e-santewallonie
L'Institut wallon de la formation des prestataires de soins à la e-santé

Version – Avril 2022

# BONNES PRATIQUES DE SÉCURITÉ DES DOSSIERS PATIENT

## 1. Hébergement des données « en local »

En tant que professionnel de santé, il est important que vous preniez toutes les précautions utiles au regard des risques présentés pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Vous êtes donc invité à adopter les mesures suivantes, à justifier de leur équivalence ou du fait que leur mise en œuvre n'est pas nécessaire.

***AVEZ-VOUS PENSE A ?***

***Tout document imprimé > prévoir une déchiqueteuse***

| Catégories | Mesures |
|---|---|
| **Sensibilisation des utilisateurs (membres du personnel/ proches aidants)** | ☐ Informer et sensibilisation du personnel du cabinet accédant aux données personnelles.<br><br>☐ Pour un cabinet de groupe (mutualisant les ressources informatiques), rédiger une charte informatique et lui donner force contraignante. |
| **Authentification des utilisateurs (membres du personnel/ proches aidants)** | ☐ Définir un identifiant (« login ») et mot de passe propres à chaque utilisateurs (ils sont **strictement personnels** et ne peuvent en aucun cas être partagés)<br><br>☐ Définir une politique de mot de passe ( ! complexité du mot de passe, renouvellement du mot de passe)<br><br>☐ Authentification à double facteurs (car accès à des données sensibles) ex : mot de passe + carte d'identité, itsme.be, microsoft.com/authenticator, www.authy.com. Clé USB U2F |
| **Gestion des habilitations** | ☐ Attribuer un profil d'habilitation adapté à chaque utilisateur (distinguant notamment les données administratives des données médicales)<br><br>☐ Supprimer les permissions d'accès obsolètes<br><br>☐ Informer les utilisateurs de la mise en place d'un système de journalisation |

| | |
|---|---|
| | ☐ Informer les utilisateurs de la procédure à suivre en cas de constatation d'une violation de données à caractère personnel<br><br>☐ Suppression des scans ou fichiers laissés en partage sur le réseau |
| **Sécurisation des postes de travail** | ☐ Prévoir une procédure de verrouillage automatique de la session informatique (après 20 min maximum d'inactivité)<br><br>☐ Permettre la mise à jour régulière des antivirus<br><br>☐ Recueillir l'accord de l'utilisateur avant toute intervention sur son poste de travail<br><br>☐ Limiter le stockage d'informations d'ordre médical sur une tablette ou un GSM (en raison des conséquences pour les patients en as de vol ou de perte de matériel). Si ces équipements sont utilisés, leur niveau de sécurisation des données doit être équivalent à celui de votre ordinateur (chiffrement, code d'accès, etc.)<br><br>☐ Exiger un code secret pour le déverrouillage des GSM ou des tablettes.<br><br>☐ Protéger les écrans des regards indiscrets (orientation, filtres optiques de confidentialité)<br><br>☐ Limiter l'utilisation de supports de stockage amovibles (clés USB, disques durs externes) et chiffrer systématiquement les données sensibles (données de santé) qui y sont conservées.<br><br>☐ Distinguer l'usage privé de l'usage professionnel de vos GSM et tablettes. Les GSM, tablettes professionnels ne peuvent pas être prêtés. |
| **Protection du réseau informatique interne du cabinet** | ☐ Limiter les connexions d'appareils non professionnels sur le réseau<br><br>☐ ISOLER/distinguer LE RESEAU WIFI INVITES DU RESEAU PRO |
| **Sécurisation des serveurs** | ☐ Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées<br><br>☐ Permettre l'installation sans délai des mises à jour critiques |
| **Sauvegardes et continuité d'activité** | ☐ Effectuer ou permettre l'exécution des sauvegardes régulières<br><br>☐ Stocker les supports de sauvegarde dans un endroit sûr<br><br>☐ Vérifier l'intégrité des sauvegardes (scénario de restauration complet) |

Version – Avril 2022

| | |
|---|---|
| **Archivage des données sécurisé** | ☐ Archiver de manière sécurisée en mettant en place des modalités d'accès spécifiques aux données archivées<br><br>☐ Détruire les archives obsolètes de manière sécurisée |
| **Maintenance et destruction des données** | ☐ Enregistrer les interventions de maintenance dans une main courante<br><br>☐ Encadrer par un responsable du cabinet les interventions par des tiers<br><br>☐ Effacer les données de tout matériel avant sa mise au rebut |
| **Sous-traitance** | ☐ Prévoir des clauses spécifiques dans les contrats des sous-traitants (mise à disposition de tous les mots de passe, pas de rétention par le sous-traitant pour un éventuel changement de prestataire à tout moment)<br>☐ Prévoir des conditions de restitution et de destruction des données<br>☐ S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)<br><br>☐ Assurer un plan de continuité en cas de panne internet |
| **Transmission sécurisée avec d'autres professionnels de santé et aves les patients** | ☐ S'assurer qu'il s'agit bien du bon destinataire<br><br>☐ Utiliser une messagerie électronique sécurisée de santé pour les échanges entre professionnels de santé<br><br>☐ Pour les échanges avec d'autres professionnels intervenant dans la prise en charge du patient ou avec les patients eux-mêmes :<br><br>• procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard et transmettre le secret par un envoi distinct et via un canal différent ;<br>• utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ;<br>• choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes. |

Version – Avril 2022

## 2. Hébergement dans le « cloud »

En cas d'externalisation de l'hébergement des données, les prestataires de service chargés de développer, d'assurer la maintenance du logiciel et des postes de travail gérant les « dossiers patients » ou proposant une plateforme de rendez-vous sont invités à adopter les mesures suivantes, sous le contrôle du responsable de traitement (vous).

