HAUTE AUTORITÉ DE SANTÉ

MESURER
& AMÉLIORER
LA QUALITÉ

Évaluation de la gestion des risques numériques dans les pratiques de soins

selon le référentiel de certification

Date validation Collège le 7 novembre 2024

- → Le système d'information hospitalier (SIH) peut être défini comme l'ensemble des informations, de leurs règles de circulation et de traitement nécessaires à son fonctionnement quotidien, à ses modes de gestion et d'évaluation ainsi qu'à son processus de décision stratégique.
- → En interne, le SIH peut regrouper plusieurs fonctions nécessaires à la prise en charge (dossier patient), gestion des plannings, de la paye, la facturation, le suivi budgétaire, la communication (internet, intranet, protocoles, messagerie, forum, bon de commande, etc.).
- → En externe, la tendance se tourne vers le développement de réseaux de santé, « Mon espace santé », la télémédecine, le pilotage d'un robot chirurgical à distance.

Enjeux nationaux

Le numérique en santé est aujourd'hui en plein essor pour améliorer la qualité, l'efficacité et l'accessibilité des soins en santé. Au-delà des outils numériques internes à l'établissement de santé notamment pour gérer les dossiers du patient, il comprend des domaines tels que les équipements biomédicaux connectés, la télémédecine, les objets de santé connectés, l'intelligence artificielle et l'analyse de données, la réalité augmentée et la réalité virtuelle.

Depuis 2019, le ministère chargé de la Santé porte une stratégie nationale du numérique en santé destinée à accélérer la transformation numérique du système de santé tout en visant :

- la sécurisation des échanges et le partage de données entre les acteurs de soins et les patients ;
- la maîtrise des risques de sécurité numérique, en particulier en renforçant la lutte contre la cyber malveillance.

Principales données[1]

- 95% des établissements ont formalisé une politique de sécurité du système d'information (+ 2 points par rapport à 2018)
- 96% déclarent avoir désigné un référent sécurité SI.
- Les établissements consacrent en moyenne 1,7% de leurs charges d'exploitation aux SIH, proportion en baisse par rapport aux années précédentes.

1. Source DGOS/ATIH Atlas des SIH 2020.

Définitions

2023-2027 : Mettre le numérique au service de la santé

En France, la feuille de route du numérique en santé 2023-2027 « Mettre le numérique au service de la santé » pose un cadre d'action et de collaboration entre acteurs publics et privés de l'écosystème, notamment sur l'utilisation des services et référentiels numériques socles (Mon espace santé composé du Dossier Médical Partagé, Messageries Sécurisées de Santé, Identité Nationale de Santé, Pro Santé Connect, etc.).
Cette feuille de route intègre deux volets d'accompagnement financier des établissements de santé avec la définition d'objectif d'usage :

- Ségur du numérique en santé : 2 milliards d'euros pour soutenir le développement massif et cohérent du numérique en santé en France (dont le dispositif de financement à l'équipement SONS et le programme de financement à l'usage SUN-ES et maintenant HOP'EN2);
- Programme HOP'EN2 (Hôpital ouvert sur son environnement) abordant les enjeux de la transformation numérique à l'hôpital.

CARE

Le Programme Care (Cybersécurité accélération et résilience des établissements) est un programme d'actions visant à accélérer la mise à niveau des systèmes d'informations hospitaliers face à l'état de la menace et à renforcer durablement la résilience des structures de soins. Le programme se décline pour la période 2023 à 2027 autour de 4 axes (Gouvernance et résilience, ressources et mutualisation, sensibilisation et sécurité opérationnelle) et 20 objectifs. Chaque objectif comporte des actions précisant les cibles à atteindre et la période visée pour les atteindre.

Source : Présentation du programme CaRE | Agence du Numérique en Santé (esante.gouv.fr)

HOP'EN 2

Le programme HOP'EN, pour « Hôpital numérique ouvert sur son environnement », s'inscrit dans la politique du numérique en santé. Il poursuit les efforts engagés par les établissements de santé dans leur transformation numérique et leur modernisation et a eu comme ambition de les amener à un palier de maturité de leur système d'information (SI), pour répondre aux enjeux de décloisonnement du système de santé et de rapprochement avec les patients.

