# MÉMO

## M20. LA PROTECTION DES DONNÉES DE SANTÉ

## Les Données de Santé à Protéger :

Les données de santé sont considérées comme des « **données personnelles sensibles** » et dont l'utilisation est très encadrée .

Conformément au RGPD, les données à caractère personnel concernant la santé sont les données se rapportant à l'état de santé physique ou mental passé, présent ou futur, d'une personne physique (y compris la prestation de services de soins de santé).

Elles regroupent notamment :

- Les **données à caractère personnel relatives à la santé des personnes** telles que les traitements en cours, pathologies, les données recueillies à l'occasion des activités de prévention ou de diagnostic, etc.
- Toutes autres **informations venues à la connaissance du professionnel de santé et permettant de révéler des informations sur l'état de santé du patient .**

**Important : la protection des données s'applique aux données dématérialisées (informatiques) mais également à toutes les données matérielles (copies d'ordonnances par exemple).**

## Protection :

Il appartient à l'officine de garantir le respect de la confidentialité et de la sécurité de ces données :

- **Le pharmacien titulaire est responsable des données de santé utilisées et stockées au sein de son officine.**
- **Le patient dont les données personnelles sont collectées** a notamment le droit d'exiger de **connaître les informations stockées le concernant**, de **demander qu'elles lui soient remises**, qu'elles soient **rectifiées** si besoin, et sous certaines conditions, **peut s'opposer à la collecte et aux traitements des données le concernant** (sauf les données dont la collecte est obligatoire telles que les données nécessaires pour la prise en charge des frais de santé par l'assurance maladie) et demander l'**effacement** de ses données.

## Réglementation Général pour la Protection des Données (RGPD) :

**Au titre de la protection des données, toute collecte ou traitement de données personnelles doit se faire en conformité avec le RGPD** (cf. site de l'Ordre) et avec la Loi informatique et libertés du 6 janvier 1978 modifiée.

Jusqu'à présent, le titulaire d'officine pouvait s'engager auprès de la CNIL à être en conformité à la norme simplifiée 52 pour la gestion des données de son officine incluant les données de ses patients.
Depuis le 25 mai 2018, la norme simplifiée 52 a été supprimée. Le titulaire d'officine n'a plus de déclaration à effectuer sur le site de la CNIL, mais il doit toujours être en mesure de démontrer qu'il respecte les principes de protection des données énoncés dans la norme simplifiée 52, jusqu'à ce qu'elle soit transformée en référentiel par la CNIL.

## L'Utilisation des Données de Santé :

- **Traiter les données de manière licite, loyale et transparente** au regard des patients en les informant des règles d'exercice de leurs droits
- **Respecter les principes de finalité et de conserver uniquement les données indispensables** pour le bon suivi des patients
- **Ne conserver les données des patients que pendant la durée nécessaire** à la réalisation de l'objectif ayant conduit à la collecte de ces données
- Collecter des données exactes et, si nécessaire, tenues à jour
- Utiliser, si possible, une **messagerie sécurisée** (cf. verso)

# MÉMO

## M20. LA PROTECTION DES DONNÉES DE SANTÉ

### Le stockage sécurisé des informations

L'officine doit sécuriser les données dématérialisées et les données sur support papier.

Pour les données dématérialisées, l'officine doit :

- **Sécuriser les données** (chiffrement par l'utilisation par exemple de la carte CPS , authentification par mot de passe robuste, contrôle des accès via un historique…)
- **Sécuriser le réseau** (pare-feu, antivirus)
- **Recourir à un hébergeur agréé** (en cas d'externalisation des données) qui garantit la protection des données
- **Informer et former les collaborateurs aux règles à respecter pour protéger les données** (sites sensibles, accès aux mots de passe, outils de transmission...)

L'officine doit également **protéger les données de santé sur support papiers** en ayant recours à des **moyens de destruction appropriés** (broyeur par ex.) et **en étant vigilant concernant leur conservation à l'officine** (ne pas laisser trainer des copies d'ordonnance sur le comptoir par ex.)

**Identifier & prévenir les risques :**

1. Recenser les fichiers contenant des données à protéger
2. Identifier les supports de stockage (matériels, logiciels, canaux de transmission…)
3. Déterminer les risques (violation, détérioration, perte…)
4. Déterminer les mesures de sécurité

### Les Sauvegardes & Archivages

**Les sauvegardes** dupliquent les données du système informatique afin de les restituer en cas d'incident.

- Systématiser les **sauvegardes**
- Utiliser des **supports préservant l'intégrité des données** (disques durs, mémoires flash...)
- **Tester la restitution des données à partir des sauvegardes**
- Sécuriser les lieux de conservation des sauvegardes

**L'archivage** est une sauvegarde des données visant à garantir leur conservation à long terme.

- Définir les accès autorisés mise en place d'une politique d'habilitation
- **Détruire les archives après la période** obligatoire de conservation de manière à les rendre inexploitables
- Sécuriser les archivages

### La transmission des données (messagerie sécurisée)

Dans le cas d'une transmission entre professionnels de santé (l'officine et un cabinet de médecin par exemple), le pharmacien doit utiliser un service de messagerie sécurisé de santé conforme aux exigences de la loi :

- Disposer d'une messagerie qui garantit l'identification de l'émetteur et du destinataire (numéro RPPS)
- Utiliser un système d'authentification forte : CPS ou dispositif équivalent
- Assurer la sécurité des messages et des pièces jointes par le recours à des moyens de chiffrement
- Conserver sous une forme sécurisée les messages et les pièces jointes pour en assurer la disponibilité, l'intégrité et la traçabilité.

**Références :**
Quelles obligations pour les titulaires d'officine (ONP)

Pharmacie :