CNEH
ÉCOLE DE RÉFÉRENCE
CONSEILLER DE CONFIANCE

HOUDART ET ASSOCIÉS
SOCIÉTÉ D'AVOCATS

RGPD et établissements de soins : il y a urgence !

Matinale du 15 mai 2018

Intervenants :

Brigitte De Lard-Huchet, directeur, pôle JuriSanté, CNEH

Isabelle Génot Pok, Juriste consultante-formatrice, droit de la santé, pôle JuriSanté, CNEH

Laurie Dupont-Horaux, Juriste, pôle Santé Numérique, Cabinet Houdart et associés

Benoit Louvet, Avocat associé, pôle Santé Numérique, Cabinet Houdart et associés

I Introduction générale au RGPD

Intervenant :
Benoit Louvet, Avocat associé, pôle Santé Numérique, Cabinet Houdart et associés

Introduction générale

1. RGPD et Loi Informatique et Libertés

2. Les définitions relatives au traitement de données personnelles

3. Les enjeux de la protection des données dans le secteur de la santé

1. RGPD et Loi Informatique et Libertés

1. RGPD et Loi Informatique et Libertés

- De **Safari** au vote de la loi du 6 janvier 1978 créant la **CNIL**
- De la **directive 95/46** à la naissance de l'internet et des **GAFA**
- Un règlement européen d'application **directe** dans tous les pays de l'Union
- Le RGPD est avant tout un changement de **paradigme**

2. Les définitions relatives au traitement de données personnelles

2. Les définitions relatives au traitement de données personnelles

- La **donnée** à caractère personnel
- Le **traitement** de données
- Le **responsable du traitement**
- Le **sous-traitant**

3. Les enjeux de la protection des données dans le secteur de la santé

3. Les enjeux de la protection des données dans le secteur de la santé

- Le secteur de la santé traite des données considérées comme **sensibles** (particulières) par le RGPD
- Obligation de tenir un **registre** des activités de traitement
- Obligation de désigner un **DPO**
- L'hébergement de données de santé est soumis à **certification**

II Le rôle de la CNIL : quelles évolutions avec le GPRD ?

Intervenante :
Isabelle Génot Pok, Juriste consultante-formatrice, droit de la santé, pôle JuriSanté, CNEH

Rôle modifiée de la CNIL

- Elle est le protecteur et régulateur des données personnelles (en France)
- Elle accompagne les acteurs publics comme privés dans leur mise en conformité
- Elle reçoit et traite les réclamations, les violations de données
- Elle peut imposer à un acteur de régulariser son traitement par une mise en demeure
- Elle peut aussi sanctionner par une amende

Rôle modifiée de la CNIL

- Elle ne donne plus d'autorisation a priori sauf pour certains traitements qui restent régis par des autorisations
  - En santé : traitements de données à des fins de recherche

- Les labélisations ne sont plus délivrées (demandes non prises en compte depuis le 30 mars 2018)
  - Certification CNIL

- Elle contrôlera a posteriori : au responsable du ou des traitements de prouver sa conformité (documentation à fournir : registres, désignation du DPO/DPD, analyse…)

Rôle modifié de la CNIL

- La CNIL produit des référentiels et guides à destination des acteurs économiques, clarifiant la législation applicable à leur situation particulière.
  - Des méthodes (le RGPD en 6 étapes)
  - Publication des « G29 » : les lignes directrices
  - Des outils pratiques : logiciel de PIA, modèle de registre
  - Listes des traitements devant faire l'objet de PIA
  - Référentiels de certification
  - Recommandations
  - Règlements types pour assurer la sécurité des traitements de données

Rôle modifié de la CNIL

- Effectuer des contrôles : sur la base du programme annuel des contrôles, des plaintes reçues par la CNIL, …., ou pour faire suite à un précédent contrôle.

- Les contrôles opérés auront essentiellement pour but, dans un premier temps, de conseiller, accompagner l'entrée dans la démarche de conformité, faire comprendre les textes.
  - Attention : l'accompagnement n'est pas individualisé.

Rôle modifié de la CNIL

- Mais après cette « période de clémence » , il sera possible à la CNIL de prononcer des sanctions pour toute personne morale si celle-ci ne s'est pas conformée aux normes du RGPD (art 83)

  - qui doivent être effectives, proportionnées, dissuasives

  - + 11 critères : ex : violation délibérée / négligence / si avantages financiers tirés de la violation…

Rôle modifié de la CNIL

- Exemples de sanction
  - Avertissement au RT ou sous traitant (si opérations de traitement sont susceptibles de violer le RGPD)
  - Mise en demeure
    - de se mettre en conformité + délai (en cas de non respect des obligations relatives au RGPD)
    - De faire valoir les droits d'une personne
  - Limitation temporaires des traitements, suspension des traitements
  - Imposer que l'établissement informe de ces sanctions les personnes concernées par les manquements ou la violation
  - Suspension provisoire de la certification
  - Peut passer à des sanctions financières sans mise en demeure

Rôle modifié de la CNIL

- Autres sanctions possibles : l'article 84 1° du Règlement énonce que les Etats peuvent déterminer le régime des sanctions applicables en cas de violation des obligations prévues, autres que les sanctions administratives.

