Mathias | Avocats

VOS BRÈVES

14 avril 2025

DONNÉES DE SANTÉ

« Les attaques les plus violentes dont sont victimes les hôpitaux sont le fait de **rançongiciels** qui, par le cryptage des données, conduisent à la paralysie du système d'information hospitalier et comportent la menace de divulgation des données de santé et de leur revente. »

10 %

des victimes d'attaques par des rançongiciels étaient des hôpitaux, publics ou privés, en 2023.

3ème

Les hôpitaux sont au 3ème rang des secteurs les plus touchés par les cyberattaques, après les collectivités territoriales et les PME.

Source: Rapport de la Cour des Comptes, La sécurité informatique des établissements de santé, janvier 2025

La Commission européenne publie son plan d'action visant à renforcer la cybersécurité des hôpitaux et prestataires de soins de santé

Ce plan d'action, qui fait partie des orientations politiques 2024-2029 de la Commission, vise à renforcer l'amélioration de la détection des menaces, de la préparation et de la réaction aux crises dans le secteur des soins de santé.

Plus spécifiquement, ce plan d'action :

- met l'accent, en premier lieu, sur la prévention : renforcer les capacités du secteur à prévenir les incidents de cybersécurité,
- détaille les actions pour améliorer le partage d'informations sur la cybersécurité et la capacité à détecter les cybermenaces, ce qui permet de réagir plus rapidement,
- prévoit des mesures visant à améliorer la réaction et la résilience aux incidents.

Consulter le plan d'action de la Commission (en anglais)

Entrée en vigueur du Règlement européen EHDS (3025/327)

Le Règlement du 11 février 2025 (publié le 5 mars 2025) pour un **espace européen des données de santé** est entré en vigueur le 26 mars 2025. Il établit un cadre visant à améliorer l'accès des personnes physiques à leurs données de santé électroniques à caractère personnel et leur contrôle sur ces données dans le contexte des soins de santé.

Objectifs principaux :

✅ **Faciliter l'accès des personnes concernées à leurs données de santé** : leur droit d'accès et de rectification devrait être facilité et gratuit.

✅ **Faciliter l'échange transfrontalier de données de santé** : assurer l'interopérabilité des systèmes de santé dans toute l'UE (format harmonisé).

✅ **Soutenir la recherche et l'innovation** : en facilitant l'accès à des données anonymisées aux chercheurs (pour encourager le développement de traitements médicaux, etc.) et aux décideurs politiques et institutions (élaboration, des politiques de santé, préparation à la gestion de crises sanitaires).

Mesures clés:

➡️**Accès immédiat et gratuit** : Les citoyens européens auront accès à certaines catégories prioritaires de données (résumés patients, prescriptions électroniques, résultats de laboratoire, etc.) via un service électronique.

➡️**Ajout et rectification des données :** Les utilisateurs pourront compléter leur dossier de santé électronique avec des informations personnelles, clairement distinguées de celles validées par des professionnels. Ils auront également la possibilité de demander gratuitement et rapidement, via une plateforme en ligne, la correction de données incorrectes.

➡️**Interopérabilité à l'échelle de l'UE** : Les systèmes de dossiers de santé électroniques (DSE) devront adopter des normes communes pour garantir des échanges fluides, sécurisés et harmonisés des données entre les États membres

Règlement EHDS

La CNIL publie son bilan d'action 2024 concernant les sanctions…

En 2024, 87 sanctions ont été prononcées par la CNIL, pour un montant total de plus de 55 millions d'euros. La CNIL a en outre prononcé 180 mises en demeure (décision de la présidente de la CNIL ordonnant à un organisme de se mettre en conformité dans un délai fixé). Parmi les thématiques majeures abordées dans ces mises en demeure figurent :

- **L'accès au dossier patient informatisé (DPI)** : ce dossier centralise l'ensemble des données de santé des patients pris en charge au sein d'un établissement de santé. Il permet aux professionnels de santé d'accéder facilement à leurs informations médicales. La CNIL a mis en demeure plusieurs établissements de santé de prendre les mesures permettant d'assurer la sécurité du dossier patient informatisé, rappelant que les données des patients ne doivent être accessibles qu'aux personnes justifiant du besoin d'en connaître."

