à la DEI sous couvert de son responsable de pôle.

- Cette autorisation est concrétisée par l'accès à un poste de travail et par l'ouverture d'un compte (identifiant et mot de passe autorisant l'accès à une session utilisateur Windows).
- Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement à un tiers.
- Cette autorisation ne vaut que pour les activités concourant aux missions de l'établissement, dans le respect de la législation en vigueur et que pour les missions confiées à l'agent.
- L'établissement se réserve le droit de retirer à tout moment cette autorisation.

3) règles de sécurité

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'établissement à partir du compte qui lui a été ouvert ou des matériels mis à sa disposition.
Les postes de travail sont équipés d'un logiciel anti-virus. Toutefois, les utilisateurs sont invités à faire preuve de vigilance dans l'utilisation et les transferts des fichiers en provenance du réseau interne ou externe ou de dispositifs de stockage (clés ou CD).

Sauf exception motivée, l'utilisation de tels supports externes de stockage est interdite au sein des structures extra-hospitalières. Le transfert de documents entre l'extra et l'intra-hospitalier s'effectue sur les dossiers de travail du réseau de l'établissement.

Chaque utilisateur doit donc contribuer à la sécurité du système d'information, c'est pourquoi il lui est demandé :

- D'utiliser un mot de passe permettant de garantir la sécurité de l'accès et d'en changer régulièrement, systématiquement lorsque le dispositif de sécurité du système l'exige.
  A cet effet il est conseillé d'utiliser un mot de passe composé d'au moins six caractères, mêlant lettres minuscules, majuscules et chiffres.
- Ne pas divulguer ou afficher, par quelque moyen que ce soit, le mot de passe permettant d'accéder aux ressources informatiques.
- De verrouiller la station de travail (ctrl-alt-supp) en cas d'absence prolongée.
- De veiller au cheminement et à l'élimination par broyage des documents comportant des données nominatives issus des imprimantes, photocopieurs et fax.

INTERDICTIONS, OBLIGATIONS ET REGLES DE BONNES PRATIQUES

1) Interdictions

En toutes circonstances, conformément aux dispositions légales réglementaires en vigueur, il est strictement interdit :

- De consulter, charger, stocker, publier, diffuser ou distribuer à l'aide des moyens informatiques de l'établissement, des documents, informations, images, vidéos, à caractère violent, pornographique ou portant atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs.
  Sont notamment concernés les contenus à caractère raciste, révisionniste, pédophile, prônant la discrimination sur la base du sexe, du handicap, de la religion ou des convictions politiques.
- De charger, stocker ou transmettre des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle, sauf à posséder les autorisations nécessaires.
- De charger, stocker ou transmettre des fichiers contenant des éléments protégés par dispositions relatives au droit à l'image ou à la protection de la vie privée, sauf à posséder les autorisations nécessaires.
- De charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, protégés par les lois sur la propriété intellectuelle autres que ceux autorisés et installés par l'établissement.
- D'utiliser les ressources informatiques pour une activité illégale ou susceptible de porter préjudice à l'établissement.
- De détenir, transférer ou conserver sur des dispositifs de stockage personnels ou privés des données à caractère professionnel.
- De diffuser des informations confidentielles à des tiers non autorisés ou de transmettre des données médicales nominatives par des moyens ne respectant pas les impératifs de cryptage.
- D'utiliser les ressources informatiques à des fins de harcèlement, menaces ou injures.
- D'utiliser le principe de chaine c'est-à-dire la diffusion collective démultipliée par le biais de la messagerie

2) Obligations relatives aux données nominatives

Toute constitution à l'aide des moyens informatiques de l'hôpital ou sur son réseau de traitements de données nominatives doit faire l'objet, préalablement à leur mise en œuvre d'une déclaration ou d'une demande d'avis auprès de la commission nationale informatique et libertés (CNIL) (loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

Toute personne utilisant des moyens informatiques mis à disposition par le Centre Hospitalier du Rouvray s'engage à demander l'autorisation de la direction de l'établissement pour posséder ou créer de tels fichiers. La direction de l'établissement effectuera auprès de la CNIL les démarches nécessaires.

