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

CCECQA

AGISSONS POUR DEMAIN

Le risque numérique dans la certification HAS le 4 avril 2024

Catherine POURIN, Directeur du Ccecqa
Yvon RICHIR, Directeur d'établissement, Réseau des professionnels référents du Ccecqa
Fabienne SOLEILHAVOUP, Déléguée à la protection des données, Polyclinique de Limoges

Thèmes abordés

- Rappel des critères spécifiques d'usage numérique
- Quels sont les attendus pour la sécurisation des échanges et le partage des données ?
- Quel niveau de maîtrise des risques numériques attend-on en termes de pilotage, d'actions et d'évaluation ?
- Quels documents à élaborer ou à compléter ?
- Quels sont les professionnels rencontrés ?
- Questions/réponses à l'aide du menu conversation

Supports et replays sur
www.ccecqa.fr
à la rubrique ressources

Les attendus

- Répondre à l'enjeu de la sécurité informatique en cohérence avec les politiques publiques en matière du numérique et de sécurité (HOP'EN, SUN-ES, programme CaRE, feuille de route du numérique 2023-2027)

NOUVEAU A PARTIR DU 02/01/2024 DANS LE REFERENTIEL DE CERTIFICATION

Les objectifs

1) Evaluer la qualité des pratiques dans l'utilisation des outils et supports numériques, et la sensibilisation/formation aux risques, à travers:

- la gestion des risques numériques
- la promotion des bons usages, l'utilisation des outils numériques et les données patient

2) Évaluer la gestion des risques numériques dans les pratiques de soins mais aussi dans les fonctions supports (biomédical par exemple)

CE N'EST PAS: un audit technique ou une inspection qui évalue la sécurité des systèmes d'information

C'EST: un audit de résultat centré sur les professionnels

LES CRITERES D'USAGE DU NUMERIQUE

- **La gestion des risques numériques:**
  - le critère 3.6-02: maîtrise par l'établissement du risque de sécurité numérique (EVN)
  - le critère 3.6-06: la sécurisation de l'identification des professionnels dans le système d'information (EVN)
- **La promotion des bons usages et l'utilisation des outils:**
  - le critère 1.1-18: l'information du patient (EV)
  - le critère 2.2-05: l'usage du système d'information pour l'accès au dossier du patient (EVN, EV)
  - le critère 2.3-01: le respect des bonnes pratiques d'identification du patient (EV)
  - le critère 3.1-07: la sécurisation des usages des communications informatiques d'informations médicales (EVN, EV)
  - le critère 3.2-09: l'accès du patient à son dossier (EVN, EV)

Le critère 3.6-02: les risques numériques sont maîtrisés

Objectif 3.6
L'établissement dispose d'une réponse opérationnelle adaptée aux risques auxquels il peut être confronté

Critère 3.6-02 Les risques de sécurité numérique sont maîtrisés

Pour maîtriser au plus juste le risque numérique, l'établissement doit pouvoir s'appuyer sur un système d'information sécurisé, prévoir un plan d'action de continuité et sensibiliser l'ensemble des professionnels pour accroître l'implication des acteurs et la vigilance collective. Une veille de sécurité numérique (prévention active de la sécurité des systèmes d'information) suivant les recommandations de l'ANSSI est mise en place.

Tout l'établissement | Standard

Éléments d'évaluation

Gouvernance

- L'établissement a déployé un plan de continuité d'activité et un plan de reprise d'activité dans tous les secteurs.
- L'établissement a initié les correctifs à 6, 12 et 18 mois sur les actions critiques recommandées par l'audit de sécurité numérique.
- L'établissement organise régulièrement des actions de sensibilisation individualisées pour les professionnels de santé.
- L'établissement a démarré un plan de formation pluri-annuel à la sécurité informatique et à la mise en œuvre du mode dégradé pour tous les professionnels concernés.
- L'établissement a formé des référents sécurité SI en relais des équipes SI dans les secteurs les plus à risques.
- 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.

Professionnels

- Les équipes connaissent les conduites à tenir en cas d'incident/d'attaque (contact du référent de la sécurité numérique, identification des mails frauduleux...).
- Les équipes savent mettre en œuvre à tout moment leur plan de continuité d'activité et leur plan de reprise d'activité.
- Les équipes sont sensibilisées au besoin d'éradiquer sur leur poste de travail la conservation de documents de santé intégrant des données médicales à caractère personnel.

Audit système

Fiches pédagogiques

- Évaluation de la gestion des risques et des vigilances.
- Évaluation de la gestion des risques numériques dans les pratiques de soins.

