RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Régionale de Santé Normandie

Règlement général sur la protection des données personnelles (RGPD) et ETP

Les obligations qui résultent du règlement général sur la protection des données personnelles (RGPD) entrées en vigueur le 25 mai 2018, s'appliquent au cahier des charges des programmes d'éducation thérapeutique du patient.

Avec le RGPD, la commission nationale de l'informatique et des libertés (CNIL) effectue non plus un contrôle a priori, basé sur les régimes de déclaration et d'autorisation préalables, mais un contrôle a posteriori, fondé sur l'appréciation par les responsables de traitement des risques en matière de protection des données. Ainsi, l'exploitation des données afférentes aux programme d'ETP ne fait plus l'objet d'une demande d'autorisation de la CNIL (excepté dans l'hypothèse de traitements de données à des fins de recherche).

Les responsables de programmes ETP, en tant que responsables de traitement de données doivent à cette fin respecter un certain nombre d'obligations, à savoir notamment :

- Tenir un registre interne qui décrit les traitements mis en œuvre.

Ce registre doit inclure le nom et les coordonnées du responsable de traitement, ainsi que les éléments essentiels dudit traitement (la finalité du traitement de données, les personnes concernées par ce traitement, les destinataires, la durée du traitement, la durée d'archivage…).

- Assurer le droit à l'information des personnes dont les données sont traitées.

Cette information peut être effectuée par voie d'affichage dans l'établissement ou bien par la production d'un document spécifique.

Les informations fournies devront comporter :

- l'identité du responsable du traitement ;
- l'identification du délégué à la protection des données (par exemple par une adresse mail générique) ;
- la finalité du traitement ;
- le caractère obligatoire ou facultatif des réponses et les conséquences éventuelles d'un défaut de réponse ;
- les destinataires ou catégories de destinataires des données collectées ;
- les droits des personnes (droit d'opposition au traitement, droit d'accès, droit de rectification et d'effacement des données) ;

- l'existence du droit à la limitation du traitement, du droit à l'oubli, du droit à la portabilité des données, du droit de retirer son consentement à tout moment, du droit d'introduire une action devant une autorité de contrôle (en France, droit de formuler une réclamation auprès de la CNIL) ;
- les éventuels transferts de données à caractère personnel envisagés à destination d'un état non membre de l'union européenne (UE) ;
- la durée de conservation des données et leur archivage ; lorsque ce n'est pas possible d'indiquer la durée de conservation des données, indiquer les critères utilisés pour déterminer cette durée ;
- la base juridique du traitement ;
- l'intention d'effectuer un traitement ultérieur pour une autre finalité et les informations pertinentes relatives à ce traitement ultérieur.

➢ Réaliser une étude d'impact relative à chaque traitement de données susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

La CNIL détaille les critères permettant de définir les cas où cette analyse (ou étude) d'impact est obligatoire et a mis en ligne un outil permettant de la réaliser.

Les traitements déjà en cours ayant fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018 sont dispensés de cette obligation durant 3 ans à compter de cette date, dès lors qu'ils n'ont fait l'objet d'aucune modification significative.

➢ Désigner un délégué à la protection des données (DPD ou DPO).

Les établissements publics de santé sont tous concernés par cette obligation, tandis que les établissements privés de santé sont potentiellement concernés, selon qu'ils mettent ou non en œuvre un traitement de données sensibles « à grande échelle ». La mutualisation d'un DPD entre plusieurs établissements est possible.

➢ Porter une attention particulière à l'encadrement contractuel des prestations des tiers fournisseurs de service (sous-traitants article 28 du RGPD).

➢ Mettre en place des procédures permettant de garantir la sécurité et la confidentialité des données.

➢ Signaler auprès de la CNIL tout incident de sécurité impliquant des données personnelles.