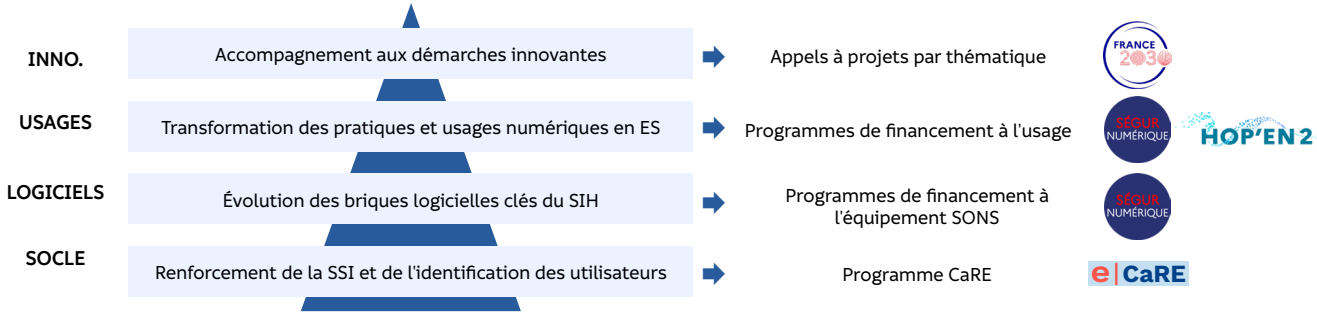
En parallèle, lancé en 2021, le programme SUN-ES, prolongement du programme HOP'EN, privilégie la production et la transmission de documents de santé dans le but d'enrichir, via le dossier médical partagé (DMP), le nouvel espace numérique de santé « Mon espace santé » ouvert en 2022.

En juillet 2024, le programme HOP'EN 2, action majeure de la feuille de route 2023-2027 « Mettre le numérique au service de la santé », prend le relais des **programmes HOP'EN et SUN-ES** pour accélérer la transformation numérique des établissements de santé, et encourager le développement des usages numériques permettant d'améliorer la prise en charge des patients et de simplifier la vie des soignants.

Sa première phase, d'une durée d'un an, s'attache à poursuivre les travaux sur :

- **l'identitovigilance** via la progression du taux de qualification de l'identité nationale de santé (INS) des patients, indispensable pour préparer l'arrivée des mises à jour de la vague 2 du Ségur numérique qui permettront aux professionnels des établissements de santé de consulter simplement le DMP des patients pris en charge ;
- **le partage des principaux documents de santé hospitaliers vers le profil Mon espace santé du patient** : documents de sortie, CR opératoires, CR de consultation, d'imagerie et de biologie médicale ;
- **les usages de la messagerie sécurisée de santé**, avec les professionnels pour le partage de ces documents, et avec les patients via la messagerie de Mon espace santé.

Des programmes de financement hospitaliers nationaux complémentaires pour répondre aux enjeux numériques des établissements



Source : Le programme HOP'EN 2 - Ministère du travail, de la santé et des solidarités (sante.gouv.fr)

En quoi la certification répond aux enjeux du thème ?

Pilotage

- Identifier les risques numériques et auxquels l'établissement peut être confronté et avoir une réponse opérationnelle adaptée aux risques :
  - les risques de sécurité numérique sont maîtrisés (critère 3.6-02) ;
  - l'identification des utilisateurs et des patients dans le système d'information est sécurisée (critère 3.6-06).

Actions

- Assurer l'accès aux données de santé par le patient et les professionnels qui le prennent en charge :
  - les équipes de soins ont accès aux informations du patient avec un système d'information adapté (critère 2.2-05).
- Sécuriser l'identification et la transmission de données de santé :
  - les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge (critère 2.3-01) ;
  - les modalités de communication permettent aux usagers et aux médecins de ville de contacter l'établissement aisément (critère 3.1-07).

Évaluation

- Mesurer le niveau de maturité du système d'information et mettre en œuvre les actions d'amélioration requises :
  - la gestion des tensions hospitalières et des situations sanitaires exceptionnelles est maîtrisée (critère 3.6-01) ;
  - les risques de sécurité numérique sont maîtrisés (critère 3.6-02).

Les points clés nécessitant l'attention des experts-visiteurs pendant la visite

L' évolution vers un système d'information hospitaliser ergonomique

Avec la gouvernance, vous vous assurez qu'il existe un plan d'action pour soutenir l'évolution du système d'information hospitalier en lien avec les programmes nationaux (HOP'EN, SUN-ES, CARE).

