


Direction des Systèmes d'Information
GHT d'Armor
CHARTE D'UTILISATION DES OUTILS INFORMATIQUES

PREAMBULE

Les Systèmes d'Information (SI) des Centres Hospitaliers de Lannion et de Saint Brieuc permettent de gérer et de partager de manière contrôlée les informations nécessaires pour exercer leurs activités et remplir leurs missions auprès de la population et ce, dans les meilleures conditions. Le traitement des informations qui y circulent et y sont stockées, qu'elles soient nominatives, confidentielles, médicales ou de l'ordre de la recherche, mais aussi de nature privée (données personnelles de l'utilisateur), doit être l'objet de toutes les attentions.

Afin d'offrir le meilleur usage de ces outils de traitement de l'information, des règles d'utilisation sont définies dans le respect de la réglementation en vigueur, dans l'objectif de protéger le patrimoine informationnel des établissements et de parer à toute utilisation frauduleuse.

Cette charte, régissant l'utilisation des outils informatiques mis à disposition par les établissements formalise pour chaque acteur, son niveau de responsabilisation et la nécessité de respecter les bonnes pratiques d'usage pour assurer l'intégrité et la sécurité dudit système.

Cette charte, annexée au règlement intérieur des établissements, comporte 9 articles et une conclusion et fait partie des éléments fondateurs de la Politique de Sécurité du Système d'Information.

ARTICLE 1- DEFINITIONS

Sont désignés sous le terme « ressources informatiques », les moyens informatiques de calcul ou de gestion centraux et locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'Institution.

Sont désignés par « Services Internet », la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum…

Sont désignés sous le terme « Utilisateurs », les personnes ayant accès ou utilisant les ressources informatiques et services Internet.

Sont désignés sous le terme « Administrateurs », les personnels responsables du bon fonctionnement des SI. Le statut et les responsabilités particuliers et juridiques de ces administrateurs sont traités dans une charte spécifique.

ARTICLE 2 - ACCES AUX RESSOURCES INFORMATIQUES ET SERVICES INTERNET

L'usage par les utilisateurs des ressources informatiques et des services Internet mis à disposition par les établissements, s'exerce dans le cadre de l'activité professionnelle conformément à la législation en vigueur.

L'utilisation des ressources informatiques des Institutions est systématiquement soumise à autorisation et leur accès est protégé par des paramètres de connexion (identifiant, mot de passe et autres dispositifs). Ces éléments sont strictement personnels et ne peuvent en aucun cas être cédés, même temporairement, à un tiers.

Cette autorisation peut être retirée à tout moment et prend fin lors de la cessation, même provisoire, de l'activité professionnelle de l'utilisateur au sein de l'établissement.

Ces dispositions concernent également les intervenants extérieurs (acteurs d'autres organismes exerçant dans l'établissement, stagiaires, etc ..), amenés à utiliser les ressources institutionnelles, de quelque nature que ce soit, et dont l'accès fera l'objet d'une autorisation préalable à émettre auprès de la Direction des Systèmes d'Information. Cette demande d'autorisation sera accompagnée du formulaire attestant l'acceptation des conditions de cette présente charte, complétée et émargée par l'intervenant externe. L'accès aux ressources informatiques par un prestataire externe fait l'objet d'un engagement contractuel de sécurité et confidentialité établi en amont de son intervention avec la Direction des Systèmes d'Information.

Tout utilisateur, quel qu'il soit, est responsable du bon usage des ressources informatiques, du traitement et du stockage des données mises à sa disposition. Il concourt à leur protection en faisant preuve de prudence et en respectant les dispositions et recommandations liées à la sécurité générale du Système d'Information. L'utilisateur :

- Choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers, ni les rendre lisibles ou visibles ;
- Signale toute tentative de violation de son compte et, de façon générale, toute anomalie ;
- Ne met pas à la disposition d'utilisateurs non autorisés, un accès total ou partiel aux ressources de l'établissement ;
- Veille au bon usage des ressources de stockage et limite autant que faire se peut, la duplication des informations, voire le stockage d'informations qui n'ont pas vocation à être conservées,
- Ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,
- Doit préalablement se déconnecter avant de quitter son poste de travail afin de ne pas laisser libre accès aux ressources ou services des établissements.

ARTICLE 3 - DONNEES PERSONNELLES

Les établissements entendent permettre l'utilisation de ressources mises à disposition à des fins personnelles, dès lors que cela n'engendre pas de dysfonctionnement, de quelque nature que ce soit. Cette utilisation, qui doit être rationnelle et proportionnée pour ne pas engendrer de saturation ou de détournement de ressources, répond aux dispositions suivantes :

- Le stockage de données personnelles ne peut s'effectuer que dans un dossier dénommé « Personnel » localisé dans un espace accessible uniquement par l'utilisateur. Le volume d'informations personnelles stockées ne doit pas dépasser 50 Moctets.
- L'utilisateur s'interdit de conserver sur son poste des informations contraires à l'ordre public et l'intégrité des personnes, et plus généralement, contrevenant à une disposition légale ou réglementaire.
- Concernant l'utilisation de la messagerie électronique, les messages à caractère personnel devront impérativement contenir dans leur objet la mention « personnel » et sont stockés dans un dossier dénommé « Personnel » pour être reconnus comme tels par les administrateurs.