Il est rappelé que la réalisation et le stockage de documents vidéo et photo suppose au préalable de recueillir l'accord écrit des personnes concernées (droit à l'image).
Le stockage de documents vidéo et photo impliquant des patients et des personnels de l'établissement nécessite la consultation préalable de la direction de l'établissement afin de déterminer un lieu identifié et sécurisé de stockage.

3) Règles de bonnes pratiques

Les ressources informatiques de l'établissement, en termes de volume de stockage, de flux de bande passante, sont partagées par l'ensemble des utilisateurs. Il leur est donc demandé de respecter les règles de bonnes pratiques suivantes :

a) Stockage

- stocker les fichiers volumineux en format compressé (type zip)
- ne pas dépasser, s'ils existent, les quotas prévus par l'établissement
- ne pas stocker localement (dans le dossier « Mes documents » ou sous le répertoire racine C :) des fichiers qui pourraient être archivés sur les serveurs bureautiques du réseau de l'établissement
- Cas des fichiers volumineux (photos, vidéos, musique) : ne pas stocker localement (dans le dossier « Mes documents » ou sous le répertoire racine C :) ces fichiers. La détention des fichiers photos, vidéos, musique doit se faire dans le respect des dispositions législatives et réglementaires liées à la propriété intellectuelle. La responsabilité de l'établissement ne saurait être engagée en la matière.

b) Archivage

- supprimer ou archiver les fichiers les plus anciens et qui ne sont plus utilisés,

c) Impression

- limiter au strict nécessaire les impressions de documents
- n'imprimer les documents volumineux ou incluant de nombreux graphiques que pendant les heures creuses.

4) Signalement des incidents et évènements indésirables liés aux ressources informatiques

L'utilisateur est tenu de signaler à la DEI dans les plus brefs délais tout incident de sécurité (apparition de virus, tentative d'intrusion ou intrusion), tout dysfonctionnement qu'il serait amené à observer dans le système d'information de l'établissement. Il dresse en parallèle une fiche d'évènement indésirable.

REGLES COMPLEMENTAIRES CONCERNANT LES APPLICATIONS GERANT DES INFORMATIONS DE SANTE A CARACTERE PERSONNEL

Les informations de santé à caractère personnel des patients sont conservées dans un dossier informatisé et un dossier papier.
Chaque patient a un dossier informatisé unique commun à toutes les structures de soins du Centre hospitalier du Rouvray.
Le dossier informatisé du patient est constitué par le logiciel CORTEXTE®.

1) Accès à CORTEXTE (dossier patient informatisé)

Les professionnels de santé de l'établissement se connectent en utilisant leur session, cet accès est strictement individuel.
Le mot de passe ne doit pas être communiqué, il doit être difficile à deviner, il contient au moins 6 caractères alphanumériques. Le logiciel CORTEXTE est configuré pour demander un nouveau mot de passe tous les 45 jours. Il faut verrouiller sa session lorsqu'on quitte le poste. Il est interdit d'utiliser les identifiants d'un autre utilisateur.
La gestion des accès des professionnels au logiciel CORTEXTE est réalisée par le Département de l'information Médicale (DIM).
Les professionnels ont des droits variables de lecture et d'édition (écriture) dans ce dossier en fonction de leur métier et de leur lieu d'exercice.

Les professionnels sont autorisés à accéder au contenu du dossier d'un patient uniquement s'ils sont directement impliqués dans le soin de ce patient. Toute consultation dictée par des intérêts personnels directs (dossiers patients concernant des proches, voisins, relations de travail, etc…) ou indirects (demande venant d'un proche, d'une relation, famille d'un patient etc…) est interdite et donnera suite à des poursuites selon la réglementation en vigueur.

Le Département de l'information Médicale effectue des contrôles systématiques sur les accès au dossier des patients (consultations de dossiers, actions effectuées) et est en mesure de relever ainsi l'identité des contrevenants à cette charte.

