



Ma fiche certification

DSI / RSSI

Mes repères qualité au quotidien, reliés aux critères du référentiel HAS V2027.

8 repères pratiques

Niveaux HAS vérifiés

1 avancé

Chapitre 3.1 et 3.4

Repères pratiques Hospi-Academy, actualisés le 26 septembre 2026 à partir du référentiel HAS V2027, applicable aux visites à compter du 1er janvier 2027. La V2025 reste applicable jusqu'au 31 décembre 2026. Les exemples et questions sont des propositions pédagogiques, à adapter au métier, aux activités et aux procédures de l'établissement ; ce document n'est ni une publication ni une validation de la HAS.

IMPÉRATIF Exigence fondamentale pouvant influencer sur la décision

STANDARD Attendu de certification

AVANCÉ Souhaité, non exigible à ce jour

1 Cybersécurité et plan blanc numérique

Repères à adapter à votre activité

3.1-05 **IMPÉRATIF**

Intégrer le numérique au plan de gestion des tensions et des situations sanitaires exceptionnelles

Intégrer les risques numériques au plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles. Garantir les outils dont la cellule de crise a besoin pour être opérationnelle dans les 45 minutes suivant l'alerte : communication, accès aux données, postes de secours. Prévoir la continuité des activités critiques en cas de cyberattaque, participer aux exercices et mettre en œuvre les actions issues du retour d'expérience.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Quel est votre rôle en cas de déclenchement du plan et qu'avez-vous amélioré après le dernier exercice ?*

3.1-07 **STANDARD**

Piloter un programme structuré de maîtrise des risques de sécurité numérique

Disposer d'un plan de continuité et de reprise d'activité formalisé. Mettre en œuvre le plan d'actions correctives issu des audits Active Directory et d'exposition sur internet. Déclarer sans délai les incidents significatifs ou graves sur le portail de signalement des événements sanitaires indésirables (transmission à l'ARS et à l'ANS / CERT Santé) et appliquer les mesures d'urgence de l'ANSSI ; à défaut d'incident, disposer d'une procédure pour les qualifier et les déclarer. Faire connaître aux équipes la conduite à tenir en cas d'incident ou d'attaque et les modes dégradés, et les former aux logiciels métier avec un interlocuteur identifié.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Comment poursuivez-vous une activité critique si le système d'information devient indisponible ?*

REPÈRE V2027	NIVEAU DU CRITÈRE	EXEMPLES DE SUPPORTS À CONSULTER
3.1-05 · Organisation de crise	Impératif	Volet numérique, exercices et retours d'expérience
3.1-07 · Risques numériques	Standard	Analyse de risques, continuité/reprise, signalements applicables
3.1-08 · Accès au SI	Standard	Habilitations, revues des droits, traçabilité

2 Identités numériques et accès au SI

*Repères à adapter à votre activité*3.1-08 **STANDARD**

Sécuriser l'identification des utilisateurs et proscrire les comptes génériques

Définir les règles d'habilitation au système d'information (accès, droits d'usage). Dès son arrivée, chaque professionnel, intérimaire, étudiant ou stagiaire compris, dispose d'un compte nominatif avec identifiant et mot de passe personnels : les comptes génériques sont proscrits. Mettre à jour les habilitations dès qu'un professionnel change de statut (départ, fin de contrat, changement de service). Fournir un poste professionnel ou une session à distance sécurisée au personnel en astreinte ou en télétravail, avec authentification à deux facteurs pour accéder à distance aux données de santé.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Comment les droits sont-ils adaptés lorsqu'un professionnel arrive, change de fonction ou quitte l'établissement ?*

3 Données de santé et Mon Espace Santé

*Repères à adapter à votre activité*1.1-03 / 3.3-06 **1.1-03 : STANDARD** **3.3-06 : STANDARD**

Protéger les données de santé et sécuriser leurs échanges

Contrôler les accès au dossier patient pour faire cesser les connexions illégitimes, qui violent le secret, et faire connaître aux équipes les risques et sanctions encourus. Disposer, avec le DPO, d'une procédure d'information des patients en cas de fuite de leurs données. Déployer une messagerie sécurisée de santé (MSSanté) pour les échanges avec les professionnels du territoire : cartographier les échanges de données de santé non sécurisés et suivre un plan de transfert vers la MSSanté.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Comment repérez-vous une connexion illégitime au dossier patient, et que se passe-t-il ensuite ?*

4 Télésanté, IA médicale et innovations numériques

*Repères à adapter à votre activité*3.4-04 **STANDARD**

Soutenir techniquement le déploiement de la télésanté

Mettre à disposition des professionnels des outils de télésanté conformes aux exigences applicables, choisis avec les utilisateurs, et prévoir une solution de repli en cas de difficulté technique. Former les équipes aux outils et aux procédures. Contribuer à l'évaluation de l'activité de télésanté ; pour la télésurveillance médicale, l'activité est déclarée au préalable à l'ARS.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Comment garantissez-vous la continuité et la confidentialité lorsqu'un acte de télésanté rencontre une difficulté technique ?*

