DAWAN

Plan de la formation

www.dawan.fr

Formation Cybersécurité et conformité dans le secteur de la santé (RGPD / HDS / NIS2)

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 775,00 CHF HT (standard) 1 420,00 CHF HT (remisé)
Public :	Responsables SI / RSSI d'établissements de santé ou d'acteurs e-santé - DPO, juristes, responsables conformité dans le secteur sanitaire et médico-social - Responsables de solutions SaaS / hébergeurs manipulant des données de santé
Pré-requis :	Bonne connaissance de base du RGPD et du fonctionnement d'un SI de santé ou d'un SI hébergeant des données de santé
Objectifs :	Comprendre le cadre règlementaire spécifique au secteur de la santé (RGPD, HDS, NIS2)- Identifier les obligations des établissements de santé et des hébergeurs de données de santé - Cartographier les traitements et les données de santé à caractère personnel pour en mesurer les risques - Structurer une démarche de conformité et de sécurisation des SI de santé- Élaborer un premier plan d'actions pragmatique pour son établissement ou son activité
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102757-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Clarifier le cadre réglementaire spécifique aux données de santé

Rappeler les fondamentaux du RGPD appliqués aux données de santé (données sensibles, bases légales, droits des patients)
Comprendre le cadre légal français applicable aux données de santé (Code de la santé publique, acteurs, responsabilités)
Situer les référentiels HDS et leurs évolutions récentes (nouveau référentiel, calendrier, impacts pour les hébergeurs)
Identifier les cas où la certification HDS est obligatoire et ceux où elle ne l’est pas
Atelier fil rouge : cartographier les principaux textes applicables à son établissement ou à sa solution e-santé

Identifier les traitements et les données de santé à caractère personnel

Recenser les principaux traitements de données de santé dans un établissement ou chez un éditeur e-santé
Différencier les catégories de données (administratives, médicales, facturation, télésanté, recherche, etc.)

Analyser les finalités, les bases légales et les durées de conservation applicables
Identifier les flux de données : internes, externes, hébergeurs, prestataires, dispositifs médicaux connectés
Atelier fil rouge : construire une fiche de registre RGPD pour un traitement de données de santé représentatif

Comprendre les exigences HDS et leur articulation avec le RGPD

Présenter le référentiel HDS (version en vigueur), ses activités et son périmètre d'application
Analyser les obligations de sécurité, de traçabilité, de localisation et de transparence imposées aux hébergeurs de données de santé
Relier les exigences HDS aux principes du RGPD (sécurité, confidentialité, intégrité, disponibilité, accountability)
Identifier les impacts organisationnels et contractuels pour un établissement de santé et pour un prestataire hébergeur
Atelier fil rouge : vérifier, sur un cas d'école, si l'activité exercée nécessite une certification HDS et avec quelles conséquences

Intégrer les apports de NIS2 pour les acteurs de la santé

Comprendre pourquoi et comment certains acteurs de la santé sont concernés par NIS2 (entités essentielles / importantes)
Identifier le lien entre NIS2, RGPD et HDS sur la gestion des risques, la gouvernance et la gestion des incidents
Analyser les obligations de notification d'incidents de sécurité et leur articulation avec les obligations CNIL
Appréhender les sanctions et les attentes en matière de résilience des services de santé numériques
Atelier fil rouge : analyser l'impact d'un incident de sécurité sur un SI de santé et lister les notifications à réaliser

Structurer un dispositif de sécurité et de conformité pour un SI de santé

Définir les rôles et responsabilités : DPO, RSSI, direction, métiers, prestataires, hébergeurs
Mettre en place une démarche de gestion des risques adaptée aux traitements de données de santé
Articuler politiques, procédures, contrats et clauses spécifiques dans le contexte santé / HDS
Prévoir la gouvernance des projets e-santé : privacy by design, sécurité by design,

AIPD lorsque nécessaire

Atelier fil rouge : élaborer les grandes lignes d'un plan d'actions sécurité / conformité pour un projet e-santé

Construire un plan d'actions opérationnel et priorisé

Prioriser les chantiers : données sensibles les plus exposées, dépendances critiques, hébergeurs, dispositifs médicaux

Définir des actions rapides (quick wins) et des actions structurantes à moyen terme

Préparer la relation avec les autorités (CNIL, ANS) et les audits de certification HDS éventuels

Identifier les besoins en formation et sensibilisation des équipes (médical, administratif, IT, partenaires)

Atelier fil rouge final : formaliser une feuille de route sur 12 à 18 mois pour renforcer la conformité RGPD / HDS / NIS2 de son SI de santé