Avec les professionnels vous évaluerez l'ergonomie du système d'information hospitalier, c'est-à-dire si la navigation est aisée. Ainsi, vous vérifierez que :

- les outils (ex : ordinateurs, internet, Wifi, etc.) sont en nombre suffisant et fonctionnels pour garantir l'accessibilité au système d'information à tous les professionnels impliqués ;
- l'interopérabilité, c'est-à-dire la possibilité d'échanges et de partage d'informations entre plusieurs éléments informatiques (systèmes, appareils, logiciels, etc.), garantit l'accès rapide et sûre aux informations de la prise en charge. Par exemple, le logiciel du bloc communique avec le logiciel des services de soins pour éviter que le patient quitte le bloc avec une feuille de liaison remplie par le bloc et ressaisie par le service de chirurgie ;
- les outils informatiques qui composent le dossier patient, sont consultables sans devoir se déconnecter de l'un pour se connecter à l'autre.
- les équipes sont accompagnées dans la prise en main des outils et logiciels ;
- l'établissement octroie au personnel en mobilité (astreintes ou travail à distance) un poste professionnel ou un dispositif d'ouverture sécurisé de sessions à distance (ex : VPN).

1. Soutenir l'évolution vers un système d'information hospitaliser ergonomique

Plan d'actions, en lien avec les programmes nationaux, pour soutenir l'évolution du SIH

Outils efficaces et ergonomiques pour garantir l'usage par les professionnels

Experts-visiteurs

Concernant la **gestion des risques**, **vous vérifierez** que :

- l'établissement réalise régulièrement des exercices de crise cyber ;
- l'établissement réalise des audits réguliers des annuaires techniques et de l'exposition internet ;
- l'établissement a réalisé des audits de sécurité numérique et, qu'au regard des résultats, il a :
  - hiérarchisé ses risques numériques et élaboré un plan d'actions,
  - initié des correctifs à 6, 12 et 18 mois sur les actions critiques recommandées.

Concernant la **formation et la sensibilisation des professionnels**, vous vérifierez que l'établissement :

- forme, dans les secteurs les plus à risques, des **référents sécurité SI** en relais des équipes SI ;
- a démarré un **plan de formation pluriannuel** à la sécurité informatique et à la mise en œuvre du mode dégradé ;
- sensibilise régulièrement les professionnels aux risques numériques et aux moyens de les prévenir ;
- sensibilise à l'usage d'outils sécurisés, en promouvant, par exemple, l'usage des outils tels que « Mon espace santé » (dossier médical partagé, messagerie citoyenne), une messagerie sécurisée de santé, dossier pharmaceutique, plateforme de télésanté (messagerie sécurisée, hébergeur de données agréé…) ;
- sensibilise au besoin d'éradiquer la conservation de documents de santé à donnée personnelle sur leur poste de travail.

Auprès des professionnels, vous vérifierez qu'ils :

- connaissent le référent sécurité SI formé en relais des équipes SI dans les secteurs les plus à risques ;
- connaissent les risques et les moyens de les prévenir ;
- connaissent les conduites à tenir en cas de doute (identification des mails frauduleux, etc.).

2. Prévenir la crise cyber

Auditer et corriger

- Audit de sécurité numérique
- Exercice de cyber crise
- Audit des annuaires techniques et exposition internet

Former et sensibiliser

- Référent sécurité SI dans les secteurs les plus à risques
- Plan de formation pluriannuel
- Risque et bon usage du SIH

Experts-visiteurs

Avec la gouvernance, vous vérifierez qu'il existe une stratégie de gestion des accès aux SIH, à savoir :

- **une politique et des règles d'accès** déclinées dans un dispositif d'habilitation au système d'information quel que soit l'utilisateur (professionnels, intérimaires, étudiants, stagiaires, patients, etc.) ;
- des règles de gestion des **arrivées et départs** des professionnels, des intérimaires, stagiaires, étudiants, etc.

Auprès des professionnels, vous vérifierez qu'ils :

- connaissent les règles d'accès au SIH ;
- utilisent **un identifiant et un mot de passe personnel et unique** et que ce dispositif d'accès par identifiant et mot de passe est complété pour les accès à distance par un autre moyen d'identification permettant ainsi **l'identification double facteur** (ex : badge, carte à puce comme les cartes CPS, etc.) ;
- ne partagent pas un identifiant et un mot de passe générique connu par tous (notamment pour les intérimaires, les étudiants, etc.).

3. Sécuriser les accès au SIH

- **Politique et règles d'accès définies par la gouvernance et connues de professionnels**
- **Identifiant et mot de passe unique et personnel**
- **Système d'identification pour les accès à distance**

Experts-visiteurs

Avec la gouvernance, vous vérifierez que :

- le **plan blanc** comporte un volet sur les risques numériques ;
- dans tous les secteurs, il existe **un plan de continuité des activités** (PCA) et **un plan de reprise des activités** (PRA) adaptés à l'activité ;
- une **veille de sécurité numérique** est en place ;
- les incidents significatifs ou graves de sécurité des systèmes d'information sont déclarés sans délai auprès du centre compétent. Les **mesures d'urgence** proposées par ce centre pour en limiter l'impact et améliorer la sécurité sont mises en œuvre.