Le bilan 2024 des sanctions et mesures correctrices de la CNIL

…ainsi que le bilan 2024 des demandes d'autorisation des traitements de données en santé

Le 7 avril dernier, la CNIL a aussi publié son bilan concernant les demandes d'autorisation pour des traitements de données de santé. Sur 619 demandes d'autorisation reçues (soit 20% de plus qu'en 2023), 397 autorisations ont été délivrées par la CNIL, 3 ont été refusées. La proportion de demandes classées sans suite et refusées diminue par rapport à 2023.

La qualité des dossiers reçus s'améliore, entraînant une réduction des délais d'instruction (65 jours, en moyenne, contre 72 en 2023).
La CNIL réaffirme son engagement à accompagner les acteurs de la santé à travers des fiches pratiques et un webinaire. Elle annonce actualiser ses référentiels santé en tenant compte des contributions issues de sa récente consultation publique.

Demandes d'autorisations de santé : bilan 2024

Voir l'article du blog sur les axes de contrôle de la CNIL pour 2025

Un laboratoire de recherche sanctionné à hauteur de 85 000 euros en Estonie

Le 10 janvier dernier, le laboratoire de recherches génétiques Asper Biogene a été sanctionné par l'autorité de protection des données estonienne. En cause :

- Une cyberattaque entraînant une fuite de données de 100 000 dossiers contenant des données de santé et des données génétiques, résultant d'une insuffisance des mesures de sécurité.
- Un délégué à la protection des données (DPO) dont la position au sein du management n'est pas compatible avec les exigences en matière d'indépendance.

Voir l'article du blog « Cyberattaque : comment déposer plainte auprès du Procureur de la République ?

Sanction prononcée par l'autorité espagnole à l'encontre d'une société médicale en oncologie

Le 14 mars dernier, la Société d'Oncologie Médicale espagnole a été sanctionnée à hauteur de 42 000 euros par l'autorité de protection des données espagnole (AEPD).

En cause, une cyberattaque sur une application mobile recueillant des données de santé. Le contrat de sous-traitance de la Société avec le fournisseur d'application ne prévoyait pas les mesures de sécurité minimales auxquelles ce dernier doit se conformer.

Autre sanction récemment prononcée par l'autorité espagnole : le 12 février dernier, c'est un journal espagnol (les publications « Baraca ») qui a été sanctionné à hauteur de 6 000 euros. Le journal avait publié un article divulguant les données de santé d'une personne physique : l'autorité n'a pas considéré que la publication de ces données était « nécessaire à la finalité informative de l'article ».

Notre article « Droit d'accès : comment le mettre en œuvre ? »

Décision de l'AEPD

POUR ALLER PLUS LOIN : VOS FORMATIONS

Mathias | Avocats

Violation de données : L'essentiel pour maîtriser les enjeux clés et réussir votre mise en conformité

Objectifs :
- Maîtriser la définition d'une violation de données à caractère personnel
- Maîtriser une notification de données auprès de l'autorité de contrôle
- Connaître les coopérations entre responsables de traitements et sous-traitant

Compétences visées :
- Connaître les enjeux d'une violation de données
- Appréhender la notification d'une violation
- Déterminer les risques sur les personnes concernées

Pour qui ? Aucun prérequis
Juristes, DPO, Direction de la conformité, toute personne intéressée par ce sujet.

Sessions – Délai d'entrée
Intra-entreprise : nous consulter
Taille du groupe : nous consulter
Inscription : contact@avocats-mathias.com

Durée : 4 heures, en présentiel – continu
Profitez de ce format court et concis, entre professionnels ; tout en conciliant cette formation avec votre agenda d'activités professionnelles quotidiennes.

