AUDIT SYSTÈME | KIT 18 / 20

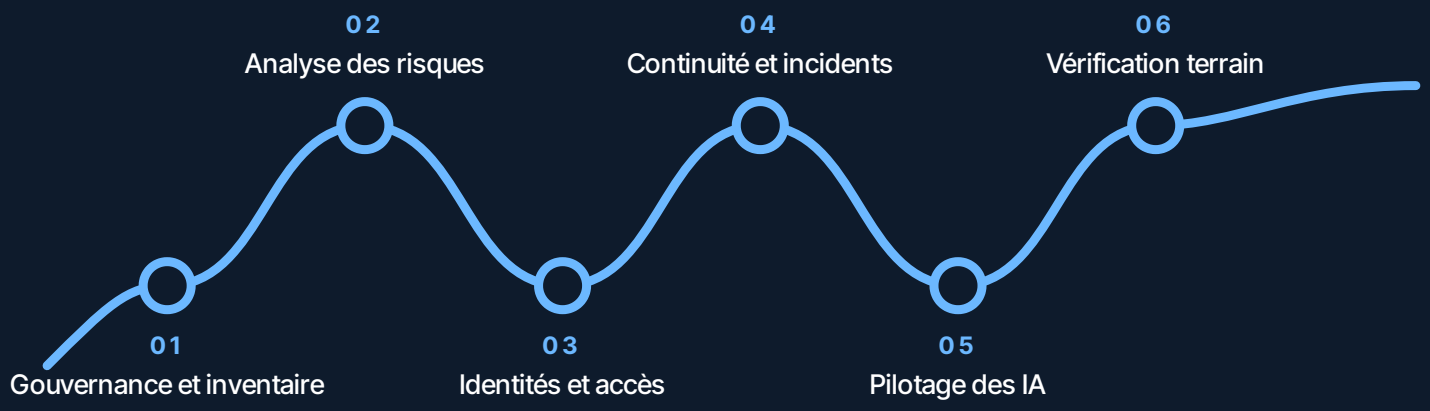
Risques numériques : gouvernance

Évaluer le pilotage institutionnel de la cybersécurité, des accès, de la continuité numérique, des incidents et des systèmes d'intelligence artificielle.

7 CRITÈRES

22 ÉLÉMENTS D'ÉVALUATION

DÉROULÉ EN 6 ÉTAPES



Développer l'engagement et la culture qualité de vos équipes

Rendez-vous sur **HospiPlay**

« La qualité nous rassemble, la sécurité du patient nous engage. »

HOSPIPLAY

À PROPOS DU KIT

Préparer l'audit interne, pas à pas.

Ce que c'est

Une aide pour conduire les audits internes avant la visite de certification. Chaque kit reprend une méthode d'évaluation de la HAS, les éléments d'évaluation du référentiel V2027 et les preuves à rechercher, à partir des fiches pédagogiques de la HAS.

Ce qu'il n'est pas

Un document officiel : ce kit est indépendant de la HAS. Le référentiel et les fiches officielles restent la référence.

COMMENT L'UTILISER

01
Préparer
Choisir le cas ou le périmètre, réunir les documents et les personnes à rencontrer.

02
Conduire
Suivre le déroulé et rechercher les preuves de chaque élément d'évaluation.

03
Coter
Reporter les constats sur la grille d'audit Excel associée au kit.

04
Restituer
Valoriser les points forts et convenir d'actions d'amélioration avec l'équipe.

LA COLLECTION : 20 KITS

MÉTHODES

- 01 Patient traceur
- 02 Parcours traceur
- 20 Observation

TRACEURS CIBLÉS

- 03 Accouchement
- 04 Circuit du médicament
- 05 Évènements indésirables graves
- 06 Isolement
- 07 Infections associées aux soins
- 08 SAMU–SMUR
- 09 Secteurs interventionnels
- 10 Transfusion

AUDITS SYSTÈME

- 11 Encadrement
- 12 Engagement du patient
- 13 Entretien avec les professionnels
- 14 Ressources professionnelles
- 15 Management qualité et risques
- 16 Positionnement territorial
- 17 Représentants des usagers
- **18 Risques numériques : gouvernance**
- 19 Risques numériques : professionnels

HOSPIPLAY | PLATEFORME D'ENGAGEMENT QUALITÉ

Le kit prépare l'audit. HospiPlay prépare les équipes.