Auprès des professionnels, vous vérifierez qu'ils :

- connaissent les conduites à tenir en cas d'incident/d'attaque, notamment comment contacter le référent de la sécurité numérique ;
- qu'ils savent mettre en œuvre leur plan de continuité d'activité et leur plan de reprise d'activité.

4. Gérer la crise cyber

- **Plan blanc**
- **Plan de continuité et de reprise de l'activité prévus et connus**
- **Veille de sécurité numérique en place**
- **Signalement et prise en compte des mesures d'urgence proposées**

Pour aller plus loin

Références HAS

- Amélioration de la qualité et de la tenue du dossier patient. www.has-sante.fr/jcms/c_438115/fr/dossier-du-patient

Références légales et documentaires

- Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique.
- Art.L.6111-2, L1111-8-2 du code de la santé publique.
- Décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information.
- Instruction 309 de 2016.
- Instruction n° SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« plan d'action SSI ») dans les établissements et services concernés.
- Instruction n° DGOS/PF5/DNS/CTO/2021/167 du 26 juillet 2021 relative au lancement opérationnel du financement forfaitaire à l'atteinte de cibles d'usage des établissements de santé dans le cadre du volet numérique du Ségur de la santé.
- Instruction n° SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement.
- Cybersécurité - Mémento DGOS à l'usage du directeur d'établissement de santé – 2017.
- PSSI-MCAS.RGS.RGPD. Cybersécurité - Mémento DGOS à l'usage du directeur d'établissement de santé – 2017.

Autres références

- Page CaRE : Cybersécurité de la santé | e-santé (esante.gouv.fr)
- Cert Santé | Portail du CERT Santé (esante.gouv.fr)
- ANAP : Cartographie fonctionnelle du SI.
- L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur.
- « Guide d'hygiène informatique » de l'Agence nationale de la sécurité des systèmes d'information.
- PGSSI-S - Corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé.
- Guide pour réaliser un plan de continuité d'activité - SGDSN – 2013.
- Recommandations relatives à l'authentification multi-facteur et aux mots de passe - guide ANSSI – 2021.
- Gestion des habilitations d'accès au SI - Guide pratique organisationnel PGSSI-S - ANS – 2022.
- Mémo « Mon espace santé et la protection des données : comment respecter vos obligations d'information des patients ».
- Mémo « Synthèse des droits et règles d'accès à « Mon espace santé DMP ».
- Boîte à outils « Mon espace santé » dédiée aux établissements.

Scannez-moi pour consulter la fiche pédagogique

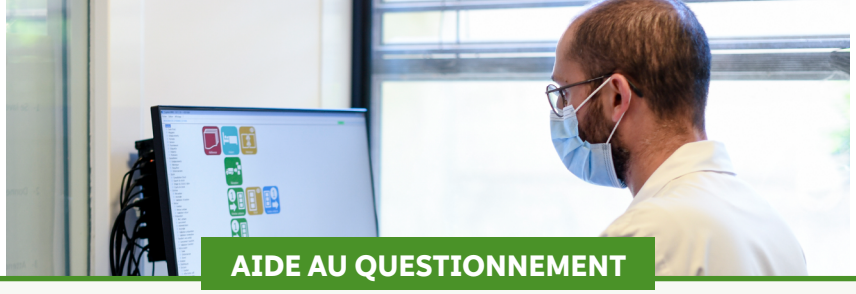
Patients, soignants, un engagement partagé

Retrouvez tous nos travaux et abonnez-vous à l'actualité de la HAS
www.has-sante.fr

HAS HAUTE AUTORITÉ DE SANTÉ

Développer la qualité dans le champ sanitaire, social et médico-social

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici



AIDE AU QUESTIONNEMENT

Évaluation de la gestion des risques numériques dans les pratiques de soins

selon le référentiel de certification

Les questions suivantes ne sont ni opposables, ni exhaustives. Elles sont données à titre d'exemple dans le cadre des entretiens d'évaluation. Elles sont aussi à adapter au contexte rencontré, aux secteurs et aux méthodes déployées. Elles ne se substituent pas aux grilles.

