AUDIT SYSTÈME | KIT 19 / 20

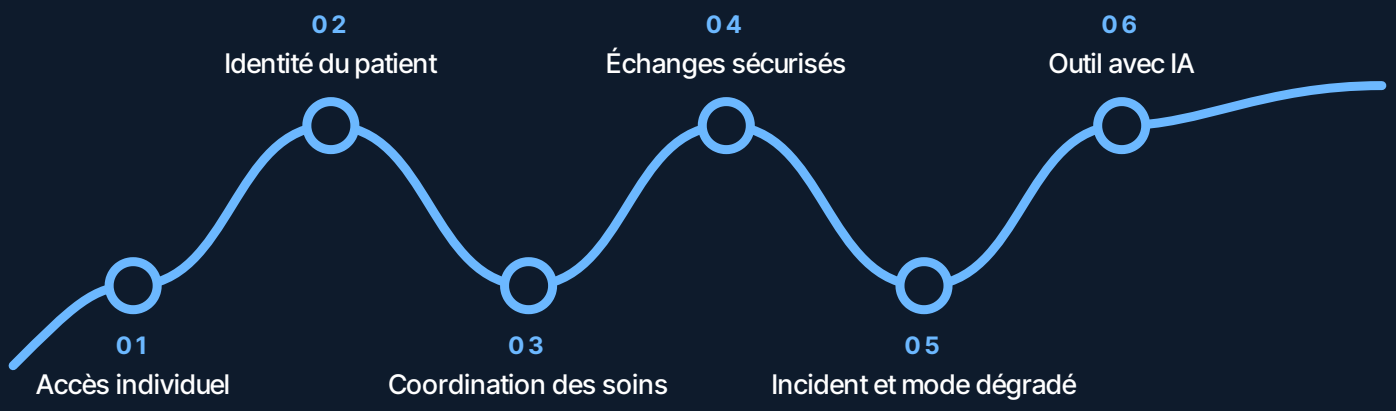
# Risques numériques : professionnels

Vérifier sur le terrain les pratiques numériques des professionnels : identité, confidentialité, accès, partage, mode dégradé, incidents et usage sécurisé des outils.

**6** CRITÈRES

**10** 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.

Documentation libre : hospi-academy.com
hospiacademy@hospi-academy.com

# 9. Audit système - Risques numériques - Professionnels

*6 critères • 10 éléments d'évaluation*

Vérifier sur le terrain les pratiques numériques des professionnels : identité, confidentialité, accès, partage, mode dégradé, incidents et usage sécurisé des outils.

## Guide méthodologique - Conduire cet audit système avec rigueur

### 1. Définir le périmètre et l'échantillon

Sélectionner au moins deux unités et un parcours patient utilisant le DPI, l'identité nationale de santé, le partage d'informations et, si présent, un dispositif médical numérique avec IA. Observer plusieurs métiers et un changement d'équipe ou de secteur.

**À préparer avant l'audit**

Règles d'accès et de confidentialité ; liste des utilisateurs et habilitations ; procédures d'identitovigilance ; DPI et projet de soins ; MSSanté, DMP ou Mon espace santé ; formations ; modes dégradés ; signalement des incidents ; consignes cyber ; documentation du DM numérique ou de l'IA.

**Personnes à rencontrer**

Médecins, infirmiers, aides-soignants, secrétaires, professionnels médico-techniques, encadrement, support informatique, identitovigilance et référent du dispositif numérique. Interroger des utilisateurs nouveaux et expérimentés.

### 2. Déroulé de l'audit système

| Étape | Niveau vérifié | Ce que l'auditeur doit démontrer |
|---|---|---|
| 1 | **Accès individuel** | Observer ouverture et fermeture de session, identifiant nominatif, verrouillage, gestion d'un changement de poste et conduite tenue devant un droit inadapté. |
| 2 | **Identité du patient** | Suivre recherche, création ou sélection de l'identité, qualification INS, traitement d'une anomalie et vérification avant un acte ou document. |
| 3 | **Coordination des soins** | Vérifier projet de soins partagé, transmissions, alertes, résultats, documents de sortie et disponibilité de l'information pour les professionnels concernés. |
| 4 | **Échanges sécurisés** | Examiner l'usage de MSSanté, DMP ou Mon espace santé, les destinataires, documents envoyés, information du patient et absence de canal non sécurisé. |
| 5 | **Incident et mode dégradé** | Faire décrire perte d'accès, poste suspect ou erreur d'identité ; vérifier consignes, support, formulaires, reprise, resaisie et signalement. |
| 6 | **Outil avec IA** | Si applicable, observer formation, limites connues, vérification du résultat, décision humaine, possibilité de correction et déclaration d'un incident. |

### 3. Conclure et coter

Croiser observation, dossier, droits, formation et réponse aux incidents. Qualifier séparément un défaut individuel, un problème d'habilitation, un outil mal conçu ou une gouvernance insuffisante.

