Systèmes d'information de santé et risques associés

AMELIORER LA QUALITE DES SOINS EN FAVORISANT L'USAGE DE SYSTEMES D'INFORMATION COMMUNICANTS

L'**informatisation progressive du dossier patient,** et potentiellement de tous les processus de production de soins (prescription, dispensation, administration), permet d'améliorer la sécurité et la qualité des soins dans l'établissement de santé. Elle exige que le système d'information puisse fonctionner en continu (haute disponibilité : 24h/24 7j/7), conserver les données dans le temps tout en préservant leur intégrité, et garantir la confidentialité des informations médicales dans des environnements ouverts et partagés (par exemple les postes au lit du patient).

Par ailleurs, les systèmes d'informations des établissements de santé deviennent de plus en plus :

- **Connectés :** ils intègrent la gestion des équipements biomédicaux et l'exploitation des informations qu'ils produisent ; les demandes d'accès au système d'information se diversifient avec l'usage de terminaux mobiles (smartphones, tablettes, ordinateurs portables), …
- **Ouverts :** pour favoriser la coordination des soins en permettant d'améliorer la prise charge du patient par tous les acteurs de santé tout au long de son parcours de soins : échange d'information médicale par messagerie sécurisée, partage de documents médicaux avec le DMP (Dossier Médical Personnel), coopération dans le cadre de réseaux de santé, développement de la télémédecine, …
- **Mutualisés** dans le cadre de regroupements : CHT/GHT, regroupement de cliniques, …
- **Interfacés** avec les partenaires financiers des établissements (organismes de sécurité sociale, mutuelles, trésor public) pour les données d'identité et de facturation

Le système d'information s'appuie sur un ensemble de plus en plus grand de dispositifs, interconnectés ou cohabitants, au service des professionnels de santé pour une meilleure prise en charge du patient et l'amélioration du système de santé.

Levier d'amélioration de la qualité des soins et d'efficience, l'informatisation va de pair avec un accroissement significatif des vulnérabilités, des menaces et des risques d'atteinte aux informations conservées sous forme électronique et en conséquence aux processus de soins s'appuyant sur les systèmes d'information de santé. L'origine de ces menaces peut être intentionnelle (développement de la cybercriminalité, acte de malveillance d'un utilisateur du système d'information), ou involontaire (faille technique, manque de sensibilisation des utilisateurs…).

MANAGER LA SECURITE DU SYSTEME D'INFORMATION : UNE GESTION DE RISQUES

Pour bénéficier pleinement des apports des systèmes d'information, l'établissement doit veiller à se prémunir des risques inhérents à leurs usages.

- en mettant en place une organisation adéquate pour manager la sécurité du système d'information ;
- en menant des analyses de risques et en mettant en œuvre une politique de sécurité du système d'information, un plan de traitement des risques et un plan d'action associé. Ce plan d'action s'inscrit dans une démarche d'amélioration continue, telles les démarches de gestion de la qualité ou de gestion des risques médicaux en établissement de santé.

La sécurité de l'information n'est pas un simple projet informatique. Elle doit être portée par la Direction générale et les responsables des métiers car elle implique la participation de l'ensemble des utilisateurs du système d'information.

Les principaux risques dont il convient de se prémunir dans les établissements de santé sont :

✓ Le **risque d'indisponibilité** du système d'information de l'établissement de santé, qui peut être lié, par exemple, à :

- la panne d'un composant informatique ;
- une erreur de paramétrage ou de procédure ou un défaut dans un logiciel mis à jour ;
- des virus informatiques ;
- des sinistres, tels qu'incendie, inondation de locaux informatiques, panne de climatisation ou défaillance de l'alimentation électrique de la salle informatique.

Exemples d'impacts : impossibilité partielle ou totale d'accéder au dossier patient informatisé du patient ou interruption d'un service de surveillance de l'état de santé d'un patient générant des risques pour le patient.

✓ Le **risque de modification intempestive de données** du système d'information de l'établissement qui peut survenir :

- de manière accidentelle, par exemple à cause d'un défaut dans un logiciel ou d'une défaillance de matériel informatique ;
- de façon malveillante, par exemple à l'initiative d'un ancien employé de l'établissement ou d'un pirate informatique.

Ce risque peut également porter sur le paramétrage d'équipements tels que des pompes à insuline ou un stimulateur cardiaque.

