Données de santé : un impératif, la sécurité

31 janvier 2013

Assurer la sécurité de vos fichiers c'est pouvoir garantir, à vos patients la confidentialité des données qui y figurent et disposer, en permanence, d'un outil de travail fiable.

Il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées surtout s'il s'agit d'informations couvertes par le secret médical.
La CNIL préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite de l'ordinateur, de sa configuration, de l'existence d'une connexion à Internet... (voir les recommandations de sécurité pour les applications fonctionnant en réseau) et recommande de chiffrer les données figurant sur votre disque dur et sur vos supports de sauvegarde.

Les précautions élémentaires :

- **Protégez l'accès à l'ordinateur**, au système d'exploitation et aux applications par des mots de passe individuels, propres à chaque utilisateur. Le mot de passe choisi doit, si possible, être alphanumérique, d'une longueur de 6 caractères au moins, pas trop courant (évitez initiales, nom, prénom, etc.), changé périodiquement et conservé confidentiellement.

- **Ne collez pas votre code personnel sur votre carte de professionnel** de santé ni sur un autre support. Cette carte est strictement personnelle et votre responsabilité pourrait être engagée en cas d'utilisation frauduleuse de celle-ci (ex. envoi de feuilles de soins falsifiées).

- **En cas d'absence**, même temporaire, **pensez à éteindre votre ordinateur**, ou à mettre en place un écran de veille protégé par un mot de passe, et ne laissez pas votre carte de professionnel de santé dans le lecteur.

- **Utilisez des antivirus** régulièrement mis à jour et **installez un «pare-feu»** (firewall) logiciel si vous utilisez Internet. Les risques d'intrusion dans votre système informatique sont réels et peuvent conduire à l'implantation de virus ou de programmes « espions ».

- **Effectuez régulièrement des sauvegardes** sur des supports amovibles (CD-Rom, DVD, Disque dur externe...) et conservez-les dans un lieu différent de votre cabinet.

- Assurez-vous, **lors de l'achat de votre équipement** informatique, que celui-ci comporte **les dispositifs répondant à l'obligation de sécurité qui vous incombe** (ex : des disques durs amovibles se branchant sur le port USB).

- Vérifiez que **le contrat d'assistance** et de maintenance comporte une **clause de confidentialité** rappelant au fournisseur ses obligations (cf. proposition de clause type).
  Sensibilisez votre personnel à ces mesures de sécurité.

Pour les applications en réseau ...

La gestion des mots de passe

- Code utilisateur individuel distinct du nom de l'utilisateur.
- Interdiction de réutiliser les trois derniers mots de passe (blocage du système).

Modalités de connexion et de déconnexion

- Impossibilité pour les utilisateurs de se connecter à plusieurs sous le même code utilisateur et le même mot de passe.
- Indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage sur l'écran, des dates et heures de la dernière connexion sous les mêmes code utilisateur et mot de passe.

Journalisation des connexions et exploitation de ces données.

- Après plusieurs frappes (ex. trois) incorrectes successives du mot de passe (associé à un code utilisateur correct), blocage de l'accès et message demandant à l'utilisateur d'appeler le responsable du système.
- Procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné (time out).
- Utilisation dans la mesure du possible de cartes à puce ou dispositifs analogues.

La confidentialité des données

- Utilisation dans la mesure du possible du codage des données nominatives.
- Chiffrement de tout ou partie des données dans le cadre de la réglementation française et européenne en vigueur

L'intégrité des données

- Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises.
- Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données.

En cas d'architecture client-serveur

- Prendre les dispositions nécessaires pour gérer le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun : limitation au minimum du transfert de fichiers complets, limitation du volume des informations rapatriées, journalisation des requêtes au niveau du serveur.
- Restriction d'accès aux données en fonction des habilitations.
- Séparation des réseaux de gestion administrative et de suivi médical.

Connexion à Internet

- En cas de connexion d'un des serveurs du réseau à Internet, prévoir des mesures de sécurités particulières comme la séparation physique des deux réseaux, la mise en place d'un firewall ou de barrières de protection logicielles.
- Lorsque des données de santé sont transférées via Internet, il convient de recourir au chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits).

Haut de page