Politique générale de sécurité des systèmes d'information de santé

EN BREF

Depuis 9 ans, la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) guide les professionnels des secteurs santé, médico-social et social pour la protection des données de santé des usagers.

- Elle prend en compte le respect de la vie privée, favorise le développement du numérique en santé et la confiance des acteurs.
- La PGSSI-S regroupe des référentiels thématiques (identification électronique des acteurs, force probante des documents de santé, imputabilité des actions…) et des guides pratiques, qui rappellent aux différents acteurs des systèmes d'information de santé les bonnes pratiques pour être en conformité avec la réglementation en vigueur.

La sécurité des SI de santé : une gestion des risques à organiser

Le développement rapide de l'**usage du numérique en santé** constitue un facteur important d'**amélioration de la qualité des soins**.

Il s'accompagne toutefois d'un **accroissement significatif des menaces et des risques d'atteinte aux informations** conservées sous forme électronique et plus généralement aux processus de santé s'appuyant sur les systèmes d'information de santé.

La gestion des risques de sécurité des systèmes d'information (SSI), tout comme la conformité au règlement européen sur la protection des données personnelles (RGPD), s'inscrivent dans la démarche **globale de gestion des risques** portée par les structures de santé pour améliorer la qualité et la sécurité des soins.

L'élaboration de la PGSSI-S

Face à ces enjeux, L'Etat a confié à l'Agence du Numérique en Santé (ANS) l'élaboration et la publication de la **politique générale de sécurité des systèmes d'information de santé** (PGSSI-S), **cadre devant être respecté par tous les acteurs de la santé, du social et du médico-social** pour sécuriser les systèmes d'information de santé (SIS). L'article L. 1470-5 du code de la santé publique prévoit en effet que l'ANS élabore, en concertation avec l'écosystème, des référentiels visant à garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel par les services numériques en santé.

La PGSSI-S fixe un cadre qui s'applique notamment :

- aux structures de santé dans la définition de leur politique de sécurité des systèmes d'information ;
- aux porteurs de projet dans la définition des niveaux de sécurité à mettre en œuvre ;
- aux industriels dans leurs choix relatifs à la sécurité pour le développement et les évolutions de leur offre.

Une élaboration en concertation avec l'écosystème

Ces référentiels sont élaborés en concertation avec des représentants de l'ensemble des parties prenantes : institutionnels, représentants d'établissements, professionnels de santé et industriels. Ce processus intègre la vérification de la conformité au cadre de référence et réglementaire européen. Les documents sont ensuite mis en concertation publique, avant finalisation et publication.

La PGSSI-S se veut pragmatique et réaliste. A cet effet, **ses référentiels et ses guides comportent généralement une notion de paliers à atteindre** : un palier minimal et des paliers progressifs, permettant aux porteurs de projet d'améliorer progressivement la sécurité de leurs projets jusqu'au palier cible défini selon leur contexte.

La PGSSI-S est régulièrement **mise à jour** pour s'adapter aux évolutions industrielles et technologiques, aux usages et aux évolutions réglementaires.

Les bénéfices de la PGSSI-S

La mise en application de la PGSSI-S permet :

- Aux usagers de bénéficier d'un système de santé numérisé qui réponde aux **exigences des soins** et assure la **protection de leurs données** ;
- Aux responsables de systèmes d'information de santé d'assurer la **conformité des SIS au cadre juridique et aux bonnes pratiques** de sécurité ;
- Aux utilisateurs de systèmes d'information de santé de s'équiper de **solutions conformes aux exigences de sécurité** propres à l'écosystème santé et médico-social ;
- La **gestion des risques spécifiques**, à savoir la prise en compte, la prévention et l'anticipation des incidents de sécurité liés au SI (qui impactent la prise en charge des patient, les coûts, …).

Les documents de la PGSSI-S

Les documents qui constituent le corpus documentaire de la PGSSI-S sont de deux types :

- Les **référentiels**, opposables ou destinés à être opposables par arrêté du ministre chargé de la santé ;
- Les **guides**, destinés à accompagner les acteurs des systèmes d'informations de santé :
  - des **guides pratiques** organisationnels,
  - des guides pratiques techniques,
  - des documents d'**aides à la mise en œuvre** de ces différents guides,
  - des **supports de sensibilisation** et de **communication**.

5 Référentiels
[Objectif d'Opposabilité]

- ✓ Identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales]
- ✓ Identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques]
- ✓ Identification électronique des usagers
- ✓ Imputabilité (gestion de preuve et traçabilité)
- ✓ Force probante des documents de santé

16 Guides
[Objectif d'Accompagnement]

communication
- ✓ Fiche Présentation de la PGSSI-S

organisation
- ✓ Memento sécurité informatique pour les professionnels de santé en exercice libéral
- ✓ Elaboration et mise en œuvre de PSSI
- ✓ Gestion des habilitations d'accès au SI

technique
- ✓ Mise en place d'accès Wifi
- ✓ Accès par application web ou mobile pour des tiers
- ✓ Protection de l'intégrité des données stockées
- ✓ Sauvegarde des SI de Santé
- ✓ Destruction sécurisée de données
- ✓ Plan de continuité informatique
- ✓ Interventions à distance
- ✓ Homologation des moyens d'identification électroniques (MIE)

aide
- ✓ Canevas de PSSI
- ✓ Modèle de charte sécurité pour les personnels IT
- ✓ Modèle de charte d'accès et d'usage du SI
- ✓ Modèle de plan d'action SSI

Ces documents sont principalement destinés aux acteurs en charge de la conception et de l'exploitation des SI de santé (porteurs de projets, équipes informatiques, responsable de la sécurité des SI, industriels…).

Certains sont toutefois établis à l'attention des responsables de ces SI (responsable d'établissement, professionnel de santé libéral…) ou des utilisateurs (PS, usagers…)

La PGSSI-S constitue un cadre qui aide les porteurs de projet dans la définition des niveaux de sécurité attendus, qui permet aux industriels de préciser les niveaux de sécurité proposés dans leurs offres et qui accompagne les structures de santé dans la définition et la mise en œuvre de leur politique de sécurité des SI.

Pour en savoir plus…

Pour plus d'informations, rendez-vous sur :
https://esante.gouv.fr/produits-services/pgssi-s

Pour consulter le corpus documentaire de la PGSSI-S, rendez-vous sur :
https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire