Le Comptoir Qualité

CCECQA

AGISSONS POUR DEMAIN

Lundi 27 avril 2026
de 13h30 à 14h30

Catherine POURIN et Fabrice D'HOLLANDER, CCECQA

Décryptages des critères du manuel de certification 2025 :

Outils Numérique et sécurité des Systèmes d'information

Action financée par l'ARS Nouvelle-Aquitaine dans le cadre du CPOM ARS-CCECQA 2023-2027

Sécurité numérique en visite HAS : exigences et organisation

- Deux objectifs dans le manuel de certification HAS
  - Objectif 3.1 : Le management global par la qualité et la sécurité des soins
    - 3 Critères : maitrise des risques numériques ; sécurisation des accès ; sécurisation des données
  - Objectif 3.4 : L'adaptation à des soins écoresponsables et aux innovations numériques
    - 2 critères sur le bon usage de IA
- Investigations par EVN en J2 mais aussi par l'ensemble des EV
- Un membre de l'équipe spécialiste SI présente les divers documents à l'expert-visiteur numérique lors du temps dédié sur le calendrier de visite (J2 matin)
- Une veille de la sécurité numérique qui s'appuie sur une documentation demandée en amont et pendant la visite
- Une attention aux formations et sensibilisations, aux audits de sécurité numérique et aux exercices cyber

Investigations en visite

- Audit système en gouvernance (1h30)
  - Direction générale
  - Direction informatique
  - RSSI
  - DPO
  - Référent DMN
  - PCME ?
  - Responsable fonctionnel(le) ?
- Entretiens professionnels (J2 après midi)
  - Rencontre des professionnels de l'accueil administratif 15 mn
    - Admission
    - Admission Urgences
  - Rencontres de professionnels dans les services de soins 45 mn
    - IDE
    - ASH
    - Médecin

Audits de sécurité numérique

- Audit active Directory (OraAD)
  - Evaluation de la gestion des identités et des droits d'accès afin de garantir que chaque professionnel accède uniquement aux données nécessaires à sa mission, dans un cadre sécurisé et traçable
  - Audit régulier sur le niveau de sécurité de l'Active Directory des établissements
- Audit d'exposition Internet (SILENE)
  - Analyse des services et équipements accessibles depuis l'extérieur afin d'identifier les vulnérabilités exploitables et de réduire le risque d'intrusion;
  - Audit mensuel pour vérifier qu'il n'y a pas de faille exploitable
- Attention à bien avoir un plan d'action des actions correctrices mises en œuvre suite à ces audits !
- Ces deux type d'audits n'empêche pas de faire des audits de sécurité de type pentest ou autres

CCECQA

Exercices cyber, scenario Des exemples

- Simulation d'un incident numérique majeur visant à tester la gouvernance, la continuité des soins et la capacité de réaction de l'établissement.
  - Blocage du SI et indisponibilité du DPI
  - Indisponibilité du DPI ou de la messagerie
  - Exfiltration supposée de données patients
  - Envoi d'un faux mail piégé aux professionnels
  - Réunion simulée de crise sans mobilisation technique
  - Test de restauration des sauvegardes
  - Panne électrique
  - Cryptage d'une partie ou de l'ensemble du SIH

