LA RÉGLEMENTATION GÉNÉRALE SUR LA PROTECTION DES DONNÉES (RGPD) AU SEIN D'UNE MSP : UNE OBLIGATION

AVEC Santé Nouvelle Aquitaine

5 ÉTAPES

1 NOMMER UN DPO

Choisir un délégué à la protection des données est une obligation légale. Il est un allié pour gérer les questions liées à la protection des données personnelles. Celui ci peut être membre de la MSP ou un prestataire extérieur (mutualisé?) mais doit être formé et indépendant du processus de traitement des données de la structure.
https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

2 CRÉER LES OUTILS

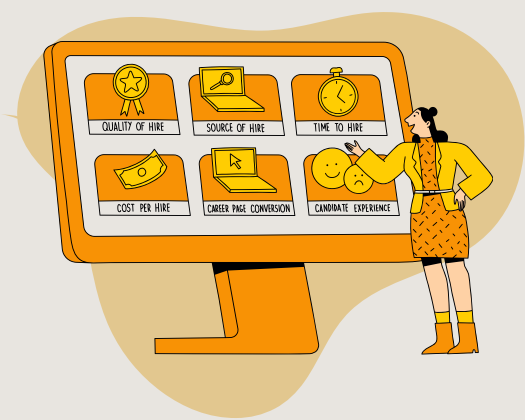
Créer un registre des traitements de données personnelles vous donne une vision complète de vos activités de traitement et facilite l'analyse approfondie de ces processus : Quelles données, qui y accède et comment sont elles traitées? Il s'agit d'une analyse des pratiques afin d'objectiver celles qui ne seraient pas règlementaires.

3 INFORMER LES PATIENTS

Établir une communication claire avec les patients pour garantir une transparence totale dans le traitement de leurs données personnelles au sein de votre MSP.
Quelles sont les données concernées, comment sont elles traitées et par qui, et surtout pour quelle finalité?

4 METTRE À JOUR LE SITE WEB

N'oubliez pas l'importance du site web pour la conformité. Il reflète les activités de la MSP, d'où la nécessité d'une politique de confidentialité à jour. Mais la RGPD ne concerne pas que les données numériques. Veillez aussi aux données stockées ailleurs!



5 FORMER L'EQUIPE

La MSP doit s'assurer que tous ceux qui manipulent des données (médecins, infirmiers, personnel administratif, etc.) respectent les réglementations. Elle doit donc former son personnel pour éviter toute violation de données

LA RGPD EST UN RÈGLEMENT QUI S'APPLIQUE POUR TOUTE PERSONNE OU ENTITÉ QUI TRAITE DES DONNÉES PERSONNELLES, MAIS QU'ENTEND-ON PAR LÀ?

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :
- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :
- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1[@]email.fr ») ne sont pas, en principe, des données personnelles.

ET LES DONNÉES SENSIBLES?

Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

A ce titre, les équipes coordonnées sont réputées traiter des données sensibles et doivent se mettre en conformité vis à vis du RGPD afin d'éviter toute sanction de la CNIL!