> **Exigence de rigueur -** *Ne jamais demander à un professionnel de révéler son mot de passe ni organiser un test d'hameçonnage sans autorisation. Toute démonstration doit utiliser un contexte de soins et des données légitimement accessibles.*

## Éléments d'évaluation et preuves à rechercher

**Exigence de rigueur -** Ne jamais demander à un professionnel de révéler son mot de passe ni organiser un test d'hameçonnage sans autorisation. Toute démonstration doit utiliser un contexte de soins et des données légitimement accessibles.

### 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 : Professionnels.** **EE 1** Les documents de santé intégrant des données médicales à caractère personnel ne sont pas conservés sur le poste de travail. | • Absence de documents patients conservés durablement sur le poste local lors d'un contrôle accompagné<br>• Circuit démontré vers DPI, espace réseau sécurisé ou outil institutionnel autorisé<br>• Suppression du fichier temporaire après intégration et absence de copie dans corbeille/dossiers usuels selon le fonctionnement du poste<br>• Conduite à tenir connue en cas de découverte d'un fichier local : sécurisation, suppression selon procédure et signalement si nécessaire |

### Critère 2.1-02 - Les équipes se coordonnent pour la mise en œuvre du projet de soins personnalisé grâce à un système d'information adapté et partagé

| Élément d'évaluation V2027 | Éléments de preuve à rechercher |
|---|---|
| **Cible : Professionnels.** **EE 1** Pour obtenir le consentement du patient, les médecins connaissent les documents de son dossier qui doivent être versés dans Mon espace santé. | • Liste ou matrice validée des documents à verser dans Mon espace santé selon leur type et l'activité du service, accessible aux médecins concernés<br>• Support d'information du patient et emplacement prévu dans le dossier pour tracer son accord, son refus ou son opposition selon la procédure de l'établissement<br>• Dossier échantillonné montrant les documents produits, leur statut de versement dans Mon espace santé et, en cas de rejet, la cause et le retraitement réalisé |

### Critère 2.2-01 - Les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge

| Élément d'évaluation V2027 | Éléments de preuve à rechercher |
|---|---|
| **Cible : Professionnels.** **EE 1** Les règles d'identification du patient, définies par l'établissement (charte d'identitovigilance) sont appliquées : qualification de l'identité nationale de santé (INS) par du personnel formé lors d'une première venue en présence du patient, mode dégradé (rejet du téléservice, indisponibilité du système d'information, anonymat...). | • Démonstration sur dossier test de la validation de l'identité à partir d'un dispositif de haut niveau de confiance, de l'appel INSi et du passage au statut d'INS qualifiée<br>• Traçabilité de la qualification indiquant le statut de l'identité, le résultat d'INSi, la date et l'utilisateur habilité, avec concordance des traits stricts dans le référentiel et le DPI<br>• Procédure de mode dégradé et cas récent ou exercice montrant le statut provisoire, les restrictions appliquées, puis le rapprochement, la correction et la qualification après rétablissement<br>• INS du mineur distincte de celle de ses parents, avec traits d'identité concordants dans le référentiel et le DPI<br>• Qualification réalisée par du personnel formé à partir des justificatifs et du dispositif de confiance prévus pour l'âge et la situation du mineur<br>• Pour les nouveau-nés avant disponibilité/qualification de l'INS : identité provisoire sécurisée, contrôles renforcés et procédure de rapprochement après disponibilité de l'identité nationale<br>• Procédure de mode dégradé en cas de discordance ou indisponibilité et traçabilité de la correction/qualification ultérieure<br>• Cas test ou dossier anonymisé montrant l'absence de confusion avec l'identité du parent |
| **Cible : Professionnels.** **EE 2** Les équipes déclarent les non-conformités auprès de la cellule / comité d'identitovigilance (doublons, collision, impossibilité de qualification de l'identité nationale de santé...) sur la base d'un document précisant les anomalies à déclarer et les modalités de déclaration. | • Document accessible aux équipes listant les anomalies à déclarer (doublon, collision, discordance, identité erronée ou qualification INS impossible) et leurs modalités de signalement<br>• Formulaire ou outil dédié d'identitovigilance avec circuit, coordonnées du référent ou de la cellule et distinction claire entre anomalie d'identité et EIAS<br>• Déclaration récente anonymisée retraçant la détection, les dossiers ou flux sécurisés, l'analyse, la correction ou fusion contrôlée, la propagation de l'information et la clôture |

