Charte d'utilisation du Système d'Information

Extrait de la charte détaillée élaborée par le « comité de gestion des risques liés au système d'information hospitalier »

1 Objet de la charte

Cette charte s'inscrit dans le cadre de la politique de sécurité du système d'information de l'établissement.
Celle-ci présente les droits et devoirs liés à l'utilisation des ressources informatiques au sein de l'EPSM de l'agglomération lilloise.

Elle vise d'abord à protéger les données de santé des « Usagers » puis également à concilier le respect de la vie privée des agents.

Partagé par l'ensemble des utilisateurs, le système d'information n'en demeure pas moins la propriété de l'établissement.

2 Les droits et les devoirs de l'utilisateur

Je suis employé de l'établissement, je dispose d'un droit d'accès aux ressources informatiques

Toute personne travaillant au sein de l'établissement dispose d'un droit d'accès au système d'information.

Je dispose de codes d'accès personnels, je ne les communique à personne

Les moyens d'authentification sont individuels et ne peuvent en aucun cas être communiqués, prêtés ou cédés à un tiers. Ces codes sont sous la responsabilité individuelle de son détenteur.

Je me déconnecte lorsque je quitte mon poste informatique

Afin d'éviter l'accès à des données confidentielles par des personnes non autorisées, l'utilisateur veille à se déconnecter des applications et du réseau lorsqu'il quitte son poste de travail.

Je ne saisis aucun nom de personne (patient ou agent) en dehors des logiciels autorisés par l'établissement

Aucun traitement ne doit être fait sur des données nominatives en dehors des logiciels autorisés par l'établissement qui eux seuls garantissent la confidentialité des informations. Eviter notamment l'usage des outils bureautiques (open office, word, excel...), de la messagerie et des répertoires partagés. L'utilisation de données nominatives dans un logiciel informatique doit faire l'objet d'une déclaration à la Commission Nationale Informatique et Libertés (CNIL) avant sa mise en œuvre.

J'utilise le matériel mis à ma disposition à des fins professionnelles

L'utilisation abusive du matériel informatique à des fins personnelles est interdite. Tout matériel non approuvé par la direction du système d'information ne peut être connecté au réseau informatique de l'établissement.

Je ne stocke pas de données confidentielles sur des supports amovibles

L'utilisation des supports amovibles (clé USB, CD, DVD, ...) est sous la responsabilité de son détenteur. Chacun veille à les stocker de manière à les préserver contre tout risque de vol et à les déposer dans un lieu sécurisé. D'autre part, les utilisateurs doivent éviter de stocker des informations confidentielles (telles que les informations médicales à caractère personnel) sur les supports informatiques.

J'utilise exclusivement les logiciels mis à disposition par l'établissement

Les logiciels acquis à titre personnel ne sont pas autorisés sur les équipements de l'établissement. L'utilisateur ne doit pas modifier la configuration ou le matériel informatique mis à sa disposition (désactiver les logiciels anti-virus, réparation de matériel par l'utilisateur...).

J'utilise la messagerie et j'engage ma responsabilité

Le message électronique est un écrit qui engage la responsabilité de son auteur et éventuellement celle de l'établissement.
Il peut être reconnu pour établir un fait ou un acte juridique.

Je m'engage à utiliser internet dans un cadre professionnel

Chaque utilisateur accédant à Internet s'engage à consulter uniquement des sites licites, et dans un cadre professionnel.

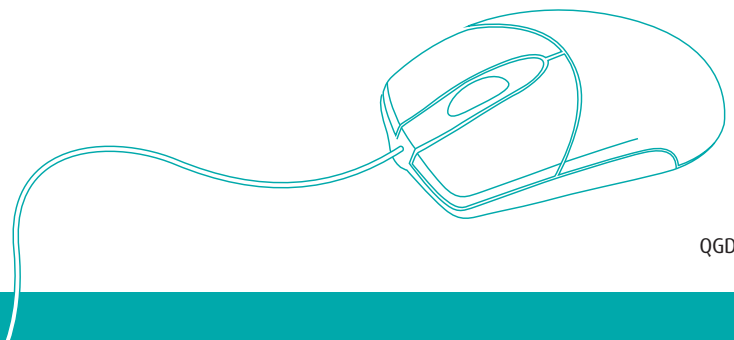
Je suis informé que des dispositifs de trace sont mis en place

L'utilisateur est informé que des dispositifs de trace et de contrôle sont mis en place, dans le respect de la législation en matière de confidentialité et de vie privée des utilisateurs.
Ces contrôles constituent un traitement automatisé d'informations directement ou indirectement nominatives et font l'objet d'une déclaration à la Commission Nationale Informatique et Libertés (CNIL) avant leur mise en œuvre.

Je signale tout incident de sécurité

Tout événement remettant en cause la sécurité du système d'information de l'établissement doit être immédiatement signalé par l'utilisateur auprès de la direction du système d'information.

L'établissement met en place et à disposition des utilisateurs, des procédures pour répondre aux besoins de sécurité.
Le contournement, ou la simple tentative de contournement, des dispositifs de sécurité est strictement interdit et passible de sanction.



QGDR-EQ-312

Service communication de l'EPSM de l'agglomération lilloise - Janvier 2014