TOOLKIT CYBERSÉCURITÉ

Vous êtes une entreprise innovante de la e-santé ?

La cybersécurité doit être au cœur de votre stratégie dès les premières étapes.

En prenant en compte ces **10 questions** essentielles, vous pourrez construire une **première base solide de cybersécurité**, adaptée aux particularités de la santé et aux exigences croissantes du numérique en santé.

Dans un environnement où les **données sensibles des patients** sont au cœur de votre activité, leur protection est non seulement une **obligation légale**, mais aussi un **levier de confiance puissant auprès de vos clients et vos investisseurs**.

ASSURER LA CONFORMITÉ ET DÉFINIR UNE STRATÉGIE

1) Quelles sont mes obligations ?

En tant qu'entreprise innovante de la e-santé, je peux être soumis à diverses réglementations françaises et européennes. Voici les principales obligations auxquelles je dois répondre :

- Mettre en place des processus pour garantir la conformité au **règlement général sur la protection des données (RGPD)** qui impose des exigences strictes sur la collecte, le stockage et la gestion des données personnelles, dont celles relatives à la santé.
- Héberger mes données de santé chez un **hébergeur certifié HDS** ou être moi-même certifié HDS.
- Être conforme à la **PGSSI-S, en particulier au Référentiel d'Identification Électronique**.

2) Quelles sont les données sensibles que je traite ? Comment est-ce que je les protège ?

La protection des données sensibles est essentielle pour garantir la confidentialité, prévenir les abus, et maintenir la confiance des utilisateurs tout en respectant la vie privée et le secret médical. Pour cela, je dois :

- Identifier les **typologies de données sensibles** traitées par l'entreprise (informations de santé, données personnelles, historiques médicaux, etc.).
- Mettre en place des **mécanismes de protection adaptés** (ex : chiffrement, anonymisation des données).
- Utiliser des **protocoles de chiffrement sécurisés** (ex : TLS) pour protéger les données en transit, en particulier lors des échanges avec les patients, les professionnels de santé ou les partenaires externes.

3) Mes collaborateurs sont-ils sensibilisés à la cybersécurité ?

L'humain est la première faille de sécurité dans de nombreuses cyberattaques. Il est donc essentiel de sensibiliser et de former mes employés aux enjeux de la sécurité. Pour cela, je dois :

- Formaliser une **charte informatique**, diffusée à l'ensemble de l'entreprise.
- Mettre en place des **formations régulières** pour les employés afin qu'ils comprennent les **enjeux de cybersécurité**, les **bonnes pratiques à adopter** (gestion des mots de passe, détection de phishing, etc.) et les **risques spécifiques liés au numérique en santé**.

4) La sécurité de mes tiers est-elle évaluée ?

Les tiers peuvent représenter une porte d'accès pour un cyberattaquant et, si leurs pratiques de sécurité sont insuffisantes, rendre vulnérables mes données sensibles par le biais de nos interconnexions ou d'échanges non sécurisés. Je dois ainsi :

- Identifier les **différents types de tiers** : accédants, propriétaires, sous-traitants, fournisseurs, prestataires de services de (télé)maintenance et support, partenaires R&D, utilisateurs externes…
- Formaliser un **Plan d'Assurance Sécurité (PAS),** incluant les **exigences** que mes partenaires doivent respecter ainsi qu'une **répartition claire des responsabilités** avec l'entreprise (matrice RACI).
- S'assurer que les **prestataires ayant accès à des données sensibles** ou à des systèmes critiques font l'objet d'**audits de sécurité réguliers**, réalisés par des auditeurs reconnus ou des équipes internes qualifiées, en lien avec les exigences du PAS.

PROTÉGER LE SYSTÈME D'INFORMATION

5) Quels mécanismes de contrôle d'accès ai-je mis en place ?

La gestion des accès (IAM) est essentielle pour garantir que seules les personnes autorisées accèdent aux informations sensibles, minimisant ainsi les risques de violations de données. Pour cela, je dois :

- Identifier **qui peut accéder à quelles données** et tenir à jour un **inventaire des comptes à privilèges**.
- Appliquer le **principe du moindre privilège** : chaque utilisateur ne dispose que des accès nécessaires à son rôle.
- Assurer une authentification sécurisée : définir une **politique de mots de passe robustes** et recourir aux outils d'**authentification forte (MFA).**

6) Comment la sécurité de mon parc informatique est-elle assurée ?

