La sécurité et la confidentialité des données de santé, quelles obligations ?

Les données de santé sont considérées comme sensibles, donc soumises à un haut niveau de sécurité, physique, logique et organisationnelle (Voir notre Fiche « ***Qu'est-ce qu'une donnée de santé ?*** »).

Références textuelles en matière de sécurité et de confidentialité des données personnelles :

- **Règlement européen relatif à la protection des données personnelles du 27 avril 2016** (RGPD) : les données doivent être traitées de façon à garantir leur **sécurité** et leur protection contre le **traitement non autorisé ou illicite** et contre la **perte**, la **destruction** ou les **dégâts accidentels**.
- **Directive européenne Network and Information Security (NIS) du 6 juillet 2016** visant à assurer dans l'UE un **niveau élevé et commun de sécurité** des réseaux et des systèmes d'information.
- **Article 34 de la loi Informatique et Libertés** (LIL) : le responsable de traitement (RT) doit prendre **toutes les précautions utiles** pour préserver la sécurité des données et empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Si l'obligation de sécurité est généralement de moyens, elle peut tendre vers une **obligation de résultat** selon la nature des données traitées, les risques encourus par les personnes, les moyens humains, matériels et financiers dont dispose le RT pour assurer la sécurité de ses systèmes d'information.

Les obligations de sécurité et de confidentialité

✓ Les étapes de sécurisation du traitement au regard du Règlement européen

1- Analyse d'impact relative à la protection des données [Article 35 RGPD]

Le RT qui souhaite mettre en œuvre un nouveau traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (tels que la destruction, la perte ou l'altération, la divulgation ou l'accès non autorisés des données traitées, de manière accidentelle ou illicite), doit réaliser au préalable une **auto-évaluation des risques** que présente son projet (Voir notre Fiche ***« Le principe d'accountability et ses conséquences en matière de santé »***).

2- Mesures techniques et organisationnelles [Article 32.1 RGPD]

En pratique, le RT et le sous-traitant doivent mettre en œuvre les **mesures physiques, logiques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque, telles que :

- **Contrôle de l'accès aux locaux** hébergeant les serveurs (procédure d'habilitation pour restreindre l'accès aux seules personnes habilitées, badges d'accès) ;
- Protection des serveurs par **des firewalls, filtres anti-spam et anti-virus** ;
- **Mots de passe** des postes de travail répondant à des exigences de sécurité (caractères spéciaux, nombre de caractères imposés, etc.) et régulièrement mis à jour ;
- **Pseudonymisation** (mécanisme masquant l'identité réelle de l'utilisateur en y associant un pseudonyme) et **chiffrement** (les données chiffrées n'apparaîtront sous leur forme d'origine que si elles sont déchiffrées à l'aide de la bonne clé) ;
- Procédure visant à **tester, à analyser et à évaluer régulièrement** l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- **Formation du personnel** aux mesures à mettre en place pour assurer la sécurité ;
- Adoption d'une **charte informatique** ;
- Mesures techniques permettant de **rétablir la disponibilité** des données et l'accès à celles-ci dans des **délais appropriés** en cas d'incident physique ou technique.

NB : L'absence de mesures de sécurité ou la négligence dans le déploiement de ces mesures sont sanctionnées pénalement (jusqu'à 5 ans de prison et 300 000 € d'amende[1]).

3- Registre des activités de traitement [Article 30.1.g RGPD]

Chaque RT tient un **registre des activités de traitement**, qui comporte notamment une description générale des mesures de sécurité techniques et organisationnelles précitées.

✓ Obligations de sécurité et de confidentialité pesant sur le professionnel de santé

Les professionnels de santé, ainsi que ceux intervenant dans le système de santé, sont soumis au **secret médical**[2]. La violation du secret médical est punie d'1 an de prison et 15 000 € d'amende.

Ils doivent également respecter des référentiels de sécurité mis en place par le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS).

Il est recommandé aux directeurs d'établissements de santé de sensibiliser leur personnel aux bonnes pratiques à adopter (formation à la sécurité informatique, adoption d'une charte informatique).

✓ Obligations de sécurité et de confidentialité pesant sur le sous-traitant en matière de santé

L'**article 35 de la LIL** oblige le sous-traitant à présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34 (charge de la preuve pesant sur le RT). Le contrat conclu entre le sous-traitant et le professionnel de santé doit détailler les obligations du sous-traitant et prévoir qu'il ne peut agir que sur instruction du RT.

*En cas d'**hébergement de données de santé par un tiers**, le professionnel ou l'établissement de santé devra s'assurer que le prestataire est agréé[3]. L'obtention de l'agrément est soumise à la mise en œuvre de mesures assurant la sécurité des données, et d'une **politique de confidentialité et de sécurité.** Les hébergeurs de données de santé sont soumis au **secret professionnel**.*

Failles de sécurité : quelles conséquences ?

Le RGPD prévoit une obligation du RT de notifier aux autorités (si possible dans un **délai de 72h au plus tard** après en avoir pris connaissance) et aux personnes concernées les failles de sécurité impactant les données traitées. [Articles 33 et 34 RGPD].

Cependant, pour les individus, seules les violations de données susceptibles de les exposer à un **risque élevé** doivent leurs être notifiées. Ainsi, cette notification n'est pas nécessaire si :

- Des mesures de protection techniques et organisationnelles appropriées, telles que le chiffrement, ont été prises ;
- Des mesures ultérieures garantissent que le risque n'est plus susceptible de se matérialiser ;
- La communication exige des efforts disproportionnés.

Le sous-traitant doit notifier toute faille de sécurité au RT.

[1] Article 226-17 du code pénal.
[2] Article L.1110-4 du code de la santé publique.
[3] Articles L. 1111- et R. 1111-9 du code de la santé publique.

La Loi de modernisation de notre système de santé[4] instaure une ***obligation de notification pour les établissements de santé, sans délai, à l'agence régionale de santé,*** *en cas d'incidents grave de sécurité des systèmes d'information[5].*

Le rôle joué par la soft law

L'application d'un code de conduite ou d'un mécanisme de certification approuvé peut servir à **démontrer la conformité aux exigences du devoir de sécurité**[6]. [Section 5 RGPD].

La CNIL délivre également des labels à des produits et procédures permettant d'identifier ceux qui garantissent un haut niveau de protection des données. De même, l'ANSSI peut certifier le niveau de sécurité de matériels et logiciels en s'appuyant sur des tests d'intrusion.

Enfin, des **normes ISO** pour la sécurité numérique, telles que la série ISO/CEI 27000[7], fournissent un cadre pour la protection de la vie privée et la gestion des incidents.

[4] Loi n°2016-1214 du 26 janvier 2016 de modernisation de notre système de santé.
[5] Article L. 1111-8-2 du code de la santé publique.
[6] Article 32.3 du Règlement européen du 27 avril 2016 relatif à la protection des données à caractère personnel.
[7] Norme ISO/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Vue d'ensemble et vocabulaire*, Mai 2009 (révisée en 2012).