Annexe 12

Règlement relatif à l'utilisation des moyens informatiques du CHU de POITIERS

Version 2.0
Juin 2017

Ce document est la propriété du CHU de POITIERS. Les informations qu'il contient sont la propriété de l'Etablissement et ne peuvent pas être reproduites en totalité ou en partie ou être transmises par tout moyen sans l'autorisation écrite de l'Etablissement.

CYCLE DE VIE DU DOCUMENT

HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
1.1	30 septembre 2011	Version initiale	
1.2	23 mars 2012	Version amendée (Règles, Droit)	
2.0	Juin 2017	Version amendée (Règles, Droit)	

Règlement relatif à l'utilisation des moyens informatiques du CHU de POITIERS

1 - Objet

Les présentes dispositions ont pour objet de définir les conditions d'utilisation et les règles de bon usage des moyens informatiques du CHU de Poitiers et d'assurer le développement de l'utilisation de l'informatique dans le respect des lois et des règlements.

2 – Domaine d'application

La présente Charte définit les droits et devoirs de chaque utilisateur.
Ce règlement s'applique à l'ensemble des personnes qui, quel que soit le lieu où leur statut, ont accès aux moyens informatiques du CHU de Poitiers, mis à disposition sur ses différents sites.

3 – Moyens informatiques

Sont **notamment** constitutifs de moyens informatiques, les serveurs, les stations de travail, les postes de travail, les réseaux internes et externes du CHU de Poitiers, les micro-ordinateurs des services, laboratoires, instituts, écoles, associations, personnels ainsi que l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits.
Sont également considérés comme moyens informatiques, les ressources extérieures accessibles par l'intermédiaire des réseaux du CHU de Poitiers, incluant ceux des opérateurs de télécommunications opérant pour le compte du CHU de Poitiers, et notamment le réseau RENATER (Réseau National des Télécommunications, de l'Enseignement et de la Recherche) et sa passerelle INTERNET. L'utilisation dans le contexte du CHU d'un réseau autre que RENATER ne modifie en rien les obligations des utilisateurs citées dans le présent document, les conditions d'utilisations s'appliquant de la même manière.

4 – Utilisations

4.1 – Finalités de l'utilisation des moyens informatiques du CHU de Poitiers

L'utilisation des moyens informatiques est limitée au strict cadre et aux seuls besoins de l'activité professionnelle et de la vie hospitalière.

4.2 – Autorisations particulières

Toute autre utilisation des moyens informatiques du CHU de Poitiers doit être préalablement autorisée par le Directeur Général.

4.3 – Utilisations prohibées

Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui ont pour objet ou pour effet la diffusion d'idéologies politiques ou qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur ou à la vie privée des personnes.

5 - Utilisateurs

5.1 – Identification des utilisateurs

Pour bénéficier d'un accès au système d'information, chaque nouvel utilisateur doit être déclaré.
Tout départ ou changement d'affectation doit être signalé.
Les utilisateurs sont responsables de l'utilisation de leur(s) accès au système d'information et des données associées.
Cet accès est strictement personnel et ne peut donc en aucun cas être prêté ou cédé. Il peut être retiré partiellement ou totalement, temporairement ou définitivement, en cas de non-respect de la Charte.

5.2– Obligations des utilisateurs

5.2.1 – Règles générales

Les utilisateurs sont tenus de respecter les règles de bon usage de l'informatique du CHU de Poitiers.
Les utilisateurs doivent respecter les lois et règlements en vigueur ainsi que les règles de courtoisie et de politesse lors de l'utilisation des moyens informatiques du CHU de Poitiers.
Les utilisateurs doivent faire une utilisation non-abusive des moyens informatiques auxquels ils ont accès.
Les utilisateurs doivent respecter les mesures de sécurité des moyens informatiques prévus à l'article 8 du présent règlement.
Les utilisateurs sont tenus de se conformer aux décisions du responsable informatique.

