

FICHE RÉFLEXE

GESTION DES DONNÉES PATIENTS



Les données de santé sont extrêmement sensibles et couvertes par le secret médical (diagnostic, histoire personnelle...). Chaque employé est tenu légalement et « éthiquement » de protéger la confidentialité des informations patients. C'est pourquoi il faut appliquer les bonnes pratiques suivantes !

#1

GESTION DES ACCÈS AUX DOSSIERS MÉDICAUX NUMÉRIQUES (DPI)

- **Consultez uniquement les dossiers des patients sous votre responsabilité** ou pour lesquels vous avez une autorisation explicite. Les dossiers médicaux informatisés ne doivent être accessibles qu'aux personnes ayant besoin d'en prendre connaissance pour leur mission.
- **Utilisez vos propres accès** pour consulter les données, et en aucun cas ceux d'un collègue. Ne prêtez pas vos identifiants. Le système hospitalier est configuré pour que chaque rôle n'ait accès qu'aux données nécessaires à son activité.
- **Se déconnecter systématiquement** après utilisation du DPI



Sachez que les accès au DPI sont systématiquement contrôlés et tracés. Cette traçabilité protège les patients et les professionnels en décourageant les consultations inappropriées. Protéger la confidentialité, c'est aussi éviter des sanctions disciplinaires ou pénales liées à un accès illégitime.

#2

ANONYMISATION ET PSEUDONYMISATION DES DONNÉES SENSIBLES

- Utiliser des pseudonymes pour les recherches médicales
- Supprimer les données non nécessaires avant de partager des dossiers
- Utiliser des outils approuvés par l'hôpital pour sécuriser l'envoi de données sensibles (Nextcloud / MSSanté)
- Évitez d'évoquer des informations pouvant identifier un patient dans des conversations non sécurisées (téléphone personnel, espaces publics, couloirs...)

#3

SÉCURISATION DES IMPRESSIONS ET DES DOCUMENTS SENSIBLES

- Effectuer une impression sécurisée si nécessaire (nécessite une authentification par code PIN ou par badge)
- Ramassez immédiatement les impressions/documents médicaux après utilisation pour ne pas les laisser accessibles à tous
- Stockez les dossiers papiers dans des armoires verrouillées.
- Détruisez les documents contenant des données patients dans un broyeur (ou directement dans une poubelle dédié) une fois traités.

#4

ARCHIVAGE ET SAUVEGARDE

- Conservez les documents au format numérique si possible, dans les partages sécurisés.
- Ne pas copier ou conserver des fichiers contenant des données patients sur un support personnel (ex : clé USB, smartphone).

SIGNALEZ IMMÉDIATEMENT

- Une tentative suspecte d'accès à un dossier patient.
- Toute perte de documents sensibles (liste de patients, compte-rendu psychiatrique...).



Avertir le service informatique
1017 ou 05 55 43 10 17



Ou nous contacter sur
informatique@ch-esquirol-limoges.fr