DÉCOUVRIR

01
Faire tomber la peur du traceur
Onze parcours démontent chaque méthode pas à pas, puis mettent le soignant face aux vraies questions de l'auditeur.

02
Des expériences courtes et collectives
Quiz du jour, défis express, chambre des erreurs, histoires interactives et olympiades qualité.

03
Simple à déployer, mesurable
Un QR code, sans compte individuel, et le suivi de la participation par service.

« La qualité nous rassemble, la sécurité du patient nous engage. »

Conçu par Babacar Ndiaye, ingénieur qualité et gestion des risques.
Version V2027, novembre 2026.

8. Audit système - Risques numériques - Gouvernance

7 critères • 22 éléments d'évaluation

Évaluer le pilotage institutionnel de la cybersécurité, des accès, de la continuité numérique, des incidents et des systèmes d'intelligence artificielle.

Guide méthodologique - Conduire cet audit système avec rigueur

1. Définir le périmètre et l'échantillon

Définir le périmètre institutionnel puis sélectionner un service numérique critique et, s'il existe, un système d'IA ou un dispositif médical numérique. Suivre leur gouvernance, leurs risques, leurs utilisateurs, un incident ou test de continuité et les résultats de surveillance.

À préparer avant l'audit
Gouvernance SI et sécurité ; cartographie des actifs et risques ; politique d'accès ; revues d'habilitations ; journaux ; sauvegardes ; PCA-PRA ; incidents et CERT Santé ; violations de données ; MSSanté et DMP ; fournisseurs ; inventaire IA ; analyses d'impact ; validation, supervision et vigilance.

Personnes à rencontrer
Direction, DSI, responsable sécurité, DPO, direction médicale et des soins, qualité–risques, biomédical, achats, référents identitovigilance, propriétaires des applications et utilisateurs. Associer le fournisseur uniquement pour les éléments qui relèvent de sa responsabilité.

2. Déroulé de l'audit système

Étape	Niveau vérifié	Ce que l'auditeur doit démontrer
1	**Gouvernance et inventaire**	Faire préciser responsabilités, actifs critiques, traitements, applications, IA, propriétaires, dépendances et critères de criticité.
2	**Analyse des risques**	Vérifier risques cyber, confidentialité, intégrité, disponibilité, impacts patients, mesures de réduction, acceptation des risques et plans financés.
3	**Identités et accès**	Contrôler création, validation, moindre privilège, MFA si applicable, revues, retrait, comptes techniques et analyse des journaux d'accès.
4	**Continuité et incidents**	Suivre un test ou incident réel : détection, alerte, mode dégradé, sauvegarde, restauration, communication, déclarations et retour d'expérience.
5	**Pilotage des IA**	Distinguer DM numérique avec IA et IA sans finalité médicale ; vérifier choix, conformité, données, performances, supervision humaine, incidents et arrêt.
6	**Vérification terrain**	Dans une unité, contrôler l'usage réel, les droits, la connaissance du mode dégradé et la concordance avec les politiques ; examiner indicateurs et remédiations.

3. Conclure et coter

Pour chaque système ciblé, relier propriétaire, analyse de risques, mesures, preuve technique autorisée, pratique utilisateur, incident ou test, résultat et décision de remédiation.

> **Exigence de rigueur -** *Ne pas demander l'affichage de mots de passe, de secrets techniques ou de données non nécessaires. Les preuves de journaux et de sécurité doivent être consultées avec une autorisation et un périmètre maîtrisés.*

Éléments d'évaluation et preuves à rechercher

Exigence de rigueur - Ne pas demander l'affichage de mots de passe, de secrets techniques ou de données non nécessaires. Les preuves de journaux et de sécurité doivent être consultées avec une autorisation et un périmètre maîtrisés.