Dans le cadre d'une recherche scientifique ou d'une évaluation des pratiques, des dérogations peuvent être obtenues auprès du DIM pour accéder à certaines informations, dans les conditions prévues par la règlementation en vigueur

2) Traçabilité dans CORTEXTE

Tous les accès à un dossier patient sont tracés : dates, heures nom, prénom et fonction de l'utilisateur. Ces informations sont accessibles sur la page d'accueil du dossier d'un patient (bouton "*Utilisateurs*"). Elles font parties du dossier du patient et bénéficient des règles de communication et de conservation du dossier patient.
Il est possible d'imprimer des éléments choisis du dossier du patient. Les documents imprimés rejoignent le dossier papier du patient et doivent être traités comme tel. Les documents imprimés sont tracés : date, heure, nom, prénom, fonction de l'opérateur ainsi qu'une copie numérique du document imprimé. Ces informations sont accessibles sur la page d'accueil du dossier du patient : bouton « *Histo. Imp.* »

Les données à caractère personnel des patients ne doivent pas être dupliquées, ni stockées sur des supports externes (clés USB ou autres) ou être transmises dans des emails qui ne soient pas sécurisés.
En cas de manquement aux règles de la présente charte, la personne responsable de ce manquement est passible de sanctions internes à l'établissement et éventuellement de sanctions civiles ou pénales, selon la gravité du manquement et la règlementation en vigueur.

NB : Les règles complémentaires concernant les applications gérant des données de santé ont été rédigées par le DIM, validées par le Directoire, la CME et le CTE de février 2014.

ANNEXE : Règles d'utilisation d'Internet et de la messagerie électronique

Le non respect des recommandations ci-dessous énoncées ne constitue pas un délit au sens strict sans préjudice du respect de l'ensemble des dispositions législatives et réglementaires en vigueur. Le Centre Hospitalier du Rouvray se réserve toutefois le droit de prendre les mesures nécessaires pour faire cesser les abus observés.

1) Accès à Internet

a) Modalités d'accès

Les accès individuels ouverts par la DEI sont réservés à la consultation de sites concernant le domaine professionnel.
L'établissement se réserve donc le droit de :
- bloquer l'accès à des sites n'ayant aucun rapport avec l'activité professionnelle ;
- bloquer l'accès internet (Web) en cas de constatation d'abus de l'utilisateur ;
- limiter l'accès des utilisateurs à quelques sites ; par défaut, les agents disposant d'une session utilisateur Windows ont accès aux sites internet figurant sur la page d'accueil du site intranet de l'établissement.

b) Bonnes pratiques d'utilisation

La bande passante du réseau est une ressource coûteuse et limitée. Pour assurer un équilibre optimal de la charge du réseau, un partage équitable de la bande passante, et donc des performances satisfaisantes pour tous, l'application des règles suivantes d'utilisation des services est recommandée :

- Ne pas charger de fichiers volumineux et/ou exigeants en espace disque et bande passante (fichiers vidéo, sons, ...).
- Ne pas utiliser de sites exigeants en bande passante (sites de conversation en temps réel type « chat », de consultation de vidéo en « streaming »)

c) Traces laissées par les utilisateurs, protection contre la malveillance et sécurité

A des fins statistiques, de qualité de service et de sécurité, le trafic Internet est supervisé par la DEI, qui dispose des éléments d'information remis par son fournisseur d'accès. Pour les mêmes raisons, l'établissement procède à des vérifications régulières du trafic, dans les limites fixées par la loi. Les administrateurs informatiques (DEI) qui effectuent ces opérations, sont tenus au secret professionnel. L'historique des traces de connexion sur Internet des utilisateurs est sauvegardé sur une période de 6 mois, conformément aux recommandations de la CNIL.

Il est rappelé aux utilisateurs que les serveurs hébergeant les sites consultés conservent des marques électroniques susceptibles d'impliquer l'utilisateur et l'établissement. Ces traces sont parfois recueillies de façon malveillante à l'aide de programmes dits « logiciels espions » destinés à favoriser l'enregistrement de l'adresse électronique (adresse IP) du poste utilisé, de données relatives aux centres d'intérêt de l'utilisateur ou susceptibles de favoriser des tentatives d'accès non autorisées.
Le fournisseur d'accès Internet de l'établissement assure la protection contre la malveillance et l'intrusion au moyen d'un logiciel anti-virus et d'un logiciel pare-feu.

