Fiche 2.

Le dossier patient

Check-list des bonnes pratiques à respecter :

→ Je recueille le consentement de mon patient pour l'échange électronique et sécurisé de ses données avec d'autres professionnels de la santé (*ex : RSW*) ;

→ Je collecte seules les données qui strictement nécessaires à la tenue du dossier patient ;

→ Je conserve les données de mes patients conformément à mes obligations légales et supprime toute information ayant dépassé la durée de conservation préconisée ;

→ J'informe mes patients et m'assure du respect de leurs droits (Téléchargez vite votre affiche sur www.e-santewallonie.be) ;

→ Je prends toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données ;

→ Je mets en place des mesures de sécurité adéquates pour la protection des données de mes patients ;

→ Je veille à conclure un contrat de sous-traitance avec les prestataires de service ;

→ Je notifie à l'autorité de protection des données et aux personnes concernées toute violation de données.

Version du 16 novembre 2018

Que vous utilisiez, dans le cadre de votre activité professionnelle, un **logiciel métier** fourni par un prestataire informatique ou que vous teniez vos dossiers patients sous **format papier**, ces dossiers contiennent nécessairement des **données personnelles** sur vos patients et sur les professionnels de la santé qui interviennent dans leur suivi.

Au sens du RGPD, vous êtes considéré comme « **responsable de traitement** ». A ce titre, vous devez vous assurer de **la conformité de vos dossiers patients avec cette nouvelle réglementation.**

Devez-vous recueillir le consentement de vos patients ?

Vous n'avez **PAS** **besoin de recueillir le consentement de vos patients pour collecter et conserver des données de santé** les concernant dans la mesure où leur collecte et leur conservation sont nécessaires pour exercer votre activité de prévention, de diagnostics médicaux et de soins.

Le **consentement** du patient a toutefois vocation à s'appliquer dans le cadre d'**un partage électronique et sécurisé des données de santé entre professionnels de la santé soumis au secret professionnel**. Aucun partage de données de santé ne pourra s'effectuer au travers du Réseau Santé Wallon sans avoir préalablement recueilli le consentement du patient.

Si vous réalisez ou participez à des **recherches scientifiques ou études épidémiologiques**, destinées à mieux comprendre et à lutter contre différents problèmes de santé, vous devez également obtenir le **consentement** de vos patients.

Quelles sont vos obligations ?

Vous devez vous assurer que vos dossiers patients respectent bien les principes directeurs du RGPD[1].

1. Vos dossiers patients (papiers ou logiciel métier) doivent répondre à des finalités déterminées, explicites et légitimes.

Les données personnelles que vous collectez sur votre patient sont utilisées et enregistrées dans son dossier patient en vue d'exercer **votre activité de prévention, de diagnostics, de soins et servent à la gestion de votre cabinet**. De manière générale, elles répondent aux besoins d'une prise en charge optimale de la santé de votre patient.

Il s'agit plus particulièrement de permettre :

- la **gestion des rendez-vous** ;
- la **création et la gestion des dossiers administratifs** ;
- la **création et la gestion des dossiers santé** ;

[1] Article 5 du RGPD.

- la **production de documents de santé** ;
- la **demande d'examens et interventions complémentaires** ;
- la **prescription de médicaments et de soins** ;
- la **facturation de soins** ;
- l'**échange d'informations avec des destinataires ciblés** ;
- le **suivi des soins** avec l'ensemble des acteurs de santé ;
- l'**étude épidémiologique** et l'établissement de **protocole de recherches cliniques**.

