Les 12 Normes Santé à connaître !

1 RGPD ET LOI INFORMATIQUE & LIBERTÉ

Concerne tout le monde

Vous développez un produit impliquant des données à caractère personnel : les traitements réalisés doivent être conformes au RGPD.

OBLIGATOIRE

Focus cyber

Vous devez intégrer les principes du RGPD dès la conception de votre dispositif médical. Par exemple, les données que vous traitez doivent être limitées au strict nécessaire !

2 ISO 14791 : EVALUATION DES RISQUES ASSOCIÉS À UN DM

Concerne les DMIL

Vous souhaitez obtenir le marquage CE pour votre Dispositif Médical intégrant un Logiciel (DMIL). Une évaluation des risques est recommandée.

FACULTATIF ET NON CERTIFIANT

Focus cyber

Lorsque vous réalisez votre analyse de risques, pensez à intégrer les risques cyber. Par exemple, si votre DMIL intègre des données, assurez-vous d'avoir envisagé une bonne redondance des sauvegardes !

3 MARQUAGE CE, MDR 2017/745

Concerne les DMIL

Les fabricants de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro doivent détailler les mesures de sécurité appliquées au DM.

OBLIGATOIRE POUR COMMERCIALISER UN DISPOSITIF MÉDICAL

Focus cyber

Lors de l'examen de votre dossier marquage CE, une attention particulière est portée à vos mesures de sécurité informatique (la gestion des accès notamment !).

4 NIS 2 – NETWORK AND INFORMATION SECURITY

Concerne les DMIL

Les fabricants de dispositifs médicaux sont considérés comme des "entités importantes". Ils doivent respecter des normes de sécurité informatique.

OBLIGATOIRE DANS LE CADRE DES DM

Focus cyber

En qualité de fabricants de DM, vous êtes la cible de cyberattaques. A ce titre, vous êtes tenus de disposer d'un programme de cybersécurité complet (politique de sauvegarde, reprise d'activité, veille des menaces, etc.) !

5 NIS 2 – NETWORK AND INFORMATION SECURITY

Concerne les prestataire informatiques

Dans le cadre de partenariats avec des “entités essentielles” ou “entités importantes”* vous intégrez leur chaîne de risques et devez alors démontrer des mesures de sécurité.

OBLIGATOIRE

** Voir les définitions plus bas !*

Focus cyber

Ces entités sont susceptibles d’auditer votre système de Management du SI, en vous demandant par exemple de fournir une PSI.

6 ISO 27001 – SYSTÈME DE MANAGEMENT DU SI

Concerne la e-santé

La norme ISO 27001 offre un cadre complet de la mise en place d’une gouvernance de la sécurité du SI. Il est possible de faire certifier votre SMSI. Cette certification est obligatoire dans le cadre d’une qualification HDS.

Focus cyber

La norme ISO 27001 est le texte de référence afin de développer un programme de cybersécurité efficace. Il vous permettra de créer des politiques et procédures afin de sécuriser votre société et vos partenaires.

OBLIGATOIRE

SI HDS
FACULTATIF MAIS FORTEMENT RECOMMANDÉ (NIS2)

7 ISO 13485

SYSTÈME DE MANAGEMENT DE LA QUALITÉ RELATIF AUX ORGANISMES FOURNISSANT DES DISPOSITIFS MÉDICAUX

Concerne les DMIL

La norme de référence pour démontrer l’aptitude d’une société à fournir des dispositifs médicaux sécurisés.

FACULTATIF ET CERTIFIANT

Focus cyber

La cybersécurité d’un dispositif médical est un élément particulièrement observé par vos partenaires. La capacité de présenter une analyse de risques efficace est un élément à valoriser !

8 ISO 27701

STANDARD POUR LE MANAGEMENT DES INFORMATIONS PERSONNELLES

Concerne la e-santé

La norme ISO 27701 permet de démontrer à vos partenaires votre conformité au RGPD et votre gouvernance des données personnelles.

FACULTATIF MAIS RECOMMANDÉ POUR RGPD

Focus cyber

La norme ISO 27701 permet aux startups de la santé de démontrer leur bonne gestion des données à caractère personnel. Le texte offre un framework au sein des systèmes d’information de la société : procédures de sauvegardes, politique de conservation, etc.

9 PGSSIS – RÉFÉRENTIEL D'IDENTIFICATION ÉLECTRONIQUE DES ACTEURS DES SECTEURS DE SANTÉ

Concerne la e-santé

Vous traitez des données de santé dans le cadre de votre solution numérique, vous êtes tenus au respect des référentiels de la PGSSIS.

OBLIGATOIRE

OBLIGATOIRE SI DES ACTEURS DE LA SANTÉ S'IDENTIFIENT SUR VOTRE SOLUTION NUMÉRIQUE.

Focus cyber

Afin de mieux sécuriser les utilisateurs, vous devez respecter des exigences en matière d'authentification, en utilisant par exemple des certificats au standard x509 !

10 PGSSIS – RÉFÉRENTIEL D'IDENTIFICATION ÉLECTRONIQUE DES PATIENTS

Concerne la e-santé

Détermine les règles associées à la bonne authentification des patients au sein du SI.

OBLIGATOIRE

OBLIGATOIRE SI DES PATIENTS S'IDENTIFIENT SUR VOTRE SOLUTION NUMÉRIQUE.

Focus cyber

Lorsque vous développez votre solution, vous devez respecter les exigences relatives au choix de mots de passe : 8 caractères minimum, chiffres et lettres, etc.

11 PGSSIS – RÉFÉRENTIEL IMPUTABILITÉ

Concerne la e-santé

Détermine les règles associées à la collecte et la conservation des traces.

OBLIGATOIRE

Focus cyber

La sécurisation des données passe également par votre capacité à collecter des traces des utilisateurs qui utilisent votre outil : pensez à déployer des outils de journalisation des logs !

12 REREFENTIEL D'INTEROPÉRABILITÉ ET DE SECURITE DES DISPOSITIFS MÉDICAUX NUMERIQUES

Concerne les DMIL

Le référentiel précisant les garanties attendues en matière d'intéropérabilité lors de la création d'un DMN.

OBLIGATOIRE

Focus cyber

Afin de faciliter la transmission des données entre tous les acteurs de la santé, les données doivent respecter des formats communs. Le référentiel détaille les mesures à prendre pour s'assurer de la bonne portabilité des données !

Vocabulaire

- **E-BIOS RM** : méthode d'analyse de risques recommandée par l'ANSSI
- **SMSI** : système de management du système d'information
- **Actifs** : toute ressource, information matérielle ou immatérielle qui a de la valeur pour la structure
- **PSI** : politique de sécurité de l'information
- **Entité Essentielle (EE)**: au sens de NIS2, les grandes entreprises qui fournissent des services considérés comme critiques (prestataires de soin, laboratoires de référence, fabricants de DM critiques en cas d'urgence de santé publique, etc.)
- **Entité Importante (EI)** : au sens de NIS2, les entreprises non-essentielles, qui réalisent des services critiques : les fabricants de DM et DM in-vitro notamment.