10/13 JuriSanté

CNEH
ÉCOLE DE RÉFÉRENCE
CONSEILLER DE CONFIANCE

25 janvier 2018

Données de santé à l'hôpital : le RGPD

CNEH - Centre National de l'Expertise Hospitalière
3 rue Danton 92240 Malakoff - Tél. 01 47 17 15 15 - Fax : 01 41 17 15 32
www.cneh.fr

1 Le règlement 2016/679 dit règlement général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnels et la libre circulation de ces données (dit RGPD : règlement général sur la protection données) du 27 avril 2016

LE RGPD : Points essentiels

Objectifs :

- **Renforcer et unifier** la protection des données pour les individus au sein de UE
  - Il remplace la Directive européenne sur la protection des données personnelles de 1995
- **Redonner aux citoyens le contrôle** de leurs données personnelles tout en simplifiant l'environnement réglementaire

- **Définir la notion de données de santé** */renforcer leur protection* : nouvelles obligations

- Compte à rebours lancé :

  - **Reste moins de 6 mois pour mettre en place le Règlement européen et se mettre en conformité**
  - **Application au 25 mai 2018**

- Nouvelle modification de la loi CNIL / projet de loi présenté en conseil des ministres en décembre 2017 : adaptation au RGPD

RGPD : Points essentiels

À qui s'applique le RGPD

- Les administrations, grands groupes… les PME, les cabinets libéraux …
  - **Bref les établissements de santé, les établissement médico-sociaux**

- Les critères d'application des dispositions du RGPD sont liés
  - Au lieu de l'établissement (en UE)
  - Aux traitements des données à caractère personnel
  - Aux personnes concernées (ressortissants en UE)

  - La typologie de traitement des données à caractère personnel et leur niveau de sensibilité : vaut pour tous les traitements de données à caractère personnel localisé en Europe ou concernant un citoyen européen
    - *Il s'appliquera donc à chaque fois qu'un résident européen sera directement visé par un traitement de données (y compris par interne)*

RGPD : Points essentiels

Définition des traitements de données de santé à caractère personnel

Données à caractère personnels	Données de santé
• Origine raciale ou éthique • Données génétiques • Données biométriques aux fin d'identifier une personne de manière unique • Des données concernant la santé ou, des données concernant la vie sexuelle ou l'orientation des personnes physiques	• **Les données** 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.

RGPD : Points essentiels

Définition des traitements de données de santé à caractère personnel

Mais c'est aussi : 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

- **+ 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
- **+ les données biométriques** : résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique

RGPD : Points essentiels

Des droits individuels renforcés

- La confirmation des droits déjà reconnus par la loi CNIL+++
- Droits des personnes et leurs modalités d'exercice
  - 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
  - Le profilage limité
  - Protection des mineurs
  - Recours collectifs
- Principe générale de transparence applicable au responsable du traitement
- Confidentialité et partage des données entre professionnels/équipe

RGPD : Points essentiels

Le principe de responsabilité (l'accountability)

- Renforcer la responsabilité des responsables de traitement de données
- Démontrer la conformité à la règlementation
- Mettre en œuvre des mesures techniques et organisationnelles (niveau de sécurité adapté au risque encouru)
- Des formalités allégées / la CNIL contrôle a posteriori

- Possibilité pour chaque états de fixer des conditions ou restrictions supplémentaires … à voir dans la prochaine loi CNIL
  - Ex en France : maintien des autorisation/avis sur Santé NIR génétique ..