Dans le cadre d'un cabinet de groupe tel qu'une maison médicale, les données du patient sont également utilisées par toute ou partie de l'équipe pluridisciplinaire dans le respect du secret professionnel en vue d'adopter une **approche globale coordonnée intégrant soins, démarches préventives de santé et suivi médico-social.**

Toute autre utilisation des données doit être réalisée avec une grande précaution. En particulier, **toute utilisation personnelle ou commerciale des dossiers de vos patients est naturellement prohibée.**

2. Les données que vous collectez doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostics et de soins.

Toutes les informations que votre patient a pu vous révéler dans le cadre de vos échanges ne doivent pas nécessairement être inscrites dans son dossier. **Seules les données qui sont strictement nécessaires au suivi de votre patient peuvent être enregistrées et conservées.**

Dans le cadre de votre mission de soins, il est légitime que vous collectiez certaines catégories de données personnelles, notamment :

- Les **données d'identification** : nom, prénom, NISS, registre national, date de naissance, adresse, numéro de téléphone, email.
- Les **données de santé** : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale, numéro de nomenclature des prestations et tout autre élément de nature à caractériser la santé de votre patient et considéré comme pertinent.
- Les **données d'assurabilité** : assuré bénéficiant d'un BIM, assuré obligatoire, inscription dans une maison médicale au forfait, etc.
- **Selon les contextes** : particularités financières, loisirs et intérêts, habitudes de vie et de consommation, profession et emploi, contexte familial…

Toute information qui serait sans lien avec l'objet du suivi de la santé de votre patient ou qui ne serait pas indispensable au diagnostic ou à la délivrance des soins **doit être exclue**. Par exemple, vous ne devez pas inscrire des informations sur la vie privée du patient qui ne sont pas médicalement nécessaires (*ex : religion du patient, orientation sexuelle, etc*.).

3. Les données que vous collectez sur vos patients doivent être conservées pour une durée qui n'excède pas la durée nécessaire à l'utilisation que vous en faites.

Les données que vous collectez sur vos patients doivent être conservées **pour une durée déterminée**. A titre d'exemple, les médecins sont, conformément à l'article 24 du Code de déontologie médicale, tenus de conserver les dossiers médicaux **pendant 30 ans** à compter de leur dernière consultation avec le patient.

Vous devez ensuite veiller à **supprimer toute information ayant dépassé la durée de conservation préconisée**.

4. Vous devez informer vos patients de l'existence de vos dossiers et de leurs droits à cet égard.

Vous devez **informer vos patients que leurs données personnelles sont recueillies et traitées en vue d'assurer une prise en charge optimale de leur santé** en conformité avec le RGPD. Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un dépliant au patient par exemple.

Cette information doit comporter impérativement les éléments suivants :

- les coordonnées du responsable de traitement
- les finalités y compris les finalités ultérieures (*par exemple, si un prestataire de soins souhaite utiliser ultérieurement les données à des fins de recherche*)
- les destinataires des données
- la durée de conservation
- les droits de la personne concernée : accès, rectification, effacement à certaines conditions, limitation, opposition auprès de l'autorité de protection des données

Vos patients disposent ainsi de plusieurs droits conformément au RGPD. Ils peuvent :

- accéder aux données qui les concernent
- rectifier leurs données en cas d'erreur
- s'opposer au traitement de leurs données pour des raisons tenant à leur situation particulière
- demander à effacer leurs données dans certaines situations particulières (*dossier patient conservé trop longtemps ou données non adéquates*).

Chaque demande portant sur ces droits doit être examinée dans **un délai raisonnable**. Dans le cas d'une demande d'accès, vous avez 15 jours pour présenter le dossier à votre patient, à l'exclusion des annotations personnelles (notes dissimulées à des tiers, réservées à votre usage personnel et dénuées d'intérêt pour la qualité des soins) et des données relatives aux tiers (ex. identité des proches qui ont confiés des informations à l'insu du patient)[2].

[2] Voy. à ce sujet la loi du 8 août 2002 relative aux droits du patient, *M.B.*, 6 octobre 2002, p. 43719.

5. Vous devez prendre toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données de santé.

Seules certaines personnes sont autorisées, au regard de leurs missions et en vertu de dispositions légales les y habilitant, à accéder aux données figurant dans le dossier patient.