Incidents significatifs ou grave, des exemples

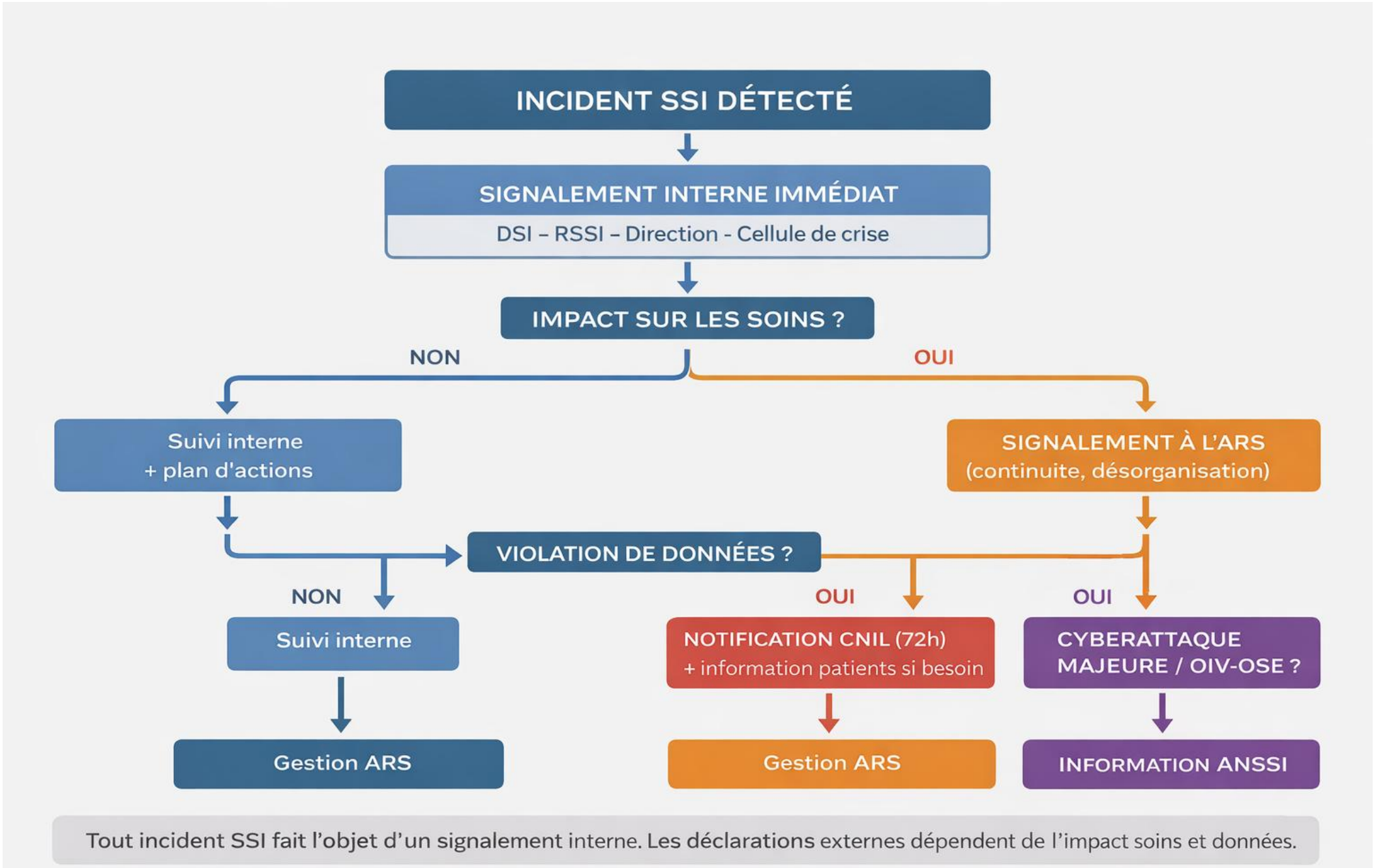
Atteinte à la disponibilité, par exemple : Ransomware bloquant le DPI ou la prescription informatisée ; Indisponibilité prolongée du serveur d'identité patient ; Panne majeure du réseau impactant les urgences ou le bloc)

Atteinte à la confidentialité, par exemple : Exfiltration de données de santé ; Piratage de comptes professionnels avec accès massif aux dossiers ; Publication accidentelle de données patients en ligne

Atteinte à l'intégrité, par exemple : Altération ou suppression de données médicales; Modification frauduleuse d'une prescription; Corruption de bases de données critiques

Compromission d'identités numériques, par exemple : Usurpation d'un compte administrateur; Comptes génériques utilisés de manière inappropriée ; Vol d'identifiants via phishing réussi;

Mauvaise configuration exposant l'établissement, par exemple : Serveur accessible sans authentification; Port RDP ouvert sur Internet sans MFA; Sauvegardes accessibles depuis l'extérieur


INCIDENT SSI DÉTECTÉ
SIGNALEMENT INTERNE IMMÉDIAT
DSI – RSSI – Direction - Cellule de crise
IMPACT SUR LES SOINS ?
NON
OUI
Suivi interne
+ plan d'actions
SIGNALEMENT À L'ARS
(continuite, désorganisation)
VIOLATION DE DONNÉES ?
NON
OUI
OUI
Suivi interne
NOTIFICATION CNIL (72h)
+ information patients si besoin
CYBERATTAQUE
MAJEURE / OIV-OSE ?
Gestion ARS
Gestion ARS
INFORMATION ANSSI
Tout incident SSI fait l'objet d'un signalement interne. Les déclarations externes dépendent de l'impact soins et données.

