G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Protection des données de santé et vie privée

But de la formation

- Apprendre les exigences juridiques et de sécurité en matière de :
  - Protection des données personnelles de santé, y compris le RGPD et la loi Informatique & Libertés 3 dans le cadre de la santé
  - Hébergement des données de santé (certification HDS)
  - Interopérabilité des systèmes d'information de santé (CI-SIS)
  - Sécurité des systèmes d'information de santé (PGSSI-S, CPS, RGS, LPM, NIS)

Pré-requis

- Avoir une culture générale en sécurité des systèmes d'information ou en droit est un plus mais n'est pas imposé
- Pour les participants souhaitant apprendre la certification HDS, il convient d'avoir suivi la formation ISO27001 Lead Implementer avant cette formation

Type de public

- Personnes des secteurs santé et social :
  - RSSI,
  - Juristes,
  - DPO,
  - Toute personne confrontée à la gestion d'un système d'information de santé.

Moyens pédagogiques

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Sanction de la formation

- Cette formation n'est pas certifiante.
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec échanges interactifs

Durée

21 heures (3 jours).

G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme

Module 1 : Présentation du contexte

- Cadre légal et normatif
- Notions fondamentales
- Données de santé, dossier médical partagé, systèmes d'information, etc...
- Principaux acteurs
    - Patient, Professionnel de santé et médico-social, établissements de santé, hébergeur, ASIP-santé, CNIL, etc.

Module 2 : Droits des patients et secret

- Droits des patients
    - Confidentialité de leurs données de santé, information et accès aux données, droit de rectification et d'opposition, etc.
- Secret
    - Secret professionnel, secret médical, secret partagé

Module 3 : Gestion des données personnelles de santé

- Licéité des traitements de données personnelles
- Recueil des données de santé
- Formalités préalables, PIA
- Elaboration et tenus du registre des activités de traitement
- Conservation, suppression, anonymisation et archivage des données
- Transferts internationaux de données
- Gestion des droits des personnes concernées

Module 4 : Sécurité du système d'information de santé

- Obligations légales de sécurité de données et systèmes d'information de santé
- Enjeux de la sécurité du SI-S : Confidentialité, Intégrité, Disponibilité, Traçabilité et imputabilité
- PGSSI-S

Module 5 : Interopérabilité du système d'information de santé

- Obligation légale d'interopérabilité
- Présentation du cadre d'interopérabilité des systèmes d'information de santé

Module 6 : Hébergement des données de santé

- Exigences légales en matière d'hébergement
- Certification HDS
- Passage de l'agrément de la procédure
- Médecin de l'hébergeur de la procédure d'agrément à la certification

Module 7 : SMSI

- Présentation de la norme ISO 27001
- Organisation de la sécurité
    - Rôles et responsabilités, Politique de sécurité, SMSI
    - Médecin hébergeur
    - Responsabilités vis-à-vis du CSP
- Gestion des risques
    - Appréciation des risques
    - Plan de traitement des risques
    - Déclaration d'applicabilité étendue
    - ISO27018
    - Exigences HDS
- Processus de certification
- Mesures de sécurité opérationnelles
    - Gestion des accès, identification, authentification
    - Classification et chiffrement
    - Architecture réseau et applicative
    - Sécurité des échanges
    - Durcissement des systèmes
    - Objets connectés et accès distants
    - Cycle de vie et obsolescence des systèmes
    - Sauvegarde et archivage
    - Auditabilité (Traçabilité, Imputabilité)
- Gestion des incidents dans les contextes des données de santé
    - Notifications aux autorités
- Gestion de la continuité d'activité