DPO Consulting
Your personal data protection officer

sfmp
société française de médecine polyvalente

RGPD : ce qu'un médecin hospitalier doit savoir

25 février 2021

Maurice Monnot

De quoi parle-t-on ?

Quelques définitions

Données Personnelles	**Toute information** se rapportant à une **personne physique** et permettant de l'identifier **directement** ou **indirectement** • Peu importe que l'information relève de la sphère privée ou professionnelle • Il s'agit par exemple du nom de vos patients, de leurs coordonnées, de leur vie personnelle (nombre d'enfants…) ou encore de toute informations relatives à leur santé (pathologie, diagnostic, prescriptions…)
Catégories particulières de données (données sensibles)	**Toute donnée personnelle relative aux sujets suivants :** ▪ **Les données de santé**, génétiques et biométriques ▪ L'orientation sexuelle ▪ Les données personnelles relatives aux condamnations pénales et aux infractions ▪ Les opinions syndicales, philosophiques et religieuses ▪ Les données perçues comme sensibles par les personnes concernées : numéro de sécurité sociale, etc.
Traitement de données personnelles	**Toute opération (informatisée ou non) effectuée sur des données** telle que la collecte, l'analyse, la consultation, la mise à disposition, la collecte, le transfert à des confrères, la conservation dans le dossier patients, l'effacement.
Responsable de traitement	**Organisme qui définit les finalités du traitement et les moyens essentiels utilisés** (votre hôpital de rattachement ou un ou plusieurs organismes conjointement responsables) : ▪ Les finalités de traitement sont les objectifs du traitement : pour quelles raisons traite-t-on les données ? ▪ Les moyens de traitement sont les mesures mises en œuvre (comment le traitement est mis en œuvre) : quelles personnes sont concernées, quelles données doivent être collectées, combien de temps sont-elles conservées, où les données sont-elles stockées et qui peut y accéder…
Sous-traitant	**Les organismes qui participent à la mise en œuvre du traitement pour le compte du responsable de traitement**, par ex. un prestataire informatique, un gestionnaire de rendez-vous, un prestataire de télémédecine ▪ Le sous-traitant doit se conformer aux instructions et exigences du responsable de traitement ▪ Le sous-traitant partage la responsabilité avec le responsable de traitement en cas de violation de sa part de ses obligations légales et contractuelles

De quoi parle-t-on ?

Principes fondamentaux

Finalités déterminées, licites et légitimes	**Les données sont traitées pour des finalités définies.** Vous devez avoir identifié de manière précise les finalités pour lesquelles vous collectez et traitez les données (par ex. recherche, tenue des dossiers médicaux, recours à la télémédecine, établissement et télétransmission des feuilles de soins). Chaque finalité doit reposer sur l'une des bases légales fixées par le RGPD (par ex. l'obligation légale pour la tenue du dossier médical ou les transmissions à l'assurance maladie).
Minimisation et pertinence de la donnée	**Les données doivent être adéquates, pertinente et non excessives au regard de la finalité pour laquelle elles sont traitées.** Vous devez identifier de manière précise les données dont vous avez besoin pour achever vos objectifs (par ex. ne collecter des informations sur la vie familiale, religieuse ou sexuelle du patient que si cela est indispensable au diagnostic ou à la prescription de médicaments).
Conservation des données	**Les données personnelles traitées doivent être conservées pour une durée déterminée.** Vous devez vous assurer que les données personnelles sont supprimées lorsqu'elles ne sont plus nécessaires afin de réduire le risque qu'elles deviennent inexactes ou non pertinentes, ou bien archivées pour répondre à vos obligations légales avant suppression (par ex., en principe 20 ans pour les dossiers médicaux des patients).

De quoi parle-t-on ?

Principes fondamentaux

Transparence

Les données sont traitées de manière loyale et transparente.
Vous devez avoir être transparents sur la manière dont vous prévoyez d'utiliser les données collectées auprès de vos patients et donc les informer sur les traitements mis en œuvre (tenue d'un dossier médical…) et sur leurs droits, par ex. dans le livret d'accueil ou via une affiche apposée dans les couloirs de l'hôpital.

Droit des personnes concernées

Les droits des personnes concernées sont respectés.
Vous devez définir et mettre en place les procédures internes appropriées à la gestion des droits des individus et y répondre dans les délais : droit d'accès, droit de rectifier les données, droit de s'opposer au traitement ou d'en demander la limitation, droit de suppression (par ex. pour des dossiers médicaux conservés plus de 20 ans).

Sécurité

Les données doivent être protégées contre les accès non-autorisés, la perte, la destruction ou l'altération.
Vous devez mettre en places les mesures techniques et organisationnelles adéquates pour protéger les données de vos patients ou collaborateurs. Seules certaines personnes doivent y avoir accès au regard de leurs missions (par ex. le service du secrétariat n'a accès qu'aux données nécessaires à la gestion des rendez-vous) et les accès doivent être sécurisés (mot de passe, chiffrement…) → saisir la DSI pour toute question.
En cas de violation de données, il peut être obligatoire de prévenir la CNIL et les personnes concernées.

Concrètement, que dois-je faire ?

Les étapes à suivre

1 Recenser vos traitements

Avec l'aide du Délégué à la protection des données, **recensez les traitements de données personnelles** mis en œuvre par votre service (par ex. gestion du dossier patient, dépistage prénatal, recherches).