3.4-05 **STANDARD**

Encadrer les dispositifs médicaux numériques utilisant l'IA

Cartographier les dispositifs médicaux numériques à usage professionnel, en particulier ceux qui font appel à l'intelligence artificielle. Organiser leur acquisition avec les équipes informatiques, biomédicales et juridiques. Former les utilisateurs aux performances, aux conditions d'usage et aux limites, organiser une supervision humaine

en situation réelle et déclarer les dysfonctionnements (EIAS, matériovigilance), suivis d'actions d'amélioration. Lorsqu'une IA d'aide à la décision médicale est utilisée, le patient en est informé.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Comment les utilisateurs connaissent-ils les limites d'un dispositif et contrôlent-ils ses résultats ?*

3.4-06 **AVANCÉ**

Encadrer les systèmes d'IA sans finalité médicale

Cartographier les systèmes d'intelligence artificielle sans finalité médicale utilisés ou repérés dans l'établissement (rédaction, planification, traduction...), analyser leurs risques (données transmises, réutilisation par l'éditeur) et faire cesser les usages non sécurisés. Organiser leur acquisition avec les services compétents, notamment informatiques et juridiques. Assurer une supervision humaine, former les utilisateurs aux performances et aux limites, et évaluer l'effet sur l'organisation des soins. Ce critère est avancé.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Quels outils d'IA sans finalité médicale sont utilisés dans l'établissement, et comment avez-vous repéré ceux qui n'étaient pas sécurisés ?*

Σ Mémo · Ce que l'expert attend de la DSI/RSSI

Repères impératifs de cette fiche

3.1-05 · 3.2-12

Préparer un exemple concret

Une situation récente, les informations disponibles, la décision prise et son suivi. Les documents cités sont des exemples de supports, pas une liste officielle de preuves exigées.

Croiser les points de vue

Comparer le vécu du patient, les pratiques des équipes, l'organisation et les résultats ; expliquer les écarts et les actions engagées.

Faire vivre les repères au quotidien

Votre contribution DSI : sécuriser les outils et les accès, organiser la continuité technique et coopérer avec les utilisateurs, le RSSI et le DPO.

LEXIQUE CLÉ · CERTIFICATION HAS V2027

CERT Santé : Cellule de l'Agence du numérique en santé (ANS) qui accompagne les établissements face aux incidents de sécurité informatique. Les incidents significatifs ou graves de sécurité des systèmes d'information se déclarent sans délai sur le portail de signalement des événements sanitaires indésirables, qui les transmet à l'ARS et à l'ANS (critère 3.1-07).

MSSanté : Messageries sécurisées de santé : espace de confiance qui permet aux professionnels d'échanger des données de santé de façon sécurisée, y compris avec le patient via Mon espace santé. Elles évitent l'envoi de données de santé par une messagerie non sécurisée.

PCA / PRA : Plan de continuité d'activité et plan de reprise d'activité : organisation prévue pour maintenir les activités critiques en mode dégradé pendant une panne ou une cyberattaque, puis pour rétablir les systèmes. Le critère 3.1-07 attend un plan formalisé.

DMN : Dispositif médical numérique : logiciel ou application ayant une finalité médicale au sens de la réglementation des dispositifs médicaux. Le critère 3.4-05 porte sur ceux à usage professionnel qui font appel à l'intelligence artificielle.

MFA : Authentification multifacteur : connexion qui exige au moins deux preuves distinctes (mot de passe et code ou carte, par exemple). Le critère 3.1-08 l'attend pour les accès à distance aux données de santé.

HDS : Hébergeur de données de santé : tout prestataire qui héberge sur support numérique des données de santé pour le compte d'un établissement doit être certifié HDS (article L1111-8 du Code de la santé publique).

3.2-12 IMPÉRATIF

Prévenir les violences sexistes et sexuelles entre professionnels

Connaître les comportements concernés, les interlocuteurs et le circuit de signalement des violences sexistes et sexuelles entre professionnels, étudiants compris. Accueillir la parole sans minimiser les faits, protéger la personne et l'orienter vers les relais compétents. L'établissement organise prévention, formation, traitement des signalements et accompagnement des victimes. Distinguer ce circuit de la gestion ordinaire des conflits.

QUESTION D'ENTRAÎNEMENT PROPOSÉE PAR HOSPI-ACADEMY : *Si vous êtes victime ou témoin de violences sexistes et sexuelles, qui pouvez-vous contacter et quel accompagnement est prévu ?*

Références

- [HAS · Référentiel HAS V2027](#)
- [HAS · Tableau comparatif V2025 / V2027](#)
- [HAS · EIAS / EIGS](#)
- [HAS · Violences sexistes et sexuelles](#)
- [HAS · Ressources professionnelles](#)
- [HAS · SSE](#)
- [HAS · Page de référence et calendrier des publications](#)

Hospi-Academy · Mes repères qualité · HAS V2027 · Actualisation du 26 septembre 2026 · Document pédagogique indépendant de la HAS