2) Messagerie électronique

Les comptes de messagerie sont ouverts par l'établissement et réservés à un usage professionnel.

a) Application du principe du secret des correspondances privées

Les messages électroniques (ou courriels) émis depuis les comptes ouverts par l'établissement constituent des écrits impliquant l'établissement. Tout message de ce type est susceptible d'être stocké, réutilisé ou exploité par son destinataire. Le message électronique constitue une preuve ou un commencement de preuve par écrit. L'établissement s'engage à respecter le secret des correspondances privées dans les limites fixées par les dispositions législatives et réglementaires en vigueur ainsi que par la jurisprudence. En particulier, l'établissement peut être saisi par une autorité compétente dans le cadre d'une instruction pénale ou par une décision de justice pour lever, sous le contrôle d'un juge ou d'un huissier, le secret des correspondances privées.

b) Ouverture

Se référer au paragraphe 2 de la charte d'utilisation des ressources informatiques
Toute ouverture de boîte à lettres s'accompagne d'une inscription sur l'annuaire global de la messagerie de l'établissement.

c) Règles de bonnes pratiques

- Bref et pertinent

L'extension de la messagerie dans l'établissement fait que plusieurs centaines de boîtes aux lettres peuvent s'échanger des messages. Ainsi le nombre des messages diffusés par une boîte aux lettres est en augmentation constante. Déjà quelques boites aux lettres reçoivent et/ou émettent plusieurs centaines de messages par jour.
Il est donc nécessaire que les messages soient les plus brefs et les plus pertinents possibles. Chacun y gagnera du temps.

- Chaîne.

La caractéristique principale d'une chaîne est d'augmenter d'une manière exponentielle le nombre de messages circulants (un message d'une chaîne pointant sur dix destinataires peut devenir un million de messages au bout de six générations), elle peut mettre en péril l'ensemble du système
L'utilisateur devra donc s'abstenir de créer et/ou de participer à ces chaînes.

- Courtoisie

Les règles habituelles de courtoisie devront s'appliquer à l'ensemble des messages émis.

- .Utilisation de listes de distribution collectives (tous, tous médecins…) ou personnelles.

Ces listes ont été créées pour permettre aux instances d'informer rapidement un groupe ou une corporation. Elles n'ont pas pour objet de passer de petites annonces, diffuser de la publicité ou des informations associatives ou tout autre information qui ne soit pas d'un caractère professionnel.
Il en est de même pour les listes de distributions personnelles que chacun peut se constituer dans son carnet d'adresse personnel.
Par de très gros volumes de données instantanés qu'elles engendrent par les tempêtes de messages, l'antivirus de la messagerie peut demander plusieurs minutes, après l'envoi, pour nettoyer des messages et leur utilisation à outrance peut déstabiliser la messagerie jusqu'à la rendre inutilisable.

L'utilisateur devra donc être vigilent à n'utiliser ces listes que dans le cadre institutionnel, à bon escient et s'abstenir d'envoyer des documents attachés aux messages lors de leur utilisation.

Conseils :

Éviter les messages trop volumineux (taille supérieure à 1 Mo) ou utiliser des utilitaires de compression de fichiers ou de tronçonnage des messages si nécessaire;

Effectuer les envois les plus volumineux et non urgents pendant les heures creuses (de 18 h à 8 h);

Pas d'images en arrière-plan des messages.

d) Archivage des messages

Il ne peut être envisagé de conserver indéfiniment les messages sans risquer de créer des dysfonctionnements sur le serveur de la messagerie :

- Épurer régulièrement les messages et/ou pièces jointes devenus inutiles;
- Vider régulièrement la corbeille de la messagerie;
- Respecter les quotas limitant l'utilisation de l'espace disque des messageries

La durée maximale de conservation des messages est limitée actuellement à 1 an ce qui signifie que les messages antérieurs à 1 an sont systématiquement détruits.

Chaque utilisateur doit prendre lui-même, s'il souhaite, l'initiative de conserver dans les dossiers personnels les messages qui pourraient ainsi être supprimés.

Cette durée de conservation pourra être diminuée si le besoin s'en fait sentir. Chacun en sera averti.

e) Manquement à la charte

L'établissement se réserve donc le droit de désactiver l'adresse email en cas de constatation d'abus de l'utilisateur.