ARTICLE 4 - CONDITIONS DE CONFIDENTIALITE ET PROTECTION DES DONNEES

L'accès aux informations et documents conservés et traités sur les systèmes d'information par les utilisateurs doit être limité à ceux qui leur sont propres, et pour lesquels ils sont habilités. Les règles d'accès au dossier médical informatisé sont définies par le Collège de l'Information Médicale (CIM) et formalisées sur le document INFO.S.010 (SB) / I GSI 04-01-00 (LN).

L'utilisateur protège les données en les stockant dans les espaces sécurisés prévus à cet effet. A défaut, il s'assure que l'accès à celles-ci respecte les règles précédemment énoncées et utilise les moyens de sauvegarde adéquats pour en assurer la pérennité.

L'utilisateur ne doit pas tenter de lire, modifier, copier ou détruire directement ou indirectement, des données autres que celles pour lesquelles il est autorisé à le faire, quand bien même leur propriétaire ne les aurait pas explicitement protégées.

Seuls les personnels de la Direction des Systèmes d'Information, reconnus comme administrateurs dans le cadre de leur activité de maintien et surveillance des outils relevant de leur domaine d'intervention, sont habilités à prendre directement ou indirectement connaissance d'informations détenues par les utilisateurs. Ceci dans le respect du secret professionnel, de la confidentialité et de la vie privée, et ce au regard des lois et statuts professionnels en vigueur.

ARTICLE 5 - RESPECT DE LA LEGISLATION CONCERNANT LES LOGICIELS

L'installation et la mise en œuvre de l'ensemble des composants logiciels et matériels sont du ressort exclusif de la Direction des Systèmes d'Information. L'utilisateur ne doit tenter en aucun cas d'installer un logiciel de quelque nature que ce soit, d'en contourner les restrictions d'usage ou d'utiliser de copies de fichiers illicites.
En cas de non-respect, la législation concernant la propriété intellectuelle et les sanctions prévues par la loi pourront s'appliquer.

ARTICLE 6 - PRESERVATION DE L'INTEGRITE DES SYSTEMES D'INFORMATION

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques par des manipulations anormales de matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, applications « peer to peer », téléphonie gratuite sur IP non institutionnelle, analyseurs de trames et outils d'administration, par exemple…).

La Direction des Systèmes d'Information prend les dispositions pour protéger les équipements mis en œuvre. Seuls les administrateurs sont habilités à modifier la configuration des équipements.

De son propre chef, l'utilisateur ne procèdera en aucun cas à quelque installation de matériel informatique que ce soit dans l'enceinte des établissements sans autorisation préalable de la Direction des Systèmes d'Information.

ARTICLE 7 - USAGE DES SERVICES INTERNET

Pour des raisons de sécurité et d'intégrité, des outils de filtrage et de traçabilité des accès aux services Internet sont mis en œuvre par la Direction des Systèmes d'Information.

Dans l'usage des services Internet, l'utilisateur :

- Fait usage des services Internet dans le respect de la législation en vigueur et notamment celle relative à l'accès aux publications à caractère illicite de type injurieux, raciste, pédopornographique, diffamatoire, ... ;
- Ne se livre pas à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs et du réseau auxquels il accède ;
- N'utilise pas ces services pour transmettre à un tiers des données et informations confidentielles en dehors d'un procédé de cryptologie conforme à la législation en vigueur ;
- N'utilise pas ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Fait preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions… ;
- N'émet pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'institution.

L'utilisation des services Internet à titre personnel est autorisée au regard du Code du travail à condition de respecter les principes de proportionnalité et de loyauté et de ne pas être porteuse d'activité commerciale ou assimilée.

ARTICLE 8 - ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES

La Direction des Systèmes d'information doit, au regard de ses missions, assurer le contrôle et le bon fonctionnement du système d'information, et à ce titre veille à l'application des règles de la présente charte. Pour mener à bien sa mission, elle met en œuvre des outils d'analyses, de traçabilité et de contrôle de l'usage des ressources et en exploite les informations dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés (Cyber surveillance et droits de l'utilisateur).

Ces surveillances s'exercent sur :

- L'utilisation des logiciels applicatifs, pour contrôler les accès, modifications, et suppressions d'informations ;
- Les flux transitant sur le réseau informatique, en entrée comme en sortie : connexions Internet, intranet, messagerie ;
- L'usage des ressources techniques (poste de travail, imprimantes, etc…).

Les établissements, dans un souci de respect de la loi, se réservent la possibilité de contrôler à tout moment les données traitées et stockées par les ressources mises à disposition.