Critère n°3.1-07 : Les risques de sécurité numérique sont maîtrisés

Crit.3.1-07-ee03-ASY : L'établissement déploie **un plan de formation** pluri-annuel à la sécurité et l'hygiène informatique et organise des **actions de sensibilisation** à destination de tous les professionnels.

Crit.3.1-07-ee04-ASY : L'établissement a formé des **référents sécurité SI** en relais des équipes SI **dans les secteurs de soins.**

Crit.3.1-07-ee05-ASY : 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**.

Critère n°3.1-08 : L'identification des utilisateurs et des patients dans le système d'information est sécurisée

Crit.3.1-08-ee01-ASY : Les règles d'habilitation (accès, droit d'usage…) du système d'information de santé sont définies.

Crit.3.1-08-ee02-ASY : Pour proscrire les comptes génériques, l'établissement gère les arrivées/départs pour l'octroi des habilitations au système d'information (notamment pour les intérimaires, étudiants, stagiaires…).

Crit.3.1-08-ee03-ASY : 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.

Crit.3.1-08-ee04-ASY : Pour les accès à distance, les identités et accès aux données de santé sont gérés par un système d'authentification renforcé avec deux facteurs.

Critère n°3.1-09 : Les données du patient sont sécurisées

Crit.3.1-09-ee01-ASY : L'établissement a cartographié les échanges de données de santé non sécurisés et établi un plan de transfert vers une messagerie sécurisée de santé.

Crit.3.1-09-ee02-ASY : La qualité et la complétude des éléments versés dans Mon espace santé sont évaluées par l'établissement. Les résultats sont diffusés, en CME et en CDU, et donnent lieu à un plan d'actions pour améliorer le taux d'alimentation du dossier médical partagé.

Crit.3.1-09-ee03-ASY : En cas de fuite des données, une procédure est prévue pour informer les patients victimes de la fuite de leurs données. Le cas échéant, elle a été mise en œuvre.

Intelligence Artificielle

Critère n°3.4-05 : L'établissement pilote l'usage des dispositifs médicaux numériques professionnels, en particulier ceux faisant appel à l'intelligence artificielle

Crit.3.4-05-ee01-ASY : L'établissement établit et met à jour, au moins une fois par an, une cartographie de l'ensemble des dispositifs médicaux numériques à usage professionnel et, le cas échéant, analyse les risques et l'impact de chacun (transmission de données, réutilisation par l'industriel…).

Crit.3.4-05-ee02-ASY : Pour répondre aux besoins des équipes de soins, l'établissement dispose d'une organisation structurée pour l'acquisition des dispositifs médicaux numériques qui implique les services compétents, notamment les équipes informatiques et juridiques.

Crit.3.4-05-ee03-ASY : L'établissement organise la formation des professionnels utilisateurs d'un dispositif médical numérique afin que ces derniers en connaissent les performances, les conditions d'usage et les limites.

Crit.3.4-05-ee04-ASY : Dans le contexte de soins, pour les dispositifs médicaux numériques à usage professionnel, l'établissement se dote d'un processus de contrôle qualité impliquant, le cas échéant, un contrôle humain des résultats donnés par les dispositifs médicaux numériques en situation réelle d'utilisation.

Crit.3.4-05-ee05-ASY : Conformément à l'organisation de l'établissement et à la règlementation en vigueur, les utilisateurs déclarent les dysfonctionnements potentiels des dispositifs médicaux numériques à usage professionnel (évènements indésirables associés aux soins, ou, pour les dispositifs médicaux numériques, évènements de matériovigilance…).

Critère n°3.4-06 : L'établissement utilise des outils technologiques innovants sans finalité médicale pour améliorer son organisation, en particulier ceux faisant appel à l'intelligence artificielle

Crit.3.4-06-ee01-ASY : L'établissement maîtrise l'acquisition d'outils technologiques innovants sans finalité médicale, en particulier ceux faisant appel à l'intelligence artificielle, en associant les équipes informatiques et juridiques.

Crit.3.4-06-ee02-ASY : L'établissement se dote d'un processus de contrôle qualité pour ce type d'outils, dès lors qu'il s'agit de technologies dont le fonctionnement repose sur un système d'intelligence artificielle.