Exemples de questions susceptibles d'être posées pendant les évaluations

À la gouvernance

- Avez-vous réalisé un audit de sécurité numérique (AD et internet) ? Quels sont les principaux risques que vous avez identifié à la suite de votre audit de sécurité numérique ? Sur les risques critiques, quelles sont les actions à mettre en œuvre à 6 mois ? À 12 mois ? À 18 mois ? Votre calendrier est-il respecté ? (Crit.3.6-01 ; Crit.3.6-02)
- Avez-vous réalisé un exercice de crise cyber ? Quelles sont les conclusions ? Et quelles actions correctives avez-vous mis en œuvre ? (Crit.3.6-01)
- Pouvez-vous me présenter les principaux axes du volet de sécurité numérique de votre plan blanc ? Un PCA et PRA est-il adapté à chaque secteur (technique, administratif, soignant, ...) ? Pouvez-vous me donner un exemple d'action spécifique et prévue au PCA et PRA d'un ou deux secteurs (ex : réanimation, chirurgie) ? (Crit.3.6-02)
- Avez-vous formé des référents sécurité SI formé en relais des équipes SI ? Quel est le dispositif de formation ? Quel est le taux de personnels formés ? Avez-vous formalisé une fiche de mission pour les référents SI ? (Crit.3.6-02)
- Quelles actions de sensibilisation menez-vous auprès des professionnels ? Sur quels thèmes en particulier ? Avez-vous démarré un plan de formation pluriannuel à la sécurité informatique et à la mise en œuvre du mode dégradé ? Quelle proportion de professionnels sont déjà formés ? Pouvez-vous me montrer les listes d'émargement ? (Crit.3.6-02 ; Crit.3.6-02)
- Avez-vous été confronté à un incident significatif ou grave de sécurité des systèmes d'information ? Comment l'avez-vous déclaré ? Et les mesures d'urgence qui vous ont été recommandées ont-elles été mises en place ? Pourriez-vous me donner un exemple ? (Crit.3.6-02)

Au plan technique

- Quelles sont les règles d'accès au système d'information pour les professionnels ? les intérimaires ? les étudiants ? les stagiaires, les patients ? Et quelles sont vos règles de gestion des arrivées et des départs ? (Crit.3.6-06 ; Crit.3.6-06)
- Quel matériel ou dispositif d'ouverture sécurisé de sessions à distance (ex : VPN) mettez-vous à disposition des personnels en mobilité (astreintes ou travail à distance) ? Pouvez-vous me montrer la liste des utilisateurs en mobilité ? (Crit.3.6-06)
- Comment les professionnels s'identifient-ils dans le SI ? (Crit.3.6-06)

Avec les professionnels

- Diriez-vous que vous disposez d'outils (ordinateurs, internet, Wifi, etc.) en nombre suffisant et fonctionnels pour vous permettre d'accéder au système d'information ? Les divers outils du dossier patient sont-ils interopérables ? À défaut, naviguez-vous facilement entres les divers outils du dossier patient ? Est-il nécessaire de se déconnecter de l'un pour se connecter à l'autre ? (Crit.2.2-05)
- Pouvez-vous me donner un exemple de formation à laquelle vous avez participé au moment du déploiement d'un nouvel outil informatique ou au moment d'une évolution de ceux que vous utilisez habituellement ? (Crit.2.2-05)

Avec les professionnels (suite)

- Comment vous connectez vous au SIH (identifiant et mot de passe personnel + autre moyen d'identification) ? Existe-t-il un ordinateur partagé entre professionnels dans votre service ? Si oui, comment procédez-vous pour accéder au système d'information et pour vous déconnecter ? Existe-il un identifiant et un mot de passe générique que vous partagez avec d'autres professionnels, par exemple, les étudiants ou les intérimaires ? Avez-vous la possibilité de vous connecter à distance ? Si oui, comment procédez-vous ? (Crit.3.6-06)
- Quels sont les principaux risques cyber auxquels l'établissement est confronté ? À votre échelle, les connaissez-vous ? Comment les prévenez-vous ? Quelle est la conduite à tenir quand vous avez un doute, par exemple quand vous recevez un mail qui vous parait frauduleux ? (Crit.3.6-02)
- Dans les secteurs les plus à risques : qui est le référent sécurité SI ? Pourriez-vous me dire comme le contacter en cas d'attaque ? (Crit.3.6-02)
- Connaissez-vous les actions à mettre en œuvre pour assurer la continuité et la reprise de l'activité en cas d'indisponibilité du système d'information ? Quel est le mode dégradé que vous devez mettre en place si votre système d'information ne fonctionne plus. Disposez-vous de documents papier ? (Crit.3.6-02)
- Vous arrive-t-il d'enregistrer des documents de santé de vos patients sur votre poste de travail ? De quelles données s'agit-il ? Si vous avez un document de santé intégrant des données médicales d'un patient sur un poste, que faites-vous ? Avez-vous été sensibilisé sur ce sujet ? (Crit.3.6-02)