Les données personnelles des utilisateurs stockées, dès lors qu'elles respectent les dispositions décrites ci-avant ne sont pas concernées par ces contrôles.

Toutefois, il est des cas exceptionnels où un tel contrôle est possible :

- Demande d'une autorité juridictionnelle ou de police ;
- Poursuites disciplinaires et/ou pénales contre l'agent pour une infraction facilitée ou occasionnée par l'utilisation d'un matériel informatique (fraude informatique, téléchargement de logiciels piratés…) ;
- Poursuites disciplinaires motivées par un manquement aux instructions fixées par la présente Charte ;
- Péril imminent pour le Centre Hospitalier ou l'un de ses agents ;
- Circonstances exceptionnelles.

Cette liste n'est pas limitative dès lors que l'état de nécessité est démontré par les faits de la cause.

L'utilisateur ne sera pas informé préalablement du contrôle (ni du principe du contrôle, ni de la date et de l'heure), mais en connaitra les motifs.

Il sera présent ou représenté par la personne de son choix au moment du déroulement des opérations de contrôle.

Une tolérance sera apportée, une fois la différence faite, entre le caractère intentionnel (passible de sanctions) et accidentel.

ARTICLE 9 - RAPPEL DU CADRE LEGISLATIF ET REGLEMENTAIRE

Il est rappelé que toute personne sur le sol français doit respecter la législation européenne et française notamment dans le domaine de la sécurité informatique :

- Loi CNIL N° 78-17du 06/01/1978 dite "informatique et liberté", modifiée par la loi relative à « la protection des personnes physiques à l'égard des traitements de données à caractère personnel », du 06/08/2004 ;
- Loi N° 83.634 du 13/07/83, article 26, relative au secret professionnel ;
- Article 1383 du Code Civil, *« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »* ;
- Article 1384 alinéa 5 du Code Civil, relatif à la responsabilité de l'employeur en tant que commettant de ses employés ;
- Article 226-15 du Code pénal, relatif à la correspondance privée ;
- La législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal) ou loi Godfrain ;
- La législation relative à la propriété intellectuelle ;
- Loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé ;
- Articles L. 120-2 et 120-4, L.121-7 et 121-8 du Code du travail ;
- Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires) ;
- Articles R. 1110-1 et R. 1110-2 du Code de la santé publique.

CONCLUSION

Les utilisateurs des outils informatiques des établissements s'engagent à appliquer les règles de bon usage définies dans le présent document.

La Direction des Systèmes d'Information engage systématiquement les actions nécessaires à la préservation du service lorsque surviennent des problèmes liés à la sécurité du système d'Information.

Tout utilisateur qui ne respectera pas les règles présentées dans cette charte est passible de sanctions internes et les établissements se réservent le droit d'engager une procédure juridique en fonction de la nature du manquement constaté.

La sécurité et le bon fonctionnement de notre Système d'Information sont l'affaire de chacun, soyez en un acteur responsable.

Jean SCHMID
Directeur
Centre Hospitalier Saint Brieuc

Anne LEFEBVRE
Directrice
Centre Hospitalier Lannion-Trestel

CHARTE D'UTILISATION DES OUTILS INFORMATIQUES

Centres Hospitaliers de LANNION-TRESTEL et SAINT BRIEUC

REGLES D'ACCEPTATION DES CONDITIONS D'UTILISATION DES OUTILS INFORMATIQUES

Cette charte s'applique **à tous les utilisateurs du système d'information** des Centres Hospitaliers de Lannion-Trestel et de Saint-Brieuc. Elle a fait l'objet d'une validation par les instances représentatives, et est accessible sur l'intranet de chaque établissement, ainsi que sur le bureau des postes informatiques.
Les modalités de prise de connaissance et d'acceptation de cette présente charte sont déterminées par le statut de l'utilisateur, selon les règles suivantes :

- Les personnes appartenant à l'établissement sont réputés avoir pris connaissance de cette charte et d'en avoir accepté le contenu par la signature de leur contrat de travail *(annexe du règlement intérieur).*

- Les personnes n'appartenant pas à l'établissement *(stagiaire, fournisseur, prestataire, ..)* doivent attester la prise de connaissance et l'acception de l'intégralité des règles définies dans cette charte, avant tout accès aux outils du système d'information. Pour ce faire, l'attestation, ci-dessous, doit être complétée et remise à la Direction des Systèmes d'Information.

Prénom : _____

Nom : _____

Organisme d'origine : _____

Etablissement d'exercice : ❒ Lannion-Trestel ❒ Saint Brieuc

Service/Direction/Pôle ou lieu d'exercice : _____

Correspondant interne - Nom Prénom : _____

Fonction : _____

Je déclare avoir pris connaissance de la charte d'utilisation des outils informatiques des Centres Hospitaliers Lannion-Trestel et Saint Brieuc et j'en accepte intégralement le contenu.

Date : _____

Signature :