Au regard de la nature de votre mission de soins, **vous** et, dans une certaine mesure, votre **personnel** (*ex : votre secrétaire médical*) êtes légitimement autorisés à accéder aux données figurant dans les dossiers de vos patients.

De plus, dans le cadre de votre profession, vous êtes amené (avec le consentement de votre patient) à transmettre à **d'autres professionnels** de la santé des informations concernant l'état de santé de votre patient. Vous êtes également amené à transmettre des attestations de soins aux **organismes assureurs** de votre patient afin de permettre la facturation des soins que vous avez presté.

Tous ces destinataires n'accèdent qu'aux données qui sont nécessaires à l'exercice de leur mission *(ex : le secrétaire médical accède aux données administratives permettant de gérer les prises de rendez-vous mais n'accède pas à la totalité du dossier médical)*.

En pratique, il est important de veiller au respect des règles relatives à l'échange et au partage de données entre professionnels :

- **Entre professionnels membres d'une équipe de soins**

Le travail en équipe permet de coordonner les interventions des différents prestataires pour une meilleure qualité des soins et une plus grande efficacité. Le partage d'informations entre les membres de l'équipe de soins ne peut se faire sous conditions :

1. des **informations strictement nécessaires** à la coordination ou à la continuité des soins, à la prévention ou au suivi médico-social et social du patient.

2. du **périmètre de leurs missions**.

3. dans le **respect du secret professionnel** auxquels sont assujettis les membres de l'équipe de soins.

4. sous réserve du **consentement** patient. Ce dernier doit préalablement être informé de la nature des informations susceptibles d'être échangées ou partagées et de l'identité et de la qualité du destinataire.

Bon à savoir : Le patient a le droit de s'opposer À TOUT MOMENT à un échange ou un partage d'informations le concernant.

- **Hors équipe de soins**

Le **consentement** préalable du patient est requis !

➢ **Entre médecins**

Le patient doit en être informé et ne pas s'opposer à cette transmission d'informations. **Attention** : les professionnels de la santé qui participent au parcours de santé du patient ne peuvent pas transmettre d'initiative les données de santé du patient **ni au médecin d'une compagnie d'assurances ni au médecin expert judiciaire ni au médecin du travail ni au médecin-conseil des mutualités.**

➢ **Ce qui est exclu !**

A l'heure actuelle, les données de santé deviennent des ressources prisées du monde extérieur, ce pourquoi vous pourriez être sollicités par des acteurs économiques. Assurez-vous de ne pas transmettre les données personnelles de vos patients à ces acteurs qui ne sont pas légitimement autorisés à accéder à celles-ci (*ex : compagnies d'assurance, start-up commerciales…*)

6. Vous êtes responsables de la mise en œuvre des mesures de sécurité pour garantir l'intégrité et la confidentialité des données de vos patients.

En tant que responsable du traitement des données que vous traitez dans le cadre de votre mission de soins, vous êtes tenu de respecter les règles de sécurité. Vous **devez protéger les données de vos patients contre tout accès non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.**

En ce qui concerne la sécurisation du système informatique, vous devez notamment :

- utiliser un mot de passe personnel ;
- verrouiller votre session informatique automatiquement après maximum 30 minutes d'inactivité ;
- utiliser un antivirus mis à jour régulièrement ;
- utiliser une protection « firewall » en cas de connexion à Internet ;
- faire des backup réguliers (au minimum hebdomadaire, avec conservation des backup mensuels sur 12 mois glissant) et les conserver dans un lieu différent de votre cabinet ;
- utiliser une messagerie sécurisée et cryptée telle qu'e-Hbox ;
- chiffrer les données avec un logiciel adapté ;
- et limiter les connexions sur le réseau à des appareils non professionnels.