Critère 1.1-03 - Le patient bénéficie du respect de la confidentialité et du secret professionnel

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** Sur la base d'un suivi des contrôles, l'établissement démontre qu'il a éradiqué les connexions illégitimes au dossier patient qui constituent une violation du secret médical.	• Procédure de contrôle des traces avec fréquence, périmètre, critères d'alerte, responsables et règles de conservation des journaux • Rapport de contrôle permettant de relier utilisateur, patient/dossier, date/heure, action et contexte de prise en charge • Investigation contradictoire documentée avant qualification de l'accès comme légitime ou illégitime • Mesures correctives adaptées : sensibilisation, restriction/suspension des droits, action disciplinaire ou autre selon le cas, et information des acteurs compétents • Contrôle ultérieur démontrant la disparition ou la réduction du risque
Cible : Gouvernance. **EE 2** En cas de fuite des données, la procédure d'information des patients victimes de la fuite de leurs données est mise en œuvre. A défaut d'y avoir été confrontée, la procédure existe.	• Procédure de gestion des violations précisant l'analyse du risque, les responsabilités, les délais et les critères d'information des patients • Registre des violations comportant les données touchées, les personnes concernées, l'évaluation du risque et la décision d'informer ou sa justification • Message adressé aux patients ou support d'exercice précisant la nature de la fuite, les conséquences, les mesures prises et les conseils de protection, avec trace d'envoi

Critère 2.1-14 - Les équipes se coordonnent en amont de la sortie pour assurer la continuité du parcours de soins

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** L'établissement améliore ses pratiques au regard des résultats d'indicateurs de complétude et de qualité des éléments versés dans Mon espace santé.	• Référentiel local des documents attendus par activité/type de prise en charge • Tableau de bord distinguant attendus, produits, versés, rejets, absences et anomalies de qualité • Contrôle qualitatif d'un échantillon : identité, auteur, date, type, lisibilité et contenu utile • Analyse par secteur et plan d'action avec responsable/échéance • Nouvelle mesure comparable confirmant l'amélioration

Critère 3.1-07 - Les risques de sécurité numérique sont maîtrisés

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** L'établissement dispose d'un plan de continuité et de reprise d'activité formalisé.	• Analyse de criticité reliant processus de soins, applications, dépendances, délais de reprise et pertes de données admissibles • PCA/PRA versionnés avec rôles, ordre de reprise, contacts et solutions techniques/organisationnelles • Kits de mode dégradé disponibles indépendamment du SI, adaptés aux secteurs et testés • Procédure de réintégration/réconciliation des données après reprise avec contrôles de complétude • Compte rendu d'exercice ou test de restauration avec chronologie, résultats, écarts et actions
Cible : Gouvernance. **EE 2** L'établissement a mis en œuvre le plan d'actions correctives issu des audits Active Directory et exposition internet.	• Rapports datés des audits Active Directory et exposition internet recensant les actifs, vulnérabilités, niveaux de criticité et recommandations • Plan de remédiation exhaustif reliant chaque constat à une action, un responsable, une échéance et une preuve de réalisation • Contre-audit ou nouveau scan démontrant la correction des vulnérabilités prioritaires et, le cas échéant, l'acceptation formalisée du risque résiduel
Cible : Gouvernance. **EE 3** Les incidents significatifs ou graves de sécurité des systèmes d'information sont déclarés sans délai auprès de l'Agence du numérique en santé. Les recommandations et les mesures d'urgence proposées par l'ANSSI, pour limiter l'impact de ceux-ci et destinées à améliorer leur sécurité sont mises en œuvre. À défaut d'incidents significatifs ou graves ayant justifié une déclaration, l'établissement a une procédure qui permet de qualifier ce qui relève d'un incident significatif ou grave et de les déclarer.	• Procédure de qualification et d'escalade des incidents avec critères, suppléances, contacts et canal national de déclaration • Trace horodatée d'un incident ou exercice : détection, qualification, déclaration, accusé/ticket et mesures immédiates • Recommandations CERT Santé/ANSSI reçues et suivi de leur mise en œuvre • Retour d'expérience incluant impacts sur les soins, fonctionnement dégradé, reprise, causes et actions d'amélioration