La sécurité du parc informatique est essentielle pour protéger les données sensibles, garantir la disponibilité des services et prévenir les intrusions qui pourraient compromettre la confidentialité et l'intégrité du SI.

- Tenir à jour une **cartographie du parc**, en identifiant les actifs critiques et les services exposés sur internet.
- Déployer un **antivirus** sur l'ensemble des serveurs et des postes de travail.
- Configurer de manière sécurisée les **accès Wi-Fi** avec un chiffrement robuste (ex : WPA3) et des mots de passe forts et uniques.
- Déployer des solutions de **segmentation du réseau** (pare-feu, WAF, VLANs, DMZ, micro-segmentation…) pour isoler les systèmes critiques et ainsi limiter la propagation et les impacts d'une compromission.

7) Comment mes développements sont-ils sécurisés ?

La sécurité des développements est essentielle pour prévenir les vulnérabilités dans le code qui pourraient être exploitées. Voici quelques actions clés pour renforcer la sécurité des processus de développement :

- Sécuriser les **processus de développement (CI/CD)**, y compris la **gestion des secrets et des clés API**.
- Réaliser des **revues de code** et des **tests de sécurité** (ex : scans de vulnérabilités, tests d'intrusion).
- Mettre en place des **outils de vérification de la sécurité du code**.

ANTICIPER ET RÉAGIR FACE AUX CYBERATTAQUES

8) Quels outils de surveillance et de détection ai-je déployés ?

Pour renforcer la sécurité de mon SI et prévenir les risques, je dois être en mesure de détecter rapidement toute activité suspecte ou vulnérabilité.
Voici les actions à envisager :

- Gérer proactivement les **mises à jour (correctives ou de version)** pour limiter l'exposition aux vulnérabilités.
- Mettre en place des **outils de surveillance en temps réel** (sondes IDS/IPS, SIEM, EDR…).
- Formaliser des **processus pour analyser les logs** et identifier les anomalies.

9) Mon entreprise sait-elle comment réagir en cas de cyberattaque ?

Lors d'une cyberattaque, une réponse rapide et bien coordonnée permet de limiter les pertes financières, protéger les données sensibles, maintenir la confiance des parties prenantes et respecter les obligations légales. Il est donc essentiel de :

- Formaliser des **fiches réflexes** par type de cyberattaque (ex : ransomware) et rappeler les bonnes pratiques aux collaborateurs (déconnecter le poste, contacter la personne en charge de l'IT, ne pas divulguer d'informations sensibles sur l'attaque).
- Mettre en place un **plan de réponse aux incidents** qui détaille la procédure à suivre en cas de violation de données, en incluant la **notification aux autorités compétentes (ex : 72h au plus tard pour la CNIL)** et aux personnes concernées dans les délais impartis.
- Organiser des **exercices de gestion de crise** cybersécurité pour s'entraîner et améliorer le processus.

10) Quels processus garantissent la continuité de service en cas d'attaque ou de panne ?

Pour assurer la résilience face aux incidents et limiter les pertes financières et opérationnelles, il convient de :

- Disposer de **supports de sauvegarde diversifiés** selon la règle du « 3-2-1 » (3 copies, dans 2 lieux différents avec 1 copie hors ligne) à tester régulièrement.
- Formaliser un **plan de continuité des activités (PCA) et de reprise après sinistre (DRP)** pour assurer que mes services restent opérationnels en cas de cyberattaque majeure ou de défaillance système.
- **Tester et à mettre à jour le PCA et le DRP,** idéalement une fois par an.

RESSOURCES UTILES

Corpus documentaire PGSSI-S
Certification Hébergeur de Données de Santé (HDS)
Panorama des principales réglementations applicables

Fiches synthétiques sur la Sécurité du SI
Sensibiliser et Former
Gestion des identités et des accès
Authentification multifacteur (MFA)
Politique de mots de passe
Cartographie du parc informatique
Configuration sécurisée de l'accès Wi-Fi
Gestion des mises à jour et sécurité
Log management
Réagir à un acte de cyber malveillance
Gestion des sauvegardes
Cyber résilience : PCA & PRA

Règlement Général sur la Protection des Données

Guide d'hygiène informatique de l'ANSSI
Recommandations relatives à l'administration sécurisée des SI

Socle interministériel de logiciels libres

Top 10 des vulnérabilités de cybersécurité

CONTACTS

Équipe Innovation : Innovation@esante.gouv.fr