FRANCE – RGPD : guide du médecin

Auteur : Corinne FRANCE, General Secretary EFCSE
Working Group 3 : CYBERSECURITY - EDUCATION, FORMATION, COACHING
Mars 2018

Préambule

Le RGPD est un texte émis par l'Union Européenne qui oblige toutes les organisations, sociétés et autres entreprises, à clarifier leurs pratiques concernant le traitement qu'elles réservent aux données de leurs employés, de leurs clients et de leurs fournisseurs.

Définition des traitements de données de santé à caractère personnel

Données personnelles, de quoi s'agit-il ?

Le règlement européen de 2016 abrogeant la directive de 1995 sur la protection des données définit la donnée personnelle comme "*toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*".

C'est aussi, données sur l'origine raciale ou éthique, les données biométriques aux fin d'identifier une personne de manière unique, les données concernant la santé ou, des données concernant la vie sexuelle ou l'orientation des personnes physiques

Les données de santé à caractère personnel sont celles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé , qui révèlent des informations sur l'état de santé de cette personne.

Ainsi que toute information concernant une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.

Mais aussi les données génétiques : relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé

Et encore, les données biométriques : résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique.

Responsable du traitement

Article 1 du RGPD : le responsable du traitement est "*la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*".

Le responsable du traitement peut donc être soit une personne physique, soit une personne morale.

RGPD : les droits à respecter

Il s'agir des droits individuel qui sont renforcés avec le RGPD (confirmation des droits déjà reconnus par la CNIL en France) et des modalités d'exercice de ceux-ci, à savoir :

- Droit à une information compréhensible aisément accessible sur l'utilisation de ces données
- Un consentement clair et explicite
- Droit d'accès
- Droit de modification
- Droit d'opposition
- Droit à l'oubli / droit à l'effacement
- Droit à la portabilité des données
- Profilage limité
- Protection des mineurs
- Recours collectifs

Le responsable du traitement se doit d'être transparent et donc de fournir les explications inhérentes à sa pratique.

La confidentialité est obligatoire dans le cas du partage des données entre professionnels et/ou équipes.

ZOOM docteur : les règles à respecter

Conservation

Quelques conseils pour sécuriser les données que vous conservez, que ce soit des informations sur papier ou dématérialisées au format numérique

- Gardez le mot de passe confidentiel, ne le mettez pas à disposition sur l'ordinateur, sur un post-it ou sous le clavier, changez le régulièrement et utilisez des combinaisons mnémotechniques plutôt que des informations relatives à votre entourage telles que la date de naissance de votre petit dernier ou le prénom de votre maman ;

- Verrouillez l'ordinateur chaque fois que vous vous absentez ;
- Personne ne peut avoir accès aux informations relatives au patient hormis les assistantes médicales : prévoyez donc une clause de confidentialité dans leur contrat de travail.
- Rangez les dossiers papier dans un espace verrouillé ;

Si vous changez de logiciel professionnel, récupérez et archivez les données en amont du changement.

Conservez au minimum 20 ans les données personnelles numériques au même titre que le dossier médical du patient.

Collecte

Un médecin est soumis à une obligation de secret, les données à caractère personnel qu'il recueille sont soumises à cette même règle, dans ce contexte, il n'est pas nécessaire d'obtenir le consentement du patient pour cette collecte.

Communication

Messagerie électronique : le médecin est tenu d'utiliser une messagerie sécurisée (avec cryptage) pour envoyer, recevoir ou transférer des information médicales, il ne peut en aucun cas utiliser une messagerie qui ne serait pas cryptée (email personnel par exemple).

Lorsque le médecin adresse son patient à un autre médecin, c'est au patient que revient la charge de transmettre les données personnelles médicales au médecin consulté.

En cas de prise en charge du patient par une équipe de soins, les données couvertes par le secret médical sont réputées être transmises à l'ensemble de de l'équipe.

A propos de la messagerie sécurisée : en disposant d'une solution logicielle agréée HDS (Hébergeur de Données de Santé) un médecin dispose de fait d'une messagerie sécurisée associée (avec usage de la carte de professionnel de santé).

RGPD : le médecin doit pouvoir prouver le respect de ces règles

Principe d'imputabilité (accountability) : le médecin doit démontrer qu'il respecte le RGPD, pour cela il doit mettre en œuvre, au sein de son cabinet médical, les mécanismes et les procédures permettant la protection des données à caractère personnel (tant pour ses patients que pour ses éventuels collaborateurs).

Ceci se traduit par une suite d'actions répertoriées (la CNIL propose un document type) permettant de préciser

- la façon dont s'effectue la protection du mot de passe, de l'ordinateur et de tous les terminaux potentiellement associés à celui-ci, ainsi que les supports d'accès tels que le téléphone portable ou les tablettes,
- la façon dont le médecin gère sa messagerie et ses échanges d'informations concernant le patient,
- le plan éventuel de prévention des attaques informatiques et autre piratage, ainsi que toute destruction accidentelle ou perte de données.

Le volet respect des droits individuels des patients est un point à anticiper, il s'agit donc de se mettre en ordre de marche pour prévoir facilement et simplement les explications et les actions à mener pour que le patient puisse avoir accès à ses données, les rectifier et les transmettre vers un autre professionnel de santé si besoin.

Que se passe-t-il à partir du 25 mai 2018 ?

Le Règlement est « obligatoire dans tous ses éléments et directement applicable dans tout État membre » à partir du 25 mai 2018.

C'est un règlement, il est donc en vigueur directement, ce qui a pour conséquence pour les organisations, entreprises et autres personnes morales en tant que responsable de traitement pénalement responsable, de devenir amendable et soumis aux sanctions prévues, à savoir, pécuniaires - la plus grande valeur entre 4% du chiffre d'affaire mondial ou 20 millions d'euros – voire même des peines de prison (article 226-17 du Code pénal).

En France, c'est la CNIL qui est l'organe aux commandes du contrôle du respect du RGPD.

Dans les faits, il semble que la mise en conformité puisse « glisser » jusqu'à fin 2018 sous réserve que l'organisation, entreprise, cabinet médical, etc… montre qu'il a pris en compte cette démarche et qu'un plan d'action est associé.

RGPD - actualité médecin

RGPD : publication fin juin 2018 d'un guide pour les médecins élaboré par le Conseil national de l'Ordre des médecins et la Commission Nationale de l'Informatique et des Libertés.

En attendant, chaque médecin doit s'appliquer à respecter les principes essentiels guidant la protection des données. Pour ce faire, il est possible de se référer à l'ancienne norme simplifiée n°50 consacrée à la gestion des cabinets médicaux et paramédicaux, sans qu'il soit nécessaire de procéder à une déclaration auprès de la CNIL.

https://www.conseil-national.medecin.fr/node/2752