5.2.2 – Fichiers des utilisateurs

Les informations utilisées dans le cadre des missions du CHU de Poitiers sont la propriété du CHU de Poitiers : elles sont stockées dans des fichiers ou des bases de données placées sous sa responsabilité.
Les utilisateurs peuvent créer sur les supports mis à leur disposition par le CHU de Poitiers des fichiers privés pour lesquels ils ont droit d'accès exclusif. Ces fichiers doivent être enregistrés dans un répertoire dénommé « PERSONNEL ».
La responsabilité de l'utilisateur, et nullement celle du CHU de Poitiers, sera engagée dès lors qu'une donnée sera stockée par lui sur un support externe au CHU.
Sont interdites la destruction, l'altération ou la reproduction d'un fichier mis à la disposition du public, en dehors des cas où elles sont expressément autorisées.
Les traitements portant sur des données à caractère personnel au sens de la Loi « Informatique et Libertés » du 6 janvier 1978 modifiée en 2004, quel que soit le cadre de leur utilisation, doivent être déclarés auprès de la Commission Nationale Informatique et Libertés, via le Correspondant Informatique et Libertés de l'établissement.

5.2.3 – Usage de la messagerie électronique professionnelle

La messagerie est réservée à un usage professionnel. **L'usage de la messagerie de l'Etablissement engage sa responsabilité**.
Les utilisateurs doivent faire preuve de la plus grande correction vis-à-vis de leurs interlocuteurs, dans toutes leurs communications, qu'elles soient internes ou externes.
Une utilisation privée occasionnelle et raisonnable est tolérée. Dans ce cas, un message à caractère privé doit être identifiable sans ambiguïté et / ou enregistré dans un espace dédié (Message ou dossier dénommé « PERSONNEL »).
Il convient de faire régulièrement le tri et d'évaluer la pertinence de conserver ou non les messages, particulièrement ceux contenant des pièces jointes. La messagerie électronique n'est pas un espace de stockage.
Il est recommandé de ne pas divulguer son adresse électronique sur des forums ou sur des sites Internet non professionnels, en raison du risque de virus et de surcharge inutile de la boite mail.
Les messages à diffusion générale sont interdits. Seule la Direction Générale peut autoriser ou réaliser une diffusion à l'ensemble des utilisateurs déclarés.
Tout message suspect doit être signalé au Responsable Sécurité Du Système d'Information (RSSI).

Afin de garantir aux professionnels de santé la confidentialité des informations échangées, et en particulier les données sensibles ou à caractère personnel, il est mis à disposition une messagerie sécurisée, intégrant l'envoi de courriels et de pièces jointes, et d'une sécurisation garantissant la confidentialité et l'authenticité conformément au décret de confidentialité du 15 mai 2007.

D'une façon générale, le service informatique prend toutes mesures pour se prémunir des attaques extérieures (pare feu, antivirus, etc.), qui pourraient affecter le fonctionnement du réseau et des applications, utilisés par le CHU, aucune machine de pourra déroger aux règles de filtrages mises en œuvre.

5.2.4 – Usage de l'Internet
Seuls ont vocation à être consultés les sites Internet, conformes à la finalité des réseaux utilisés par le CHU de Poitiers, présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

Une consultation ponctuelle et dans des limites raisonnables du web, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation du CHU est tolérée.

Le téléchargement de fichiers, de logiciels, de vidéos, d'images, de sons, ainsi que la visualisation en ligne de médias non liés à l'activité professionnelle sont interdits.

La réglementation impose une traçabilité nominative des accès Internet (loi du 23 janvier 2006 relative à la lutte contre le terrorisme). L'Etablissement assure une traçabilité des navigations Internet et met en œuvre des outils de filtrage adaptés. Un usage inapproprié de l'Internet pourra donner lieu à sanction.

5.2.5 – Dispositions en cas d'absence d'un salarié
En cas d'absence prolongée d'un salarié 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 message est clairement identifié comme étant personnel, l'employeur ne doit pas en prendre connaissance. »

5.2.6 – Préservation des matériels et locaux
Les utilisateurs sont tenus de respecter les matériels, logiciels et locaux mis à leur disposition.
Les utilisateurs qui constatent une dégradation ou un dysfonctionnement doivent, dans les plus brefs délais, informer le responsable informatique.

5.2.7 – Pénétration non autorisée dans les moyens informatiques
Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également interdite toute manœuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur.
De la même manière, il est strictement interdit d'utiliser son code personnel ou celui d'un collègue de travail pour avoir accès aux informations administratives ou médicales relatives à un malade, en dehors d'une prise en charge pour laquelle l'utilisateur est parte prenante. Dans tous les cas, la navigation sera enregistrée pour une durée d'un an et reprendra tous les critères imposés par les textes et permettant à l'établissement, dans le cadre d'une information ou d'une enquête, de mettre à disposition le contenu aux autorités administratives et judiciaires.