Exemples d'impacts : risques pour le patient ; risque de défiance durable du personnel médical et paramédical envers les systèmes d'information de santé.

✓ Le **risque de divulgation de données de santé à caractère personnel** qui peut être effectué de manière accidentelle ou malveillante.

Ces informations sont des données particulièrement sensibles et protégées par la loi.

La divulgation de données de santé à caractère personnel, volontaire ou non, n'est pas propre à la dématérialisation de ces données, et ses enjeux sont bien connus.

Toutefois les risques sont accrus avec la généralisation de l'usage d'internet et la puissance des moteurs de recherche. Une faille de sécurité permettant la diffusion d'information sur internet peut permettre la consultation d'informations confidentielles par tout internaute qui effectue des recherches d'informations sur l'une des personnes concernées, sur l'une des pathologies citées, voire sur l'un des mots contenus dans ces dossiers.

Exemples d'impacts : manquement au devoir de confidentialité concernant les patients pris en charge dans l'établissement, atteinte à l'image (médiatisation), de poursuite judiciaire.

✓ **Risques liés à l'absence de traces des activités** réalisées au sein du système d'information de l'établissement.

Quand survient un incident de sécurité du système d'information de santé, et en particulier quand il concerne la consultation abusive, la divulgation ou la modification intempestive de données sensibles, il est essentiel de pouvoir en identifier rapidement l'origine :

- d'une part, pour être en mesure de corriger le problème, puis dans un second temps pour mettre en place les mesures de prévention et de réaction adéquates ;
- d'autre part, dès lors qu'il y a suspicion d'acte malveillant ou de faute, pour pouvoir en rechercher l'auteur ou fournir aux autorités compétentes toutes les informations requises.

Exemples d'impacts : sans traces fiables d'activités du système d'information, les responsables d'établissement s'exposent :
- à devoir assumer seuls les conséquences de l'incident, n'étant pas en mesure d'identifier la ou les personnes à l'origine d'une éventuelle faute ou malveillance ;
- à subir des sanctions pour ne pas avoir mis en place les mesures de collectes de traces de l'activité du système d'information exigées par la loi dès lors que des informations à caractère personnel sont traitées.

En outre, une démarche de conservation de traces des activités, connue de l'ensemble des utilisateurs du système d'information, a une vertu dissuasive vis-à-vis des simples indiscrétions telles que la consultation d'un dossier patient par des personnes ne participant pas à sa prise en charge, comme vis-à-vis des malveillances éventuelles.

PGSSI-S : REFERENTIELS ET GUIDES PRATIQUES PERMETTANT UNE PRISE EN COMPTE PROGRESSIVE DES EXIGENCES DE SECURITE

Pour accompagner le **développement des usages des systèmes d'informations de santé en toute confiance**, l'Etat élabore une Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), en concertation avec l'ensemble des acteurs partie prenante. La maîtrise d'ouvrage stratégique en est assurée par la DSSIS et la maitrise d'ouvrage opérationnelle par l'ASIP Santé.

La PGSSI-S constitue un cadre aidant les responsables à définir des niveaux de sécurité attendus, permettant aux industriels de préciser les niveaux de sécurité proposés

dans leurs offres et accompagnant les établissements de santé dans la définition et la mise en œuvre de leur politique de sécurité des systèmes d'information.

Elle 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 techniques** qui ont vocation à devenir **opposables**, ainsi que de **guides pratiques et organisationnels**.

La PGSSI-S se veut pragmatique et réaliste. D'une part, elle s'adapte aux évolutions industrielles et technologiques. D'autre part, les référentiels se présentent avec **une notion de paliers** : un palier cible défini en fonction de l'étude de risques réalisée dans l'établissement, un palier initial ainsi que plusieurs paliers intermédiaires permettant d'accompagner la structure dans l'atteinte du palier cible.

POUR EN SAVOIR PLUS

- Introduction à la sécurité des systèmes d'information, Guide pour les directeurs d'établissement de santé (publication DGOS, novembre 2013)

- Référentiels et guides de la PGSSI-S publiés par la DSSIS/ASIP Santé sur esante.gouv.fr/pgssi-s/presentation

- ARS et GCS esanté peuvent proposer un accompagnement des acteurs de santé à la sécurité de leur système d'information