- Sanctions pénales actuelles mais modifiables au 25 mai…
  - Non-respect de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité : articles 226-17 et 226-17-1 du Code pénal / 300.000 euros d'amende et 5 ans d'emprisonnement

  - Détournement de la finalité des données personnelles : article 226-21 du Code pénal / 300.000 euros d'amende et 5 ans d'emprisonnement

III Comment implémenter le RGPD dans les établissements

Intervenante :
Laurie Dupont-Horaux, Juriste, pôle Santé Numérique, Cabinet Houdart et associés

III- A - Les audits organisationnels : établir un état des lieux

Objectifs de l'état des lieux

Réaliser un diagnostic au sein d'un établissement de santé :

Vision globale de la protection des données

Construire un rapport → Actions de mise en conformité

III- A - Les audits organisationnels : établir un état des lieux

Objectifs de l'état des lieux

- ❑ Recensement de l'existant
- ❑ Cartographie des traitements
- ❑ Fiche DPO
- ❑ Registre

III- A - Les audits organisationnels : établir un état des lieux

L'audit organisationnel : contrôle des pratiques en matière de protection des données personnelles

Objectif : adopter une **gouvernance** à la protection des données:

- Démarrer sur des bonnes bases : projet bien défini, objectifs clairs;
- Bâtir une équipe: Répartition des responsabilités dans l'entreprise (DAF/DSI…) + Formalisation de cette répartition (procédures, règles applicable).
- S'assurer d'un bon soutien: pilote désigné, soutien de la Direction, personnel impliqué et informé.

III- A - Les audits organisationnels : établir un état des lieux

Procédures internes

Formalisation de cette répartition (procédures, règles applicables, …) :

- Chartes informatiques
- Politique de protection des données
- Sensibilisation et formation du personnel concerné

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

- Une fonction indépendante, report au plus haut niveau de la Direction
- Un intermédiaire entre les RT/ST et les personnes concernées par le traitement des données personnelles = Un chef d'orchestre
- Des ressources allouées
- Interlocuteur privilégié avec les autorités locales (CNIL)
- Secret professionnel/obligation de confidentialité en ce qui concerne l'exercice de ses missions.

Quid du conflit d'intérêts ?

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

- Quand le nommer ?
- Quelles missions ?
- Qui nommer ?
- Quelle responsabilité vis-à-vis de sa hiérarchie en interne ?
- Quelles garanties sont exigées de votre DPO externe ?

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

Quand le nommer ?

Le DPO est obligatoire lorsque :

- Le traitement est effectué par une autorité publique ou un organisme public
- Les activités de base du RT ou du ST consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées
- Les activités de base du RT ou du ST consistent en un traitement à grande échelle de catégories particulières de données / et données relatives à des condamnations pénales ou infractions

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

Quelles missions ?

Quel est son rôle ?

- Informe et conseille le RT, le ST, les employés procédant au traitement, sur les obligations qui leur incombent
- Contrôle le respect du RGPD + dispositions nationales + règles internes du RT/ST
- Sensibilise et forme le personnel participant au traitement
- Réalise les audits nécessaires
- Conseille sur demande sur l'analyse d'impact (il en vérifie aussi l'exécution)
- Coopère avec l'autorité de contrôle

Le RT ou le ST toujours responsable sauf en cas de négligences ou fautes du DPO

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

Qui nommer ? Quelles compétences doit avoir le DPO ?

- Qualités professionnelles
- Connaissances spécialisées du droit et des pratiques en matière de protection des données
- Capacité à accomplir ses missions

Recommandations :

- Déterminer si vous souhaitez un DPO dédié ou ajouter les fonctions DPO à un poste existant (pensez à éviter les conflits d'intérêts), ou désigner un prestataire externe

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

Quelle responsabilité vis-à-vis de sa hiérarchie en interne ?

- Responsabilité du responsable de traitement devant la CNIL
- Contrôle de la CNIL sur le travail du DPO
- DPO interne : responsabilité disciplinaire commune à tous salariés
- DPO externe : responsabilité contractuelle vis-à-vis de son client

III- B- Les enjeux de la gouvernance RGPD : le rôle central du DPO

Quelles garanties exigées de votre DPO externe ?

