

Formation « Hébergement des données de santé et vie privée »

Réf : SECUSANTE

Le secteur de la santé et du social est encadré par des règles spécifiques c'est pourquoi HS2 propose une formation dédiée pour couvrir ce domaine.

Objectifs

- 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)

Durée & Horaires

- 4 jours soit 28 heures
- 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participants

- Minimum 6 participants – Maximum 24 participants

Public visé

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

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 la formation SECUSANTE.

Méthode pédagogique

- Cours magistral avec échanges interactifs
- Cette formation est proposée en mode présentiel et peut être accessible en mode distanciel via ZOOM pour les personnes qui ne peuvent ou ne veulent pas se déplacer

Supports

- Support de cours en français au format papier en présentiel, au format numérique en distanciel
- 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

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSANTE par HS2.

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
- Élaboration et tenue 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 à la certification
- 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