L'ANALYSE D'IMPACT EN PROTECTION DES DONNÉES PERSONNELLES DE SANTÉ

MISE EN PRATIQUE POUR LES « PETITS » ÉTABLISSEMENTS SANITAIRES, SOCIAUX ET MÉDICO-SOCIAUX

Avec l'entrée en application du règlement général relatif à la protection des données personnelles (RGPD) le 25 mai 2018, les acteurs sanitaires, médico-sociaux et sociaux sont entrés dans une démarche de mise en conformité spécifique en raison des données sensibles que ces derniers traitent dans le cadre de leur activité.

En effet, les données personnelles relatives à la santé sont des données sensibles au sens du RGPD et nécessitent à cet égard un niveau de vigilance plus important. La mise en conformité prend en considération cette vigilance spécifique et apporte des réponses adéquates en matière de sécurité, d'intégrité et de confidentialité des données.

Avec l'établissement d'un bilan du Registre des activités de traitement et l'identification des points de vigilance relevés, cette formation pratique propose de poursuivre la démarche de mise en conformité démarrée, et sera consacrée à tous les aspects de l'analyse d'impact en répondant à des questions telles que : dans quelles conditions est-elle obligatoire ? Quels sont les traitements qui nécessitent une analyse d'impact en priorité ? Quels sont les outils qui sont mis à disposition ? Sur quelle méthodologie s'appuyer ? Quels sont les types de mesures de sécurité (technique et organisationnelle) à mettre en œuvre ?

La formation est spécialement destinée aux « petits» établissements qui ont déjà entrepris des démarches de mise en conformité.

OBJECTIFS

- Comprendre l'analyse des risques en protection des données
- Prendre en main l'outil PIA de la CNIL et la documentation annexe
- Comprendre le vocabulaire relatif aux mesures de sécurité techniques et organisationnelles
- Identifier les droits des personnes concernées par le traitement et les rendre effectifs

21 juin 2021

Classe virtuelle

325€
par personne

1 jour

01 53 98 95 03 – formation@fehap.fr

Prérequis

Bonnes connaissances sur la protection / la sécurité des données personnelles et avoir débuté la démarche de mise en conformité au sein de la structure

CONTENU

Bilan du Registre et lien avec l'analyse d'impact

- Comment utiliser le Registre pour réaliser mon analyse d'impact sur les droits des personnes ?

Rôle du DPO dans l'analyse d'impact et responsabilités

- Rédaction - Évaluation - Validation
- Matrice des responsabilités (RACI) ?

État des connaissances théoriques

- Quand est-ce que l'analyse d'impact est-elle obligatoire ?
- Comment cibler les traitements de données personnelles nécessitant une analyse d'impact ?
- Quand et comment faut-il effectuer une consultation préalable de la CNIL ?

Gestion des risques en protection des données personnelles :

- Des pratiques d'analyse issues des démarches qualité et gestion des risques
- Comment utiliser des outils qualité pour l'analyse d'impact en protection des données personnelles : roue de Deming (PDCA), analyse SWOT, matrice de criticité des risques
- De la méthodologie EBIOS (sécurité des systèmes d'information) appliquée à la gestion des risques en cas de violation des données personnelles

Cas pratique

- Réalisation d'une analyse d'impact relative à un traitement de données personnelles de santé (utilisation du logiciel PIA de la CNIL) : analyse d'impact des données personnelles traitées dans le cadre du dossier patient/résident (papier et/ou automatisé)
- Comment évaluer les risques suite à une analyse d'impact ?
- Mesurer les risques (internes et externes) : gravité et vraisemblance dans la survenance du risque ?
- Compléter les trois étapes de l'outil CNIL : cycle de vie, mesures de sécurité et risques, plan d'action

Et après ?

- Comment accompagner la mise en œuvre du plan d'actions ?
- Identifier les parties prenantes à la mise en conformité, construction d'une feuille de route, priorisation selon les risques (diagram de Gantt), résultats attendus/obtenus, mesure des écarts, ressources (humaine, financière, matérielle, etc.)

! *Venir avec un ordinateur ou une tablette disposant d'un tableur et les documents de mise en conformité (registre, procédure, rapport d'audit, note de cadrage juridique etc.)*

PUBLICS

- Délégués à la protection des données (DPO) ou référents à la protection des données
- Pilotes de la démarche de mise en conformité

MÉTHODES PÉDAGOGIQUES ET MODALITÉS D'ÉVALUATION

Pédagogie interactive alternant :

- apports théoriques et méthodologiques
- étude de cas pratiques et échanges
- mise en situation : prise en main des outils
- travaux en groupes

Grille d'auto-évaluation des acquis de la formation

INTERVENANTS

- Juriste en droit de la santé - formatrice-consultante et conceptrice d'outils de gestion de la protection des données