

FORMATION

RGPD & Protection des données de santé dans le contexte du PMSI

Formation unifiée — 7 heures — Public mixte

Directeurs généraux · Responsables DIM · Équipes soignantes

Niveau : intermédiaire (conformité 2018 réalisée — mise à jour)

Caractéristiques	Détail
Durée	7h (9h00–17h00 avec pauses)
Public	Mixte : DG, DIM, soignants, secrétaires
Niveau	Intermédiaire — mise à jour post-2018
Format	Présentiel avec ateliers pratiques
Participants	12 maximum pour garantir l'interactivité
Ratio théorie/pratique	40% apports — 60% ateliers

Positionnement pédagogique

Cette formation part d'un constat fréquent dans les établissements de santé : la mise en conformité RGPD de 2018 a été réalisée, mais elle n'a pas été actualisée. Or trois évolutions majeures ont rendu cette conformité partielle.

Ce qui a changé depuis 2018	Pourquoi c'est un risque	Ce que la formation apporte
Multiplication des cyberattaques en santé	Vos mesures de 2018 ne couvrent pas les menaces actuelles	Panorama des incidents récents + bonnes pratiques actualisées

Ce qui a changé depuis 2018	Pourquoi c'est un risque	Ce que la formation apporte
Référentiel HDS révisé, doctrine numérique en santé	Votre DPI, entrepôt de données ou télémédecine peut être hors conformité	Cartographie des nouvelles obligations réglementaires
Nouveaux usages : IA, BI, e-santé, télémédecine	Des traitements non documentés = des risques non maîtrisés	Ateliers de mise à jour du registre et des PIA
Renforcement des sanctions CNIL (jusqu'à 20 M€)	Un incident = exposition directe du dirigeant et de l'établissement	Responsabilités clarifiées pour chaque public présent

Objectifs pédagogiques

À l'issue de cette journée, chaque participant sera capable de :

- Situer les évolutions réglementaires et cyber depuis la mise en conformité initiale
- Identifier les nouveaux traitements de données à risque dans son contexte métier
- Mettre à jour sa pratique : registre, PIA, habilitations, gestion des incidents
- Adopter les bons réflexes au quotidien selon son rôle (direction, DIM, soignant)
- Construire un plan d'action personnalisé et priorisé pour son établissement

Argumentaire pour les HAD :

Pour les directeurs généraux :

La mise en conformité RGPD de 2018 était un point de départ, pas une destination. Depuis, les cyberattaques contre les établissements de santé ont explosé, les textes ont évolué (recours aux hébergeurs de données de santé (HDS) tels que définis dans l'Article L1115-1 du Code de la santé publique, doctrine du numérique en santé), et votre système d'information a profondément changé. Votre conformité d'hier ne couvre pas vos risques d'aujourd'hui.

Un incident de sécurité sur des données de santé, c'est jusqu'à 4 % de votre chiffre d'affaires annuel en sanction CNIL — mais surtout, c'est une perte de confiance irrémédiable de vos patients et de vos partenaires.

Pour les responsables DIM :

Les données PMSI ne sont pas seulement des données administratives : elles permettent d'inférer des diagnostics, des traitements, des parcours de vie. Leur

compromission engage votre responsabilité directe et celle de l'établissement. Avez-vous formalisé vos flux de données, vos habilitations, votre traçabilité des accès ?

La pseudonymisation que vous pratiquez pour l'envoi à l'ATIH est une obligation réglementaire. Mais qu'en est-il de l'usage interne de ces données — croisements, exports, tableaux de bord ? Ces usages sont souvent les angles morts des audits.

Pour les équipes soignantes :

Partager un dossier patient par messagerie non sécurisée, accéder au DPI depuis un poste partagé sans se déconnecter, photographier un écran pour le transmettre à un collègue — ces gestes du quotidien sont des violations de données. Vous êtes en première ligne, et personne ne vous a vraiment expliqué pourquoi.

Je vous propose un programme pour un public mixte ayant déjà des notions et ayant déjà mis en place des éléments en place dans le cadre de leur établissement.

Proposition de programme de formation

Public

- Direction générale
- Direction qualité
- DIM
- Médecins
- Cadres de santé
- Référents PMSI
- Responsables SI
- DPO

Durée

- 1 journée (7 heures) ou 2 demi-journées

Module 1 – Pourquoi reparler du RGPD aujourd'hui ? (45 min)

Objectifs

- Comprendre l'évolution des risques depuis 2018.
- Identifier les nouvelles responsabilités des établissements.

Contenu

- Évolution des menaces cyber dans le secteur santé.
- Augmentation des sanctions et contrôles.
- Les données de santé : un patrimoine stratégique.
- Cas concrets d'incidents dans des établissements de santé.

Module 2 – Les fondamentaux du RGPD appliqués à la santé (1h15)

Objectifs

- Revoir les principes essentiels.
- Comprendre les spécificités des données de santé.

Contenu

- Données personnelles et données sensibles.
- Base légale des traitements.
- Information des patients.
- Durées de conservation.
- Droits des personnes.
- Secret médical et RGPD : différences et complémentarités.

Module 3 – PMSI, DIM et valorisation des données (1h30)

Objectifs

- Sécuriser les pratiques liées au PMSI.
- Comprendre les responsabilités associées aux données médico-économiques.

Contenu

- Circuit de la donnée PMSI.
- Accès et habilitations.
- Pseudonymisation et anonymisation.
- Partage des données avec prestataires et consultants.
- Cas particuliers : requêtes, études, benchmarking, recherche.

Atelier

Analyse d'un cas concret de demande d'extraction de données PMSI.

Module 4 – Risques opérationnels rencontrés par les soignants (1h15)

Objectifs

- Identifier les situations à risque du quotidien.

Contenu

- Envoi de données par mail.
- Utilisation de clés USB.
- Télétravail.
- Messageries instantanées.
- Photographies de patients.
- Échanges avec les familles.
- Gestion des accès aux dossiers.

Atelier

Quiz interactif et analyse de situations réelles.

Module 5 – Cyberattaques et violations de données (1h)

Objectifs

- Comprendre les mécanismes d'une fuite de données.
- Savoir réagir efficacement.

Contenu

- Ransomwares.
- Phishing.
- Usurpation d'identité.
- Procédure de gestion de crise.
- Notification des violations.

Étude de cas

Simulation d'incident de sécurité.

Module 6 – Gouvernance et responsabilités des dirigeants (45 min)

Objectifs

- Comprendre les responsabilités des décideurs.

Contenu

- Rôle de la direction.
- Rôle du DPO.
- Rôle du DIM.
- Cartographie des risques.
- Pilotage des actions correctrices.
- Indicateurs de conformité.

Module 7 – L'IA, les outils numériques et les nouveaux défis (30 min)

Objectifs

- Anticiper les enjeux émergents.

Contenu

- Intelligence artificielle générative.

- Copilotes numériques.
- Hébergement cloud.
- Réutilisation des données de santé.
- Bonnes pratiques et vigilance.