Critère 3.1-08 - L'identification des utilisateurs dans le système d'information est sécurisée

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** Les règles d'habilitation (accès, droit d'usage...) du système d'information de santé sont définies.	• Procédure de gestion des comptes et habilitations précisant les rôles, le circuit de validation et les règles de création, modification et suppression des droits • Matrice d'habilitation versionnée reliant chaque fonction aux applications et droits autorisés selon le principe du moindre privilège • Compte rendu d'une revue récente comparant les fonctions exercées aux droits

Élément d'évaluation V2027	Éléments de preuve à rechercher
	de comptes réels, avec écarts, corrections et validation de leur clôture
Cible : Gouvernance. **EE 2** Dès qu'un professionnel change de statut (démission, fin de contrat, changement de service...), l'établissement actualise ses habilitations et accès.	• Procédure RH–DSI précisant les événements déclencheurs, responsables, canaux de transmission et délais de modification ou suppression des accès • Notifications ou tickets horodatés reliant la date du départ ou du changement de fonction à la demande puis à l'exécution de la modification des droits • Contrôle d'un échantillon de mouvements récents montrant les comptes désactivés pour les départs et les droits ajustés pour les changements de service
Cible : Gouvernance. **EE 3** L'établissement octroie un poste de l'établissement (poste professionnel) au personnel en mobilité (astreintes ou travail à distance) ou un dispositif d'ouverture de sessions à distance. **Applicabilité de l'EE :** *personnel en mobilité, en astreinte ou en travail à distance.*	• Règles d'équipement et d'accès en mobilité précisant les personnels éligibles, les dispositifs autorisés, le circuit d'attribution et les conditions de restitution • Inventaire ou fiches de remise reliant un poste professionnel ou un droit de session à distance à chaque professionnel concerné • État de conformité d'un échantillon de postes ou sessions montrant chiffrement, verrouillage, mises à jour, protection antimalware et accès distant sécurisé
Cible : Gouvernance. **EE 4** Pour les accès à distance, les identités et accès aux données de santé sont gérés par un système d'authentification renforcé avec deux facteurs. **Applicabilité de l'EE :** *accès à distance aux données de santé.*	• Cartographie des accès distants aux applications contenant des données de santé, avec populations autorisées et mécanismes d'authentification associés • Configuration du VPN, de la passerelle distante ou du fournisseur d'identité imposant deux facteurs indépendants pour les accès concernés • Résultat de test ou journaux d'authentification récents démontrant l'usage du second facteur et le refus d'une connexion réalisée avec le seul mot de passe

Critère 3.3-06 - L'établissement est aisément joignable par les professionnels adresseurs

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** Une messagerie sécurisée de santé permet un accès rapide aux échanges d'informations (données sensibles, résultats d'examen...) entre les professionnels du territoire contribuant à la prise en charge des patients.	• Inventaire des boîtes MSSanté avec propriétaires, services, règles d'accès, suppléance et fréquence de consultation • Organisation du traitement des messages reçus avec responsabilité et délai cible selon le type de flux • Exemple d'échange clinique avec traçabilité de réception, prise en compte et intégration au dossier lorsque nécessaire • Indicateurs ou suivi des erreurs/routages/indisponibilités et actions d'amélioration
Cible : Gouvernance. **EE 2** Sur la base d'une cartographie des échanges de données de santé non sécurisés, l'établissement a établi un plan de transfert vers une messagerie sécurisée de santé.	• Cartographie datée des échanges non sécurisés précisant le document ou la donnée, l'émetteur, le destinataire, le canal, le volume et le risque associé • Plan de transfert reliant chaque flux à une solution MSSanté, une boîte cible, des actions techniques ou organisationnelles, un responsable et une échéance • Tableau de suivi montrant l'état de migration de chaque flux et l'évolution des échanges non sécurisés et des usages MSSanté après les actions réalisées