2 Intégrer le RGD en établissement de santé

RGPD : Points essentiels

Comment intégrer le RGDP

- Nommer un chef de projet : **d**élégué à la **p**rotection des **d**onnées (DPD)
- Cartographier les traitements existant de manière exhaustive
- Vérifier la conformité des traitements de données de santé
- Sécurisation

Intégrer le RGD en établissement de santé

Délégué à la protection des données (DPD ou Data protection Officier (DPO))

- Désignation obligatoire pour les établissements publics
  - Piloter la conformité interne en assistant le responsable du traitement (DSI) / au RGPD
  - Vérifier qu'un PIA a été mené et maintien la documentation si nécessaire
  - Contact des autorités et des personnes concernées
  - Répondre aux sollicitations des personnes qui veulent faire valoir leurs droits
- Qualifications exigées et position dans la structure
  - Connaissances spécialisées en législation et dans les pratiques de terrain
  - Doit être associé aux questions et décisions relatives aux données: par de conflit d'intérêt
  - Indépendance dans la fonction
  - Moyens et ressources nécessaires

Intégrer le RGD en établissement de santé

Cartographier vos traitements de données

- Recenser précisément vos traitements de données
- Constitution d'un registre de traitement central
  - Documenter tous les traitements de données à caractère personnel de l'établissement
  - Inventaire exhaustif - sans condition
  - Une fois les traitements identifiés : collecter les systèmes informatiques liées comme les SI sous jacents, les flux de données correspondants des sous-traitances éventuelles (PAC informatiques gérés par une autre structure sous contrat)
  - ATTENTION identifier les risques et les gérer
    - une approche par risques doit être suivie pour identifier les priorités de la mise en conformité des traitements qui peuvent entrainer des risques élevés pour les personnes
- S'assurer du respect des obligations du RGPD

Intégrer le RGD en établissement de santéRGPD : Points essentiels

La sécurisation des systèmes d'information

- Garantir la protection des données
  - Dès la conception des produits ou services, systèmes d'exploitation des données à caractère personnel
  - Ou la sécurité par défaut :
    - obligation de disposer d'un système d'information par défaut
    - Garantir par défaut que seules les données nécessaires sont traitées.

  - Créer un référentiel sécurité à jour (charte utilisateur des SI, politique d'habilitation, politique de gestion des incidents…)

Intégrer le RGD en établissement de santé

Mais aussi d'autres responsabilités

- Signalement des violations de données, obligatoire / notification en cas de fuite de données
  - À l'autorité de contrôle (dans les 72h) sauf pas de violation susceptible d'engendrer un risque pour les droits et libertés des personnes
  - À chaque personne concernée (rapidement) si susceptible d'engendrer un risque pour les droits et libertés (quelques exceptions ex: mesures qui minimisent les risques…)

Intégrer le RGD en établissement de santé

Les recommandations

- Réaliser une analyse d'impact des opération envisagées sur la protection des données personnelles (PIA / Privacy Impact Assesment)

En attente de la liste des types d'opérations de traitement = PIA requis

  - Permettre aux responsables de traitement et aux fournisseurs de solutions de pouvoir justifier du niveau de garantie proposé en termes de protections de données
  - Pour toutes activités qui peuvent avoir des conséquences importantes en matière de protection des données personnelles

Faire converger les **démarches** existantes

  - Prévoir des mesures afin de diminuer les conséquences sur les dommages potentiels // protection des données à caractère personnel
  - Consultation des autorités de contrôle avant toute mise en œuvre des ces activités (art. 35)

- Réaliser des audits organisationnels : sur les différents traitements existants

Intégrer le RGD en établissement de santé

Des sanctions augmentées

- Des amendes de la CNIL 150 000 .. 20 million et 4% du CA mondial d'une entreprise
- Quid des hôpitaux : la Cnil peut sanctionner

- Comité européen de la protection des données
  - Autorité en ce qui concerne l'interprétation du Règlement

Intégrer le RGD dans a restructuration hospitalière

- RGDP et GHT : une organisation efficiente à l’ horizon 1er janvier 2021

3 Que faire en urgence / si ce n’est pas déjà effectué

RGPD : à faire dès maintenant

1. Désigner un pilote : déléguée à la protection des données
2. Cartographier vos traitements de données personnelles
3. Prioriser les actions à mener
4. Organiser la gestion des risques
5. Organiser les processus internes
6. Documenter la conformité

Conseil de la CNIL : le règlement européen comment se préparer … 6 étapes