Il est important de préciser que **vos codes secrets doivent rester strictement personnels** et ne doivent en **aucun cas être communiquer à votre personnel**. Vous pouvez par exemple mettre en place une authentification forte pour votre personnel au moyen d'un mot de passe à usage unique (identifiant, mot de passe et envoi d'un code à chaque connexion). Vous pouvez également attribuer à chacun du personnel des badges électroniques pour l'accès et la sécurisation de votre cabinet.

7. Vous devez conclure un contrat de sous-traitance avec vos prestataires de service.

Si vous passez par un prestataire de service pour la tenue et la gestion de vos dossiers patients, vous devez veillez à ce que celui-ci vous offre suffisamment de garanties en terme de protection de données et vous garantisse un niveau de sécurité adapté au risque.

En toute hypothèse, dès que vous sollicitez les services d'un prestataire de service **qui traite des données en votre nom et pour votre compte,** celui-ci est considéré comme **votre sous-traitant**. Vous devez donc formaliser la relation que vous entretenez avec lui par un contrat de sous-traitance. Ce contrat devra mentionner que le prestataire de service[3] :

- ne traite les données à caractère personnel que sur votre instruction
- veille à la signature d'engagements de confidentialité par le personnel
- prend toute les mesures de sécurité adéquates
- ne recrute pas de sous-traitant sans votre autorisation écrite préalable
- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement, notamment lorsque des patients veulent exercer leurs droits
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations
- collabore dans le cadre d'audits.

Si vous conservez encore vos dossiers patients **sous format papier**, vous devez également vous assurez de leur sécurité : **locaux sécurisés, armoires contenant les dossiers fermées à clé...**

Que devez-vous faire en cas de violation de données ?

En cas de violation de données (destruction, perte, altération, divulgation ou accès non autorisé), vous devez avoir les réflexes suivants :

1) **Analyser, dans la mesure du possible, l'étendue de la fuite des données afin d'identifier les démarches à accomplir et éviter que cet incident se reproduise** : Qui a eu accès aux données ? Quelle est l'origine de la fuite des données ? Les données ont-elles été envoyées à un tiers ? Des données de santé sont-elles concernées ? Quelles mesures auraient pu empêcher l'événement et quelles mesures peuvent en atténuer les conséquences ?

2) S'il existe un risque pour les droits et libertés des personnes, **vous devez notifier la violation de données en question à l'Autorité de Protection des Données** (APD) – ex-commission vie privée – dans les meilleurs délais et, si possible, 72 heures après avoir eu connaissance de l'incident.

[3] Article 28 du RGPD.

Cette notification doit contenir les éléments suivants[4] :

- la nature de la violation
- les catégories et le nombre approximatif de personnes concernées
- les catégories et le nombre approximatif d'enregistrements des données
- le nom et les coordonnées de la personne de contact de votre cabinet
- les conséquences probables de la violation de données
- les mesures prises ou à prendre pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

3) Si la violation des données engendre un **risque élevé** pour les droits et libertés des personnes concernées, vous devez **informer la personne concernée de cette violation et ce dans les meilleurs délais**[5].

4) Vous devez **documenter cette violation de données à caractère personnel**. Une inscription peut se faire dans un registre spécifique, un tableau récapitulatif des incidents ou même au sein du registre des activités de traitement.

5) De préférence, veillez à **contacter**, le plus rapidement possible, **votre assurance de responsabilité professionnelle** pour l'informer de l'incident.

Pouvez-vous être sanctionné ?

Si vous ne respectez pas les grands principes du RGPD, vous pouvez faire l'objet d'une **sanction administrative** de l'APD, voire d'une **sanction pénale**[6].

Il est donc impératif de vous mettre en conformité avec la réglementation et de **documenter cette conformité** (tenue d'un registre des activités de traitement, traçabilité des violations de données, politique de confidentialité, devoir d'information, respect des droits des personnes concernées, contrats de sous-traitance, etc.).

Par Emeraude Camberlin, Juriste.

[4] Article 33 du RGPD.
[5] Article 34 du RGPD.
[6] Article 83 du RGPD : En fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.