- Compétence :
  - Juridique
  - Technique
  - Qualité
  - Métier
- Budget clair
- Exigence d'un PAQ
- Garantie de réversibilité

III- C- Mettre en place les procédures adaptées et sensibiliser partenaires et collaborateurs

Registre des activités de traitement

(article 30 du RGPD)

- Obligatoire pour les entreprises ou organisations comptant au moins 250 employés

- Obligatoire pour les entreprise ou organisations de moins de 250 employés (conditions non cumulatives) :
  - Si le traitement est susceptible de comporter un **risque** pour les **droits et libertés des personnes ;**
  - S'il n'est pas occasionnel ;
  - **S'il porte sur les catégories particulières de données ;**
  - S'il porte sur des données personnelles relatives à des condamnations pénales et infractions

III- C- Mettre en place les procédures adaptées et sensibiliser partenaires et collaborateurs

Qu'est-ce que le registre des activités de traitement ?

Outil de pilotage

Démontre la conformité

➔ **Reflète la réalité des traitements de données personnelles**

Comment constituer un registre ?

RECENSER - **Rassembler les informations disponibles**

LISTER- **Elaborer la liste des traitements**

ANALYSER- **Affiner / préciser**

III- C- Mettre en place les procédures adaptées et sensibiliser partenaires et collaborateurs

Recommandations

- Tout établissement constitue un registre
- Les activités de traitement susceptibles d'avoir un impact sur les droits des personnes entrent dans le registre
- Séparer les registres des RT et ST
- Enrichir le registre de toutes informations complémentaires
- Mise à jour régulière (évolutions fonctionnelles et techniques des activités).

III- D – RGPD et GHT : quelle organisation efficiente ?

RGPD et GHT : système d'information convergent

- Le GHT (Groupement Hospitalier de Territoire) est un mode de coopération entre établissements d'un même territoire
- Le GHT n'a pas la personnalité morale
- **Attention** : l'établissement support du GHT agira bien souvent en qualité de **sous-traitant** des autres membre du groupement
- De même, l'établissement support devra dans le plupart des cas être certifié **hébergeur** de données de santé.

IV Des droits individuels renforcés

Intervenante :
Isabelle Génot Pok, Juriste consultante-formatrice, droit de la santé, pôle JuriSanté, CNEH

Les droits individuels renforcés

- Principe fondamental du RGPD : rendre à la personne la maîtrise de ses données
  - En établissement de santé : données de santé / données personnelles hors champ de la santé (RH)
- Les droits renforcés en conséquence
- Quels sont les droits qui s'appliquent aux établissements de santé et médico-social ?
  - Ils doivent se conjuguer avec le code de la santé publique et le code de l'aide sociale et des familles / textes relatifs aux droits des patients-résidents

Les droits individuels renforcés

- Droit à l'information
- Droit d'accès
- Droit de modification/rectification
- Droit à l'oubli
- Droit de notification pour toute rectification ou effacement de données à caractère personnel
- Consentement
- Droit à la portabilité
- Profilage
- Droit à réparation

Les droits individuels renforcés

Droit à l'information

- Elle doit être concise, transparente, compréhensible et **aisément accessible**, en des termes clairs et simples. Les informations sont fournies par écrit ou par d'autres moyens **au moment où les données en question sont obtenues** :
  - Elles portent d'une part sur : l'identité et les coordonnées du responsable du traitement et, de son représentant si besoin, le DPO, les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement, le niveau de sécurité du système utilisé et des mesures prises par le du traitement pour la protection
  - D'autre part sur **la durée de conservation des données**, les droits dont dispose la personne : accès, rectification, effacement, limitation du traitement, opposition (personnes décédées), l'introduction d'une réclamation auprès de la CNIL, information en cas de violation des données
- Choix du support

Les droits individuels renforcés

- Droit d'accès aux données personnelles
  - La personne concernée accède à ses données
    - Accès à toute demande d'information (sans préjudice à autrui)
    - Sur demande, le RT fournit une copie des données à caractère personnel faisant l'objet d'un traitement.
    - Le support est fonction de la demande
    - Le délai de fourniture est d'un mois / + un mois si impossible de transmettre dans le mois qui suit la demande
      - **Pour les données médicales : l'article L1111-7 du CSP continue de s'appliquer (8 jours…)**
      - **Pour les données personnelles type dossier de carrière : Code des relations entre le public et l'administration (CRPA) s'applique (1 mois)**