Un registre des traitements doit être mis en place par votre établissement avec une « fiche » par activité recensée. Sont notamment précisés :

- **L'objectif poursuivi** (par ex : la gestion des rendez-vous)
- **Les catégories de données utilisées** (par ex : identité, coordonnées, données de santé – pathologie, diagnostic)
- **Qui a accès aux données** (par ex : le prestataire de télémédecine)
- **La durée de conservation** de ces données (par ex : 20 ans pour le dossier médical)
- **Les mesures de sécurité** mises en place (par ex : authentification des utilisateurs)

▶ Sanction pécuniaire de l'autorité de contrôle italienne à hauteur de 40 000 euros pour une collecte de données de santé sans base légale - 17/12/2020

La réalisation d'une **analyse d'impact** peut également être nécessaire.

Concrètement, que dois-je faire ?

Les étapes à suivre

2

Sécuriser vos traitements

Assurez-vous que des **mesures techniques et organisationnelles appropriées** sont mises en œuvre pour assurer la confidentialité et l'intégrité des données personnelles (protection des accès aux locaux, système d'authentification aux logiciels, mot de passe renforcé, etc.).

- Sanction pécuniaire de 400 000 euros à l'encontre d'un hôpital portugais pour défaut de gestion des accès au système d'information (985 profils alors que l'hôpital ne comptait que 296 médecins ; les médecins avaient accès à l'ensemble des dossiers patients quelle que soit leur spécialité) – 17/07/2018

- Sanctions pécuniaires à l'encontre de 7 hôpitaux en Suède pour un montant total de 3 850 000 euros pour absence de mesures techniques et organisationnelles (absence d'analyse de risque, accès trop larges au système d'information) – 03/12/2020

Avertir le service informatique et le DPO en cas de violations de données

Demandez à ce que les systèmes d'information, services ou outils numériques utilisés soient conformes aux référentiels de sécurité et d'interopérabilité approuvés par arrêté du ministre chargé de la santé.

Concrètement, que dois-je faire ?

Les étapes à suivre

3

Respecter les droits des personnes

Vos patients doivent être informés sur leurs droits et sur les traitements de données réalisés, notamment lors de leur prise en charge (par ex. via une affiche apposée dans les couloirs de l'hôpital par le service communication ou via la remise d'un feuillet d'information à l'accueil).

- Sanction pécuniaire à hauteur de 100 000 euros en Italie à l'encontre d'une entreprise dans le secteur de la santé ayant mis en place un programme de santé (avec base de données) sans informer correctement les personnes sur leurs droits, l'utilisation de leurs données ou la durée de conservation – 17/12/2020

- Sanction pécuniaire de la CNIL de 10 000 euros à l'encontre d'un dentiste qui refusait de transmettre le dossier médical à son patient – 18/05/2017

Assurez une bonne gestion des droits (vérification de la qualité du demandeur, respect des délais…).

- 8 jours pour une demande d'accès au dossier médical (2 mois lorsque les informations datent de plus de 5 ans), après un délai de réflexion de 48h

  1 mois pour les demandes au titre du RGPD, avec une prolongation possible de 2 mois pour les demandes complexes

Concrètement, que dois-je faire ?

Les étapes à suivre

4

Encadrer les relations avec vos prestataires

Demandez au service juridique de vérifier, avec l'aide du Délégué à la protection des données, que les contrats avec les sous-traitants à qui l'hôpital peut faire appel (permanence téléphonique pour la prise des rendez-vous, fournisseur de logiciels, etc.) contiennent bien une **clause de sous-traitance** conforme à l'article 28 du RGPD, avec notamment les obligations des parties et une description du traitement confié.

Le cas échéant, l'ajout d'une annexe au contrat par le service juridique sera nécessaire.

- Sanction pécuniaire de la CNIL à hauteur 7 300 euros à l'encontre d'une société ayant notamment manqué à son obligation d'encadrement contractuel du sous-traitant – 07/12/2020

Demandez également de **ne contracter qu'avec des sous-traitants respectant le RGPD** (par ex : les prestataires à qui l'hôpital fait appel doivent assurer un niveau de sécurité suffisant). Un questionnaire de conformité et des audits des prestataires existants peuvent s'avérer utiles.

Concrètement, que dois-je faire ?

Focus : que faire en cas de nouveau traitement

Partons d'un exemple : vous souhaitez **créer une base de données à des fins de recherche.**

Voici les étapes à réaliser :

- ❑ Contacter le DPO de l'établissement qui vous aidera pour toutes les étapes suivantes
- ❑ Clarifier l'objectif du projet, les données nécessaires, la durée de conservation, etc.
- ❑ Avec le service informatique, déterminer les mesures de sécurité appropriées et, le cas échéant, réaliser l'analyse d'impact relative à la protection des données
- ❑ Avec le service juridique, encadrer les relations contractuelles avec les parties prenantes (prestataires, co-responsables)
- ❑ Préparer une information des personnes concernées (par ex : patients accueillis à l'hôpital)
- ❑ Déterminer si une formalité préalable doit être réalisée (par ex : demande d'autorisation auprès de la CNIL, déclaration de conformité à une méthodologie de référence)
- ❑ Inscrire le projet au registre des activités de traitement

Merci de votre attention!