Critère 3.4-05 - L'établissement pilote l'usage des dispositifs médicaux numériques à usage professionnel faisant appel à un système d'intelligence artificielle

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** L'établissement a réalisé une cartographie des dispositifs médicaux numériques à usage professionnel faisant appel à un système d'intelligence artificielle incluant leur analyse des risques (transmission de données, réutilisation par l'industriel...). **Applicabilité de l'EE :** *dispositif médical numérique à usage professionnel faisant appel à une intelligence artificielle.*	• Cartographie datée et versionnée précisant pour chaque DMN : fabricant, version, finalité médicale, services utilisateurs, statut de déploiement et interfaces SI • Procédure de recensement avec mise à jour au fil de l'eau lors d'un nouvel achat/essai et revue périodique documentée de l'exhaustivité • Analyse des risques et impacts propre à chaque dispositif : sécurité du patient, performances/biais, cybersécurité, données personnelles, flux vers l'industriel ou ses sous-traitants et réutilisation éventuelle • Mesures de maîtrise reliées aux risques avec responsables et risque résiduel • Pour les DMN nécessaires à la continuité des soins : intégration au PCA/PRA, procédure de mode dégradé et test ou exercice de reprise
Cible : Gouvernance. **EE 2** Qu'il en utilise ou pas, l'établissement dispose d'une organisation structurée pour l'acquisition des dispositifs médicaux numériques à usage professionnel faisant appel à un système d'intelligence artificielle qui implique les services compétents, notamment les équipes informatiques, biomédicales et juridiques.	• Procédure d'acquisition/expérimentation précisant les étapes, critères de décision et avis obligatoires des métiers, biomédical, DSI-RSSI, DPO-juridique et achats • Expression formalisée du besoin médical et technologique, population cible et contexte d'utilisation prévu • Comparaison documentée de plusieurs solutions lorsque pertinent : finalité, preuves de performance, limites, interopérabilité, sécurité, données, maintenance, coûts et impacts organisationnels • Dossier d'essai ou protocole pilote lorsque nécessaire, avec critères de succès, incidents, retours utilisateurs et décision motivée de déployer, adapter ou renoncer • Après acquisition : ajout du dispositif à la cartographie et conditions contractuelles relatives aux mises à jour, données, responsabilités et support
Cible : Gouvernance. **EE 3** Lorsqu'il en utilise, l'établissement forme les professionnels utilisateurs d'un dispositif médical numérique à usage professionnel faisant appel à un système d'intelligence artificielle, afin que ces derniers en connaissent les performances, les conditions d'usage et les limites.	• Programme de formation propre au dispositif et à sa version couvrant finalité, population cible, performances, limites, biais, contre-indications et usages hors indication à éviter • Registre nominatif des utilisateurs formés avant accès autonome, avec date et évaluation des acquis

Élément d'évaluation V2027	Éléments de preuve à rechercher
Applicabilité de l'EE : *professionnel utilisant un dispositif médical numérique faisant appel à une intelligence artificielle.*	• Mise en situation montrant que l'utilisateur sait interpréter une sortie, repérer une performance inattendue, éviter le biais d'automatisation et exercer une décision humaine indépendante • Utilisateur capable d'ignorer, corriger ou renverser la sortie du système lorsque la situation clinique l'exige et d'escalader un doute • Formation au signalement des dysfonctionnements et au mode dégradé/PCA-PRA lorsque le dispositif est critique
Cible : Gouvernance. **EE 4** Lorsqu'il en utilise, l'établissement a un processus de contrôle qualité des dispositifs médicaux numériques à usage professionnel faisant appel à un système d'intelligence artificielle impliquant leur supervision humaine en situation réelle d'utilisation. **Applicabilité de l'EE :** *dispositif médical numérique faisant appel à une intelligence artificielle utilisé en situation réelle.*	• Protocole de contrôle qualité précisant dispositif/version, population, responsable, fréquence, échantillon, indicateurs et seuils d'alerte • Audit de dossiers ou journal d'utilisation comparant sorties de l'IA, références cliniques et décisions finales, avec discordances et corrections humaines tracées • Surveillance des performances après changement de version ou évolution notable de l'usage • Personnes chargées du contrôle humain identifiées avec compétence, formation, autorité et soutien nécessaires • Décisions de maintien, restriction, revalidation ou suspension tracées en cas de risque ou de performance inattendue, avec information du fabricant lorsqu'elle est requise
Cible : Gouvernance. **EE 5** Lorsqu'il en utilise, conformément à sa procédure et à la règlementation en vigueur, l'établissement déclare les dysfonctionnements des dispositifs médicaux numériques à usage professionnel faisant appel à un système d'intelligence artificielle (évènements indésirables associés aux soins, évènements de matériovigilance...) et met en place des actions d'amélioration. **Applicabilité de l'EE :** *dysfonctionnement d'un dispositif médical numérique faisant appel à une intelligence artificielle.*	• Procédure reliant gestion des évènements indésirables et matériovigilance, avec critères de gravité, mesures immédiates, rôle du correspondant local et circuit de déclaration • Dossier d'incident ou d'exercice identifiant le dispositif et sa version, les conséquences, les dates, l'accusé de déclaration et les échanges avec l'ANSM ou le fabricant • Analyse des causes et plan d'amélioration retraçant notamment retrait ou suspension, correctif, mise à jour, formation ou surveillance, puis contrôle d'efficacité et clôture