5.2.8 – Utilisation des comptes et des dispositifs de contrôle d'accès
Les utilisateurs doivent prendre toutes mesures pour limiter les accès frauduleux aux moyens informatiques et à ce titre doivent **notamment** :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leurs sont confiés à titre strictement personnel,
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel,

- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers,
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent
- informer immédiatement le responsable Sécurité du Système d'Information (RSSI) de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect,
- changer régulièrement les codes d'accès,
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles par des tiers,
- informer le responsable informatique des périodes durant lesquelles ils n'utiliseront pas leurs comptes.

5.3 – Responsabilité des utilisateurs

5.3.1 – Responsabilité des utilisations
Les utilisateurs sont responsables de l'utilisation qu'ils font des moyens informatiques du CHU de Poitiers ainsi que de l'ensemble des informations qu'ils mettent à la disposition du public.

5.3.2 – Responsabilité des comptes et dispositifs de contrôle d'accès
Les titulaires de comptes ou d'un dispositif de contrôle d'accès, sont responsables des opérations locales ou distantes effectuées depuis leurs comptes ou sous le couvert des dispositifs de contrôle d'accès qui leur ont été attribués.

5.3.3 – Cas des Réseaux Sociaux
Toute personne se connectant sur des réseaux sociaux, blogs, ou forums, s'engage au respect de son obligation de réserve et du secret professionnel. La présence de ces personnes sur ces réseaux, blogs, ou forums, engage leur stricte responsabilité à titre privé, et ne saurait engager sur quelque motif que ce soit la responsabilité du CHU de Poitiers. Le CHU de Poitiers se réserve toutes possibilités de recours comme décrit à l'article 8.2 de la présente charte en cas de nécessité et de non-respect des principes édictés ci-dessus.

5.4 – Sanctions
En cas de non-respect de leurs obligations, les utilisateurs peuvent se voir appliquer les sanctions prévues à L'article 8.

6 – Données à caractère personnel
Les traitements automatisés de données à caractère personnel que ce soit ou pas dans le cadre de protocoles de recherche mis en œuvre par le CHU de POITIERS ou par tout utilisateur doivent respecter les dispositions de la loi **78-17 du 6 janvier 1978** modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés.

7 – Modification et altération des moyens informatiques

7.1 – Modification des environnements
En dehors des modifications ne portant pas atteinte au bon fonctionnement des moyens informatiques, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du responsable informatique.
Par modification d'environnement, on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.

7.2 – Virus, chevaux de Troie, bombes logiques…..

L'introduction, l'utilisation, la diffusion de tout dispositif logiciel ou matériel qui pourrait altérer les fonctionnalités des moyens informatiques sont interdites.
Les recherches portant sur les virus, chevaux de Troie, bombes logiques et autres dispositifs qui pourraient altérer les fonctionnalités des moyens informatiques doivent être préalablement autorisées par le responsable informatique.

Selon ces différents cas et en application de la Loi GODFRIN du 5/01/1988, les délits sont punis d'une peine de prison allant d '1 à 3 ans, et de 10000 à 500000 Frs d'amende. On peut aller si la gravité extrême est reconnue (espionnage) à la déchéance des droits civiques, civils et de famille pour une durée maximale de 5 ans.

8– Conséquences des manquements au règlement

8.1 – Mesures et sanctions applicables par le responsable informatique ou le responsable de la sécurité des systèmes d'information

Le responsable informatique ou le responsable de la sécurité des systèmes d'information peut en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation,
- limiter provisoirement les accès d'un utilisateur,
- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes, notamment les comptes de messagerie et de connexion à l'Internet,
- effacer, comprimer ou isoler toute donnée ou fichier manifestement en contradiction avec le règlement ou qui mettrait en péril la sécurité des moyens informatiques.

Le responsable informatique ou le responsable de la sécurité des systèmes d'information peut procéder à des contrôles de bonne utilisation de la messagerie et de l'Internet sur demandes internes des instances ou sur requêtes judiciaires.

8.2 – Poursuites civiles ou pénales

Le Directeur Général peut, après avis du Conseil de Surveillance, engager des poursuites civiles à l'encontre des utilisateurs.
Le Directeur Général peut, après avis du Conseil de Surveillance informer le Procureur de la République des infractions commises par les utilisateurs.