Traitement des données de santé dans un établissement de santé

Mise en pratique

Dr. Moufid HAJJAR – DPO du CHU de Bordeaux

Jeudi 23 juin 2022

Cadre général

Traitement de données

- *(cf. Article 4 – RGPD)*

  Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel,

  telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Registre des traitements (R3T)

- Registre des activités de traitement
  - recenser **l'ensemble** des traitements de données personnelles
  - disposer d'une vue d'ensemble de ce que l'établissement (ETS) fait avec les données personnelles
- Il est prévu par l'Article 30 du RGPD, et participe à la documentation de la conformité
- C'est un outil de pilotage, et de démonstration de la conformité au RGPD

Registre des traitements (R3T)

- Il doit se présenter sous forme **écrite**,
  électronique ou papier

- Responsable de traitement (RT) / Sous-traitant (ST)
  - Il doit distinguer les deux catégories d'activités
    si le cas échéant, l'ETS est aussi un ST ➔ faire deux R3T

- Sa tenue est obligatoire et concerne tous les organismes,
  publics comme privés, quelle que soit leur taille,
  dès lors qu'ils traitent des données personnelles
  - Dérogation à l'exhaustivité pour les ETS ayant moins de 250 salariés

Registre des traitements (R3T)

- Tenue du Registre
  - de principe, le RT ou la personne qu'il a délégué pour ce faire (DPO par exemple)

- Communication du Registre
  - pour un **organisme public**, à toute personne qui en fait la demande
    - document administratif, communicable à tous, au sens du code des relations entre le public et l'administration.
    - occulter toute information dont la divulgation pourrait porter atteinte aux secrets protégés par la loi, et notamment à la sécurité des systèmes d'information

Registre des traitements (R3T)

- En pratique, une fiche de registre pour chaque traitement de données à caractère personnel

- Contenu ***a minima*** d'une fiche :
  - nom et coordonnées de l'ETS, du RT (*et le cas échéant du RT conjoint*), du DPO
  - les finalités du traitement
  - les catégories de personnes concernées
  - les catégories de données personnelles
  - les catégories de destinataires
  - les transferts de données à caractère personnel
  - la durée de conservation
  - une description générale des mesures de sécurité

Mise en pratique dans un établissement de santé

notamment un Centre Hospitalier Universitaire (CHU)

Plan d’action et recensement

Hôpital = organisation complexe !

- À moyen ou court terme, et en parallèle, formaliser une politique des protection des données personnelles et sensibiliser les principaux correspondants d’intérêt à la protection des données

- Reprise de l’antériorité s’il y a lieu, éventuellement en s’appuyant sur les déclarations de traitement à la CNIL antérieures à l’application du RGPD

Plan d'action et recensement

- Repérer toutes les cibles d'intérêt
  - Récupérer tous les organigrammes disponibles (directions, pôles médicaux, écoles et instituts des métiers de la santé,…)
  - Identifier les informaticiens du service informatique ou les référents SI qui sont correspondants métiers des directions ou de domaines fonctionnels
  - Repérer les secteurs qui disposent d'un relevé circonstancié de leurs finalités de traitement ou actions (DSI, DRCI, IMS, Ecole de sage-femme, EDS…)
    - travailler sur les compléments à apporter au processus en cours pour nourrir le Registre et privilégier l'intégration régulière par import (éviter la double saisie)

Plan d'action et recensement

- Mener des entretiens avec les responsables fonctionnels et leur correspondant SI métier s'il existe
  - Ne pas oublier les IRP et la médecine du travail, en particulier les traitements concernant le personnel
  - Identifier les processus internes et les circuits permettant d'alimenter le R3T
  - Demander la désignation d'un correspondant à la protection des données personnelles (CDP), relais du DPO et futur acteur des déclarations et de la mise à jour
  - Évaluer les principes de minimisation et transparence des traitements de données au sein des différents métiers de l'ETS
  - Évaluer et sensibiliser sur les durées de conservation des traitements de données personnelles
    - Tension de gestion : s'assurer de la mise en œuvre des durées de conservation pour chaque traitement et poursuivre pour tous les nouveaux traitements.

Plan d'action et recensement

- Cartographier et catégoriser les finalités de traitement

Dans un hôpital, on doit distinguer *a minima* :

- Directions fonctionnelles et administratives
  - Direction du SI / Biomédical : quel degré d'imbrication ?
- Domaine du soin
  - À noter : Prestations externes (services à la chambre, TV,…)
- Domaine médicotechnique (laboratoires, pharmacie, imagerie, explorations fonctionnelles,…)
- Domaine support et technostructure
  - Vigilances, prévention, pertinence des soins, éducation thérapeutique, PMSI, archives, EDS,…)
  - Sûreté (télésurveillance, enquêtes internes, sécurité,…)
- Enseignement et Écoles
- Recherche interne et externe, loi JARDÉ ou hors-loi JARDÉ
- *Pour un CHU*, domaines et activités en lien avec l'Université

Plan d'action et recensement

- Exemple de catégories du R3T du CHU de Bordeaux

Catégorie	Nom / sigle
Administration et logistique	Gestion de la logistique et service technique
	Gestion de la qualité et des risques
	Gestion des ressources humaines
	Gestion économique et financière
	Vote électronique - Elections Professionnelles
Entrepôts de données	Annuaires
	Base de production et agrégats
	Référentiels
Gestion et soin du patient	Biologie médicale et Anatomie et Cytologie pathologiques
	Données administratives patient
	Dossiers médicaux de spécialité
	Dossiers soin aigus
	Imagerie médicale non radiologique
	Imagerie médicale radioloique
	Médical commun et paramédical
	Médicaments
	MédicoTechniques
	Prescription produits et actes
	Programmation ressources et Agenda patient
	Urgences
	Valorisation des activités et facturation
Infrastructure	Biométrie
	Echange de données standardisées
	Gestion des systèmes d'exploitation
	Infrastructures de confiance
	Middlewares
	Moyens de communication
	Outils de surêté physique
Pilotage Médico-économique	Traitement décisionnel
Recherche et enseignement	Enseignement
Recherche et enseignement	Recherche

Plan d'action et recensement

- Statuer sur la méthode de recensement :
  - Envoi et suivi d'un formulaire avec Excel (actuel)
    - Ajout de notions complémentaires mais indispensables : base légale de traitement, caractère mono ou multicentrique d'une étude, multi entités juridiques, cadre de MR, demande autorisation CESREES-CNIL
    - Ajout de documents : protocole, exemple de convention, schéma des flux de données, PIA ou lien avec la PIA, matrice des responsabilités
  - Saisie dans un progiciel (en cours et recommandé)
    - Collaboration RSSI / DPO +++
    - Paramétrage et fiches spécifiques par domaine
    - Habilitations des CDP
    - Liens avec PIA et gestion de la SSI
    - Tableau de bord du DPO et suivi de la conformité

Quelques particularités…

- Annuaire de volontaires sains
- Annuaire de volontaires témoins (enseignement)
- Centralisation et enregistrement des contrats et conventions par le Secrétariat Général (ContratTech)
- Sous-traitance :
  prestations de laboratoire, gestion de la paye
- Distinguer domaine courant / recherche
  - Recherche : traitements non occasionnels, volume et diversité considérable, gestion des bases de données longitudinales (EDS)
- Lien avec l'Université pour les CHU, notamment déterminer les RT conjointes et leur périmètre (matrice des responsabilités)

Merci de votre attention