***AVEZ-VOUS PENSE A ?***

| Catégories | Mesures |
|---|---|
| **Sensibilisation des utilisateurs (membres du personnel/ proches aidants)** | ☐ Informer et sensibilisation du personnel du cabinet accédant aux données personnelles<br><br>☐ Pour un cabinet de groupe (mutualisant les ressources informatiques), rédiger une charte informatique et lui donner force contraignante. |
| **Authentification des utilisateurs (membres du personnel/ proches aidants)** | ☐ Définir un identifiant (« login ») propre à chaque utilisateur<br><br>☐ Définir une politique de mot de passe ( ! complexité du mot de passe, renouvellement du mot de passe)<br><br>☐ Authentification à double facteurs (car accès à des données sensibles) ex : mot de passe + carte d'identité, itsme.be, microsoft.com/authenticator, www.authy.com |
| **Gestion des habilitations** | ☐ Intégrer des profils d'habilitation distinguant notamment les données administratives et les données médicales<br><br>☐ Supprimer les permissions d'accès obsolètes et réaliser une revue annuelle des habilitations<br><br>☐ Limiter la diffusion des documents papier contenant des données de santé aux personnes ayant besoin d'en disposer dans le cadre de leur activité. |
| **Traçage des accès et gestion des incidents** | ☐ Prévoir un système de journalisation<br><br>☐ Informer les utilisateurs de la mise en place du système de journalisation<br><br>☐ Protéger les équipements de journalisation et les informations journalisées<br><br>☐ Définir une procédure pour les déclarations de violation de données à caractère personnel |
| **Sécurisation des postes de travail** | ☐ Prévoir une procédure de verrouillage automatique de la session informatique |

Version – Avril 2022

| | |
|---|---|
| | ☐ Mettre en œuvre des antivirus régulièrement mis à jour<br><br>☐ Installer un « pare-feu » (« firewall ») logiciel<br><br>☐ Chiffrer les données stockées<br><br>☐ Recueillir l'accord de l'utilisateur avant toute intervention sur son poste |
| **Sécurisation des dispositifs mobiles** | ☐ Pour l'accès à distance aux dossiers patients, respecter les référentiels d'interopérabilité et de sécurité<br><br>☐ Protéger les écrans des regards indiscrets<br><br>☐ Limiter l'utilisation de supports de stockage amovibles (clés USB, disques dur externe) et chiffrer systématiquement les données sensibles qui y sont conservées<br><br>☐ Prévoir des mesures de sauvegarde et de synchronisation régulière des données |
| **Protection du réseau informatique interne** | ☐ Limiter les flux réseau au strict nécessaire (bloquer les protocoles et ports qui ne sont pas utilisés)<br><br>☐ Limiter les connexions d'appareils non professionnels sur le réseau<br><br>☐ Sécuriser les accès distants des appareils informatiques nomades par un VPN<br><br>☐ Mettre en œuvre le protocole WPA3 ou WPA2-PSK pour les réseaux Wi-Fi |
| **Sécurisation des serveurs** | ☐ Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées<br><br>☐ Chiffrer les données stockées<br><br>☐ Installer sans délai les mises à jour critiques<br><br>☐ Assurer la disponibilité des données |
| **Sécurisation des sites web** | ☐ Utiliser le protocole TLS et vérifier sa mise en œuvre<br><br>☐ Vérifier qu'aucun mot de passe ou identifiant n'est incorporé aux URL<br><br>☐ Mot de passe complexes pour les accès FTP et base de données SQL |
| **Sauvegardes et continuité d'activité** | ☐ Prévoir des sauvegardes régulières<br><br>☐ Prévoir le stockage des supports de sauvegarde dans un endroit sûr |

| | |
|---|---|
| | ☐ Prévoir des moyens de sécurité pour le convoyage des sauvegardes le cas échéant<br><br>☐ Prévoir et tester régulièrement la continuité d'activité |
| **Archivage des données sécurisé** | ☐ Mettre en œuvre des modalités d'accès spécifiques aux données archivées<br><br>☐ Détruire les archives obsolètes de manière sécurisée |
| **Maintenance et destruction des données** | ☐ Enregistrer les interventions de maintenance dans une main courante<br><br>☐ Effacer les données de tout matériel avant sa mise au rebut |
| **Sous-traitance** | ☐ Prévoir des clauses spécifiques dans les contrats des sous-traitants<br>☐ Prévoir des conditions de restitution et de destruction des données<br>☐ S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.) |
| **Transmission sécurisée avec d'autres professionnels de santé et aves les patients** | ☐ S'assurer qu'il s'agit bien du bon destinataire<br><br>☐ Utiliser une messagerie électronique sécurisée de santé pour les échanges entre professionnels de santé<br><br>☐ Pour les échanges avec d'autres professionnels intervenant dans la prise en charge du patient ou avec les patients eux-mêmes :<br><br>• procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard[9] et transmettre le secret par un envoi distinct et via un canal différent ;<br>• utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ;<br>• choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes. |
| **Encadrement des développements informatiques** | ☐ Proposer par défaut des paramètres respectueux de la vie privée aux utilisateurs finaux<br><br>☐ Eviter les zones de commentaires libres ou les encadrer strictement<br><br>☐ Tester sur des données fictives ou anonymisées (et non pas seulement pseudonymisées) |
| **Utilisation de fonctions cryptographiques** | ☐ Utiliser des algorithmes, des logiciels et des bibliothèques reconnus<br><br>☐ Conserver les secrets et les clés cryptographiques de manière sécurisée |

e-santewallonie

L'Institut wallon de la formation des prestataires de soins à la e-santé

Version – Avril 2022