Les droits individuels renforcés

- Droit de rectification/modification
  - Rectification/modification : Toute donnée inexacte, incomplète, équivoque, périmée ou dont la collecte est interdite
    - Obligation de rectification dans les meilleurs délais : information obligatoire en cas de difficulté
      - 1 mois
    - Si refus de rectification : information obligatoire + motif du refus à la personne concernée

Les droits individuels renforcés

- Droit à l'effacement (oubli)
  - L'effacement / droit à l'oubli : ATTENTION Hôpital !!!
    - Dans quels cas ? Avec quelles procédures ?
    - Dispositif juridique relatif aux archives hospitalières (à caractère public)
      - Délais de conservation légaux ou déterminés dépassés, pas de conservation d'archives définitives à l'hôpital,…

Les droits individuels renforcés

- Le RT doit notifier au demandeur le résultat de sa demande
  - Notification de toute rectification ou effacement
    - Sauf si impossibilité ou efforts disproportionnés

Les droits individuels renforcés

Le consentement

- Si le traitement est fondé sur le consentement le RT doit pouvoir apporter la preuve de ce consentement

- Cas ou traitement n'est pas fondé sur le consentement
  - **obligation légale** / exécution d'une mission d'intérêt public ou relevant de l'autorité publique / intérêt vital /intérêt légitime

- Attention à certaines dispositions du CSP : ex : L1110-4 modifié
  - Le transfert de données de patients/résidents hors équipe de soins

Les droits individuels renforcés

La portabilité !

- Ne concerne que les traitements automatisés fondés sur le consentement de la personne concernée ou l'exécution d'un contrat
- Données fournies au RT
- Données directement fournies
- Ne concerne pas les données dérivées ou déduites par le RT
- Utilisables facilement
  - Le responsable du traitement ne supprime pas les données par principe (sauf droit à effacement)
  - Droit autonome // aux autres droits

Droit non applicable

Les droits individuels renforcés

Le profilage !

- **Le droit pour une personne de ne pas faire l'objet d'une prise de décision individuelle automatisée**, c'est-à-dire « une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.»

- A priori interdit dans le domaine de la santé

Droit non applicable

Les droits individuels renforcés

Le droit à réparation en cas de violation de données

Conditions de la violation de données (faille de sécurité)

- Existence d'un traitement (quel qu'il soit) de données personnelles
- Destruction, perte, altération, divulgation **ou accès non autorisé** à des données personnelles : **de manière accidentelle ou illicite**
- Intervenue dans le cadre de l'activité
- Sécurisation du système interne externe : notion de d'accès aux données transfert de données, circulation de données / règles du CSP la perte de confidentialité des données soumises au secret professionnel

- Notification à la CNIL 72h après connaissance des faits
- Information de la personne concernée si atteinte à ses droits et libertés

ACTION GROUP

V La sécurisation du système d'information

Intervenant :
Benoit Louvet, Avocat associé, pôle Santé Numérique, Cabinet Houdart et associés

La sécurisation des systèmes d'information

1. Présentation de la directive NIS

2. Comment auditer et sécuriser les systèmes d'information

3. Lien avec les obligations de signalement des EI du système d'information

1. Présentation de la directive NIS

1. Présentation de la directive NIS

- La **directive du 6 juillet 2016** NIS a été transposée en France par la **loi du 26 février 2018**
- La directive prévoit le renforcement par chaque Etat de la cybersécurité des « **opérateurs de services essentiels** »
- Un **arrêté du 10 juin 2016** fixe les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activité d'importance vitale «Produits de santé»
- La liste des établissements concernés est classifiée

2. Comment auditer et sécuriser les systèmes d'information

2. Comment auditer et sécuriser les systèmes d'information

- Le RGPD impose une obligation de sécuriser les données
- Les secteurs sanitaire et médico-social disposent déjà des référentiels et des outils nécessaires
- En premier lieu la **PGSSI-S** opposable depuis avril 2018
- Complétée par plusieurs référentiels majeurs : le RGS, l'ISO 27001, EBIOS, les guides de l'ANSSI

3. Lien avec les obligations de signalement des EI du système d'information

3. Lien avec les obligations de signalement des EI du système d'information

- L'article L-1111-8-2 du CSP oblige les établissements de santé (soumis au CSP) à déclarer sans délai les **incidents significatifs de sécurité** au directeur général de leur ARS
- L'ASIP Santé met en place une **cellule** Accompagnement Cybersécurité des Structures de Santé (ACSS)
- Cette obligation sera à conjuguer avec celle de l'article 33 du RGPD obligeant le responsable du traitement à notifier à l'autorité de contrôle (la CNIL) les **violations de données**
- Les établissements devront établir des **procédures** en la matière