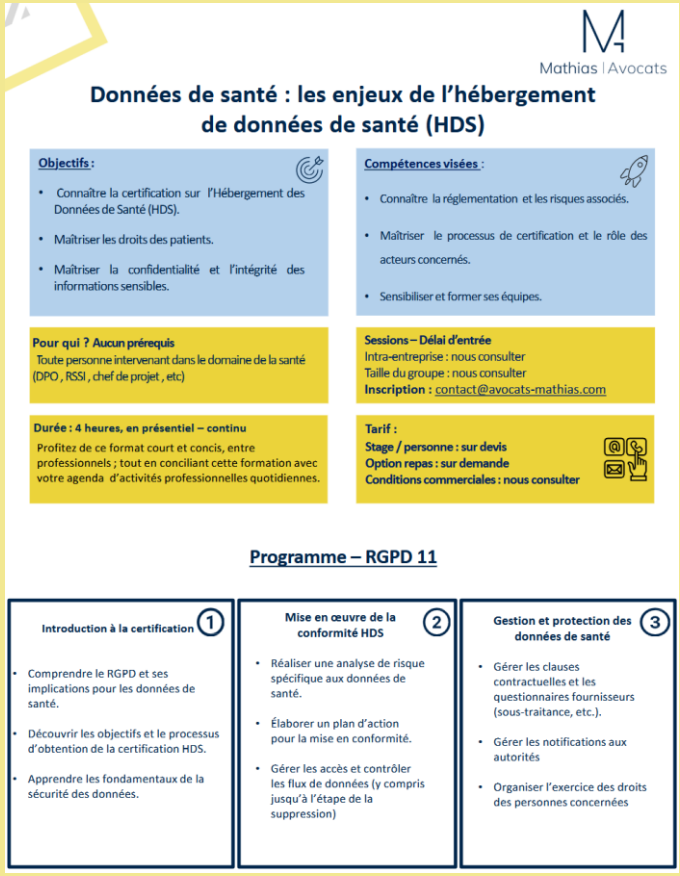
Tarif :
Stage / personne : sur devis
Option repas : sur demande
Conditions commerciales : nous consulter

Programme – RGPD 10

Quelles sont les obligations ? 1
- Qu'est-ce qu'une violation de données à caractère personnel ? notion et illustrations
- Comment évaluer l'existence d'un risque ou d'un risque élevé ?
- Quelle notification de la violation de données à l'autorité de contrôle ? délais, forme et contenu –Illustrations.

Comment gérer? 2
- Quelle procédure de gestion mettre en œuvre ?
- Quel est le rôle du DPO? Comment documenter(registre des violations, etc.)
- Comment communiquer aux personnes concernées ? (délais, forme et contenu)

Quelles sanctions ? Quelles sont les bonnes pratiques ? 3
- Quelle sanction en l'absence de notification et/ou de communication de la violation de données ?
- L'existence d'une violation de données peut-elle constituer un manquement à l'obligation de sécurité?
- Quelle coopération entre responsables de traitement et/ou avec un sous-traitant ?



Mathias | Avocats

Données de santé : les enjeux de l'hébergement de données de santé (HDS)

Objectifs :
- Connaître la certification sur l'Hébergement des Données de Santé (HDS).
- Maîtriser les droits des patients.
- Maîtriser la confidentialité et l'intégrité des informations sensibles.

Compétences visées :
- Connaître la réglementation et les risques associés.
- Maîtriser le processus de certification et le rôle des acteurs concernés.
- Sensibiliser et former ses équipes.

Pour qui ? Aucun prérequis
Toute personne intervenant dans le domaine de la santé (DPO , RSSI , chef de projet , etc)

Sessions – Délai d'entrée
Intra-entreprise : nous consulter
Taille du groupe : nous consulter
Inscription : contact@avocats-mathias.com

Durée : 4 heures, en présentiel – continu
Profitez de ce format court et concis, entre professionnels ; tout en conciliant cette formation avec votre agenda d'activités professionnelles quotidiennes.

Tarif :
Stage / personne : sur devis
Option repas : sur demande
Conditions commerciales : nous consulter

Programme – RGPD 11

Introduction à la certification 1
- Comprendre le RGPD et ses implications pour les données de santé.
- Découvrir les objectifs et le processus d'obtention de la certification HDS.
- Apprendre les fondamentaux de la sécurité des données.

Mise en œuvre de la conformité HDS 2
- Réaliser une analyse de risque spécifique aux données de santé.
- Élaborer un plan d'action pour la mise en conformité.
- Gérer les accès et contrôler les flux de données (y compris jusqu'à l'étape de la suppression)

Gestion et protection des données de santé 3
- Gérer les clauses contractuelles et les questionnaires fournisseurs (sous-traitance, etc.).
- Gérer les notifications aux autorités
- Organiser l'exercice des droits des personnes concernées

Catalogue des formations

Mathias Avocats est certifié Organisme de formation

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Ensemble, développons vos projets et formons vos équipes! Partageons nos expertises !

Ces Brèves vous sont offertes par Mathias Avocats.
Nous sommes à votre disposition pour échanger sur vos brèves personnalisées.

Mathias Avocats
19, rue Vernier – 75017 Paris
www.avocats-mathias.com
contact@avocats-mathias.com
Tél. 01 43 80 0 201

VOS BRÈVES