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

| Élément d'évaluation V2027 | Éléments de preuve à rechercher |
|---|---|
| **Cible : Professionnels.** **EE 1** Les équipes connaissent les conduites à tenir en cas d'incident ou d'attaque (contact du service en charge de la sécurité informatique, modes dégradés...). | • Professionnel capable d'expliquer immédiatement alerte, sécurisation et continuité sans improvisation<br>• Coordonnées d'urgence disponibles hors SI et fiche réflexe accessible<br>• Kit de mode dégradé complet et à jour : supports papier, règles d'identification, prescription/administration, examens et priorités de soins selon activité<br>• Procédure de retour à la normale et de réintégration des données avec contrôle de complétude et prévention des doublons<br>• Exercice ou incident récent connu de l'équipe avec enseignements partagés |
| **Cible : Professionnels.** **EE 2** Les équipes connaissent les règles | • Démonstration sur un exemple de courriel montrant le repérage de l'adresse |

| Élément d'évaluation V2027 | Éléments de preuve à rechercher |
|---|---|
| de sécurité et d'hygiène informatique (identification des mails frauduleux...). | réelle, du lien, de la pièce jointe et des indices d'urgence ou d'usurpation, puis le signalement par le canal prévu<br>• Charte ou fiche d'hygiène informatique remise aux professionnels précisant verrouillage du poste, confidentialité des mots de passe, mises à jour, supports amovibles et outils de partage autorisés<br>• Résultats récents de sensibilisation ou de simulation d'hameçonnage, avec professionnels concernés, erreurs observées, actions ciblées et nouvelle mesure montrant leur appropriation |
| **Cible : Professionnels.** **EE 3** Les équipes sont formées à l'utilisation des logiciels métier et peuvent être accompagnées par un interlocuteur compétent pour la prise en main des outils. | • Parcours de formation défini par logiciel, version et profil utilisateur, avec supports à jour couvrant les fonctions critiques, erreurs fréquentes et conduite à tenir en cas de difficulté<br>• Traçabilité nominative de la formation avant utilisation autonome, complétée par un exercice, une mise en situation ou une évaluation montrant la maîtrise des tâches attendues<br>• Canal de support clairement accessible avec interlocuteurs, horaires et modalités d'escalade, accompagné d'un ticket ou d'une demande récente retraçant réponse, résolution et délai |

### 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 : Professionnels.** **EE 1** Pour proscrire tous les comptes génériques, dès son arrivée, le personnel, y compris temporaire (intérimaires, étudiants, stagiaires...), utilise un compte permettant une connexion nominative, un identifiant et un mot de passe personnels et uniques pour l'accès au système d'exploitation. | • Session ouverte sous un identifiant nominatif propre au professionnel<br>• Absence de partage d'identifiants ou recours à un compte générique<br>• Verrouillage du poste connu et appliqué lors de l'éloignement<br>• Circuit d'aide disponible en cas de compte bloqué sans contournement des règles<br>• Retrait/ajustement des accès signalé lors d'un départ ou changement de fonction |
| **Cible : Professionnels.** **EE 2** Pour proscrire tous les comptes génériques, dès son arrivée, le personnel, y compris temporaire (intérimaires, étudiants, stagiaires...), utilise un compte permettant une connexion nominative, un identifiant et un mot de passe personnels et uniques pour l'accès aux applications métiers (ex : DPI). | • Démonstration de la connexion au DPI ou à l'application métier avec un compte personnel, puis consultation du journal attribuant une action test au professionnel connecté<br>• Demande d'habilitation validée reliant l'identité du professionnel, sa fonction, l'application, le profil de droits et les dates d'ouverture ou de fin d'accès<br>• Revue des comptes de l'application et échantillon de journaux confirmant l'absence de comptes partagés, la traçabilité individuelle des actions et le retrait des accès obsolètes |

### 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 : Professionnels.** **EE 1** Lorsque les professionnels utilisent un dispositif médical numérique à usage professionnel faisant appel à un système d'intelligence artificielle d'aide à la décision médicale impliquant un traitement de données algorithmiques (par exemple : à visée diagnostique ou thérapeutique), ils s'assurent que le patient en a été informé et qu'il est averti de l'interprétation qui en résulte.<br>**Applicabilité de l'EE :** *intelligence artificielle d'aide à la décision médicale utilisant des données algorithmiques.* | • Support ou trame d'information propre au DMN précisant sa finalité, le recours à l'IA, la nature de son résultat, ses limites et le maintien d'une décision humaine<br>• Dossier patient identifiant le dispositif utilisé, la date, le professionnel et l'information délivrée avant son utilisation<br>• Lorsque applicable : information sur la transmission ou la réutilisation des données conformément au cadre de protection des données<br>• Compte rendu distinguant clairement sortie algorithmique, interprétation par le professionnel, éventuelle discordance et décision clinique expliquée au patient<br>• Trace des questions, réserves ou incompréhensions du patient et des réponses apportées lorsque pertinent |

## Sources officielles et références

Références principales propres au guide « Audit système - Risques numériques - Professionnels ». 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
- Référentiel national d'identitovigilance et Référentiel INS
- Guide d'aide au choix des dispositifs médicaux numériques à usage professionnel
- Sécuriser les postes de travail
- Mon espace santé - Professionnels de santé
- Guide mémo Identitovigilance - Certification HAS 2025
- Guide d'hygiène informatique
- 10 règles d'or en matière de sécurité numérique
- Impliquer et former les utilisateurs
- Authentifier les utilisateurs
- Gérer les habilitations
- Se former à la e-santé
- Technologies numériques et systèmes d'IA à usage professionnel, mise à jour 3 mars 2026

*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.*