Critère 3.4-06 - L'établissement utilise des systèmes d'intelligence artificielle sans finalité médicale pour améliorer son organisation

Élément d'évaluation V2027	Éléments de preuve à rechercher
Cible : Gouvernance. **EE 1** L'établissement a réalisé une cartographie des systèmes d'intelligence artificielle sans finalité médicale incluant une analyse des risques (transmission de données non sécurisées, réutilisation par l'industriel...) et visant à éradiquer les usages non sécurisés. **Applicabilité de l'EE :** *système d'intelligence artificielle sans finalité médicale utilisé ou repéré dans l'établissement.*	• Cartographie datée des IA sans finalité médicale précisant outil, fournisseur, version, utilisateurs, finalité, données manipulées et statut autorisé, restreint ou interdit • Analyse des flux et risques documentant données personnelles ou de santé, localisation, conservation, réutilisation pour l'entraînement, accès du fournisseur, confidentialité et sécurité • Plan d'éradication des usages non sécurisés avec blocage des outils interdits, solution approuvée, règles diffusées, paramétrages protecteurs et contrôles confirmant la disparition des écarts
Cible : Gouvernance. **EE 2** Qu'il en utilise ou pas, l'établissement dispose d'une organisation structurée pour l'acquisition de systèmes d'intelligence artificielle sans finalité médicale, qui implique les services compétents, notamment les équipes informatiques et juridiques.	• Procédure d'achat, d'essai, de renouvellement ou d'autorisation couvrant aussi les outils gratuits, avec avis métiers, DSI-RSSI, DPO-juridique et achats • Expression du besoin et comparaison de solutions lorsque plusieurs outils peuvent répondre à l'usage envisagé • Grille d'évaluation couvrant finalité, utilisateurs, données et réutilisation fournisseur, sécurité-RGPD, performances/limites, supervision humaine, impacts organisationnels, support et réversibilité • Expérimentation encadrée lorsque nécessaire, avec périmètre, données autorisées/interdites, critères de succès, incidents et décision finale • Décision motivée précisant les conditions d'usage autorisées avant ouverture des accès
Cible : Gouvernance. **EE 3** Dès lors qu'il utilise des systèmes d'intelligence artificielle sans finalité médicale, l'établissement contrôle la qualité du système par une supervision humaine. **Applicabilité de l'EE :** *système d'intelligence artificielle sans finalité médicale utilisé dans l'établissement.*	• Protocole de supervision propre au système/version précisant responsables, contrôles, fréquence, indicateurs et seuils d'alerte • Échantillons de sorties contrôlées montrant erreurs, hallucinations, incohérences ou biais détectés et corrections humaines réalisées • Règle explicite interdisant la reprise automatique d'une sortie non vérifiée dans un document ou une décision organisationnelle lorsqu'une validation humaine est nécessaire • Traces de restriction, correction, suspension ou réévaluation du système après dérive, incident ou réclamation • Revue périodique des performances et de l'adéquation de l'outil à son usage réel
Cible : Gouvernance. **EE 4** Dès lors qu'il en utilise, l'établissement forme les utilisateurs (professionnels de santé ou non) d'un système d'intelligence artificielle sans finalité médicale afin que ces derniers en connaissent les performances, conditions d'usage et limites. **Applicabilité de l'EE :** *utilisateur d'un système d'intelligence artificielle sans finalité médicale.*	• Programme et supports de formation rattachés à chaque système et version, couvrant usages autorisés, performances, limites, erreurs possibles, données interdites, supervision et signalement • Liste nominative des utilisateurs concernés avec dates de formation ou de sensibilisation, fonction, système utilisé et trace de remise des consignes avant ouverture des accès • Mise en situation, quiz ou évaluation pratique montrant que l'utilisateur sait repérer une sortie non fiable, la corriger ou l'écarter, protéger les données et déclencher l'alerte prévue
Cible : Gouvernance. **EE 5** Dès lors qu'il en utilise,	• Fiche d'évaluation préalable propre à chaque système avec situation de départ,