Crit.3.4-06-ee03-ASY : Les professionnels qui les utilisent sont formés à l'utilisation de ces technologies, aux conditions d'usage et à leurs limites.

Crit.3.4-06-ee04-ASY : L'établissement évalue l'impact de l'utilisation des outils technologiques innovants sur l'organisation des soins : substitution permettant des temps de proximité avec le patient, un impact positif sur leur prise en charge...

Un dispositif médical numérique est un logiciel, une application ou une solution numérique qui est destiné par son fabricant à être utilisé, seul ou en association, à des fins médicales précises, par exemple

- Prévention (ex. suivi de facteurs de risque, prévention de rechutes)
- Diagnostic (ex. aide à l'interprétation d'images, analyse de signaux biologiques)
- Pronostic (ex. calcul du risque d'évolution d'une maladie)
- Traitement (ex. logiciels de thérapie numérique – « digital therapeutics »)
- Surveillance (ex. télésurveillance d'une pathologie chronique, suivi post-opératoire)

La HAS distingue ces dispositifs de simples applications de bien-être ou de santé grand public (ex. podomètres, applis de méditation sans visée médicale), qui ne relèvent pas du cadre des dispositifs médicaux.

Exemples typiques de DMN selon la HAS :

- Applications de thérapie numérique validées (ex. TCC digitalisées pour dépression, insomnie)
- Logiciels d'aide au diagnostic médical (imagerie, dermatologie, ophtalmologie, etc.)
- Outils de télésurveillance de maladies chroniques (diabète, insuffisance cardiaque, etc.)
- Logiciels d'aide à la prescription ou au suivi thérapeutique

Polyclinique de Limoges

Cartographie des DMN à usage professionnel
Validée en COSSI du 10/10/2025

Dispositifs médicaux numériques (DMN) à usage professionnel

Logiciels relevables du droit commun (certifiés selon un référentiel national)	Logiciels hors droit commun
Oncologie — Résilience Pro	**Endoscopie** (IA) — Module Genius IA
Médecin / Pharmacien — Module HM de prescription LAP	
Cardiologie — Télésurveillance (pacemaker, holter)	
Sommeil — Analyse du sommeil (Cidelec)	

Polyclinique de Limoges

Cartographie des Outils Innovants
Validée en COSSI du 10/10/2025

Outils Innovants

Analyse de la satisfaction patient (IA) — Better World

CECQA

Dans CALISTA deux mois minimum avant la visite et actualisés si nécessaire

- Schéma directeur des SI ou orientations stratégiques des SI ou projet des SI
- Rapport d'activité de la CDU (incluant des informations relatives à Mon espace santé)
- + PAQSS (intégrant les actions relatives aux usages du numérique en santé)
- PCA / PRA
- Charte d'utilisation des ressources informatiques
- charte de connexion des SI par les prestataires
- Cartographie des applicatifs
- Plan Blanc (avec un volet cyber)

Mis à disposition des EV lors de la visite

- Politique générale de sécurité des SI
- Plan de formation/sensibilisation sur la sécurité numérique
- Matrice d'habilitation
- Procédures de gestion et listes d'habilitation des accès et comptes aux différents logiciels métiers - prestataires compris (liste des tunnels et VPN) +Procédure de gestion des identités pour les patients (INS) et de mise en œuvre des bonnes pratiques en matière d'identitovigilance,
- Liste des déclarations d'incidents auprès des autorités compétentes,
- Bilan des exercices cyber : identification des bonnes pratiques et actions d'amélioration + bilan audits sécurité numérique et plan d'actions SSI, actions de remédiation identifiées,
- Attestation des audits sécurité des systèmes d'information (si établissement éligible),
- Audit technique : bilan audits sécurité numérique et plan d'actions SSI, actions de remédiation identifiées
- Fiche de poste référent SSI Santé
- Cartographie des usages non sécurisés d'échanges de données de santé et plan d'action pour les résorber
- Cartographie des DMN, Procédures pour l'achat, le suivi, les déclarations d'incidents, les preuves de formation spécifiques des équipes soignantes.....
- Outils innovants : cartographie des outils innovants, procédures pour l'achat, le suivi, évaluation de l'impact de l'utilisation des outils innovants sur l'organisation des soins.....
- Les PCA PRA des fournisseurs d'applications (GHT, hébergeurs HDS.....)