Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

EN BREF

- Depuis plus de six ans, la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) guide les acteurs 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 et authentification des acteurs, force probante des documents de santé, imputabilité des actions) et des guides pratiques.

La sécurité des SI : 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 de risques** portée par les structures de santé pour améliorer la qualité et la sécurité des soins.

Elaboration de la PGSSI-S

Conscient de ces enjeux et face à ces risques, l'Etat élabore depuis plusieurs années une **politique générale de sécurité des systèmes d'information de santé (PGSSI-S)**, en concertation avec l'ensemble des parties prenantes.

La PGSSI-S est un **corpus documentaire** conforme au cadre juridique de la santé numérique et à la politique de sécurité du système d'information du ministère chargé des Affaires Sociales (PSSI-MCAS).

Elle constitue un **cadre** aidant les porteurs de projet dans la définition des niveaux de sécurité attendus, permettant aux industriels de préciser les niveaux de sécurité proposés dans leurs offres et accompagnant les structures de santé dans la définition et la mise en œuvre de leur politique de sécurité des SI.

La PGSSI-S s'appuie sur des principes fondateurs qui fixent les grandes orientations en matière de sécurité des systèmes d'information de santé, et s'enrichit progressivement de **référentiels** qui sont amenés à devenir opposables, et de **guides pratiques et organisationnels**.

Les documents constitutifs de la PGSSI-S, actés dans le cadre d'un comité de pilotage, sont le fruit de groupes de travail composés d'institutionnels, de représentants d'établissements, de professionnels de santé et d'industriels.

Dès qu'un document est stabilisé, l'ASIP Santé le **soumet à concertation** auprès des industriels, des établissements, des professionnels de santé et du grand public.

Une fois les commentaires de concertation traités, une version validée est publiée sur le site esante.gouv.fr.

La PGSSI-S se veut pragmatique et réaliste. A cet effet, **les référentiels et les guides pratiques se présentent avec une notion de paliers** : 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.

Elle est régulièrement **mise à jour** pour s'adapter aux évolutions industrielles et technologiques, aux usages et aux évolutions réglementaires.

Documents publiés

Outre le document chapeau :

- principes fondateurs de la PGSSI-S.

Quatre référentiels :

- référentiel d'identification des acteurs sanitaires et médico-sociaux ;
- référentiel d'authentification des acteurs de santé ;
- référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé ;
- référentiel d'imputabilité.

Deux guides pratiques organisationnels :

- mémento de sécurité informatique pour les professionnels de santé en exercice libéral ;
- guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social, *pour des structures sans approche SSI formalisée.*

Deux documents d'aide à la mise en œuvre :

- fiche de sensibilisation à la sécurité des systèmes d'information de santé ;
- grille d'applicabilité des référentiels de la PGSSI-S.

Neuf guides pratiques spécifiques :

- règles pour les dispositifs connectés d'un système d'information de santé (SIS);
- guide pratique spécifique pour la mise en place d'un accès Wifi ;
- règles pour les interventions à distance sur les SIS ;
- guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des SIS ;
- règles de sauvegarde des SIS ;
- plan de continuité informatique, principes de base ;
- règles pour la mise en place d'un accès web au SIS pour des tiers ;
- guide des mécanismes de protection de l'intégrité des données stockées ;
- guide de gestion des habilitations d'accès au SI.

Evolutions en 2018

Plusieurs référentiels en cours d'élaboration…

- référentiel de gouvernance et de mise en œuvre de la PGSSI-S (en remplacement des principes fondateurs élaborés en 2014) ;
- mise à jour des référentiels d'identification et d'authentification des acteurs de santé ;
- référentiel d'identification des usagers et patients ;
- référentiel relatif à la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique (entrainant une modification du référentiel d'imputabilité).

Leur finalisation doit tenir compte des orientations nationales sur la mise en œuvre d'eIDAS et du RGPD.

… ainsi que des guides pratiques

- guide juridique sur l'échange et le partage des données de santé ;
- guide de gestion des équipements nomades ;
- documents pratiques à destination des structures d'exercice coordonné, telles les maisons et centres de santé (modèle de charte d'accès et d'usage du système d'information,…).

Des projets liés à **l'accompagnement, la pédagogie et la diffusion** de la PGSSI-S sont également en cours de conception :

- modules de présentation de la PGSSI-S au sein de la plateforme e-learning de l'ASIP Santé ;
- questionnaire d'auto-évaluation de maturité SSI ;
- ainsi que des labels FORMATION & ACCOMPAGNEMENT PGSSI-S destinés aux structures amenées à promouvoir la PGSSI-S, notamment pour en expliquer les enjeux et le contenu des référentiels.

Pour en savoir plus

Rendez-vous sur :
http://esante.gouv.fr/pgssi-s/presentation