Élément d'évaluation V2027	Éléments de preuve à rechercher
l'établissement évalue l'impact sur l'organisation des soins de l'utilisation de chaque système d'intelligence artificielle sans finalité médicale recensée (substitution permettant des temps de proximité avec le patient, impact positif sur leur prise en charge...). **Applicabilité de l'EE :** *système d'intelligence artificielle sans finalité médicale utilisé dans l'établissement.*	objectifs attendus, activités concernées, indicateurs, responsables et calendrier de mesure • Résultats avant-après mesurant notamment temps administratif, temps de proximité avec le patient, délais, charge de travail, qualité-sécurité et effets non souhaités • Compte rendu de revue associant métiers et gouvernance, avec analyse des résultats, décision de poursuivre, ajuster ou arrêter, plan d'action et nouvelle mesure programmée

Sources officielles et références

Références principales propres au guide « Audit système - Risques numériques - Gouvernance ». Registre consolidé mis à jour le 4 novembre 2026.

- Référentiel de certification des établissements de santé pour la qualité des soins, Version 2027
- Mettre en œuvre le 6e cycle de certification, mise à jour septembre 2026
- Fiche pédagogique : méthode de l'audit système
- L'évaluation de l'usage des dispositifs médicaux et outils technologiques numériques, Novembre 2025
- Technologies numériques et systèmes d'IA à usage professionnel
- Agence du Numérique en Santé - Indicateurs de partage et d'échange des données de santé
- Données de santé : mesures de sécurité et de confidentialité pour l'accès au dossier patient
- Violations de données personnelles : les règles à suivre
- CERT Santé - signalement et traitement des incidents de sécurité
- Programme CaRE - Audits des annuaires techniques et de l'exposition sur internet
- Guide pratique RGPD - Sécurité des données personnelles, version 2024
- Authentification multifacteur : recommandations de la CNIL
- Politique générale de sécurité des systèmes d'information de santé - PGSSI-S
- Doctrine du numérique en santé 2025 - MSSanté
- Guide de déploiement des usages MSSanté en établissement de santé
- Guide d'aide au choix des dispositifs médicaux numériques à usage professionnel
- IA et santé : développer et évaluer des systèmes d'IA conformes
- MDCG 2025-6 - articulation entre dispositifs médicaux et règlement sur l'IA
- Technologies numériques et systèmes d'IA à usage professionnel, mise à jour 3 mars 2026
- Règlement (UE) 2024/1689 sur l'intelligence artificielle, articles 14 et 26
- Guide d'aide au choix des dispositifs médicaux numériques à usage professionnel, 2023

Note : ce kit constitue une aide à l'évaluation interne. Il ne se substitue ni au référentiel officiel, ni aux grilles mises à disposition dans Calista, ni à l'appréciation des experts-visiteurs.