Références légales et réglementaires

- Art. L. 6111-2 al. 1 du CSP.
- Art L. 1111-8-2 du CSP.
- Instruction 309 de 2016. 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.
- L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur.
- Prestataires d'audit de la sécurité des systèmes d'information, référentiel d'exigences.
- 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 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.

Autres références

- PSSI-S.Programme HOP'EN – Guide des indicateurs des prérequis du socle commun.
- Boîte à outils pour l'atteinte des prérequis HOP'EN – ANAP, 2019.
- Référentiel d'identification électronique.

HAS

HAUTE AUTORITÉ DE SANTÉ

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

selon le référentiel de certification

Date validation Collège le 7 septembre 2023

- 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.

CCECQA

Les risques numériques dans le calendrier de visite

- Les critères investigués par les EV le sont dans les audits système gouvernance, ou rencontres avec les professionnels et également lors de patients traceurs : tout au long de la visite

- Les critères investigués par l'EVN sont dans un audit « risques numériques » avec la gouvernance et la DSI et par des audits systèmes rencontres avec les professionnels : le deuxième jour de la visite

La méthode de l'audit système

= Évaluation des organisations de l'établissement pour s'assurer de leur maîtrise sur le terrain.

Se déroule en 3 étapes, et dans cet ordre :

- **La prise de connaissance des documents mis à disposition :**
  * sur la plateforme Calista avant la visite
  * sur place pendant la visite (documents sensibles)
- **La rencontre avec la Gouvernance**
- **La rencontre avec les Professionnels de terrain**

Focus sur le planning de consultation documentaire faite par l'EVN

Calendrier de visite :

Attention, l'expert visiteur n'est présent qu'une seule journée. Un temps d'une heure de consultation de la documentation sur place lui est alloué.

<u>Si la visite commence le lundi:</u>

Les EV sont présents dans l'ES dès le lundi matin

et l'EVN rejoint l'équipe d'EV dans l'après midi ou fin d'après midi. Il peut donc en théorie commencer la consultation documentaire dès le lundi.

De plus , 1 heure de consultation lui est consacrée le mardi matin. L'EVN a du temps pour s'approprier les documents mis à disposition sur place.

Focus sur le planning de consultation documentaire faite par l'EVN

Si la visite commence le mardi:

L'équipe au complet (EV et EVN) commence la visite dès le mardi matin, ce qui ne laisse qu'une heure à l'EVN pour consulter la documentation sur place (doc sensible)

Conclusion :

La documentation pour l'EVN doit être accessible dès J1, même si l'EVN n'est prévu qu'à J2. La consultation étant chronophage, mettre à disposition de l'EVN soit un classeur papier avec tous les documents demandés, soit un dossier informatisé dédié à EVNUM. Cela évite le temps d'appropriation d'une gestion documentaire, et donc fait gagner du temps à l'EVN

Le calendrier de visite de l'EVN

MATIN :

- **La consultation documentaire (1 heure si J2, ou plus si arrivée fin J1)**
- **Une réunion commune EVN + Gouvernance + DSI (2 heures)**
  - **Gouvernance élargie :** Directeur, Directeur Adjoint, Qualité, président de CME, directeur des soins, gestionnaire des risques, responsable des relations ville/hôpital, représentant des usagers, Responsable de la Cellule IDTV, responsable de la gestion administrative des patients, médecin Dim
  - **DSI :** DSI, DPO, RSSI…

APRES-MIDI :

- **2 ou 3 services, avec les professionnels**

Tous les professionnels peuvent être rencontrés, principalement les acteurs impliqués dans la qualification de l'identification des patients: équipes de soins (urgences, maternité, etc..) et équipes administratives (bureau des admissions, des consultations, urgences, etc…)

Les documents à présenter:

- **Documents à déposer sur Calista:**

  - le schéma directeur des SI ou orientations stratégiques des SI ou projet des SI
  - le rapport de la CDU (informations relatives à Mon Espace Santé)
  - le PAQSS intégrant les actions relatives aux usagers du numérique en santé
  - la cartographie du SI applicatif
  - le PCA/PRA
  - la charte d'utilisation des ressources informatiques incluant la charte de connexion des SI par les partenaires

- **documents à présenter dès le 1er jour de la visite, dans cet ordre (servent à conforter les constats au regard de chaque élément d'évaluation du critère 3.6-02)**

  - la politique générale de sécurité des SI
  - le volet numérique du plan blanc
  - le plan de formation/sensibilisation sur la sécurité numérique
  - la matrice d'habilitation
  - les procédures de gestion et listes d'habilitation des accès et comptes aux différents logiciels métiers, prestataires compris (liste des tunnels et VPN)
  - la procédure de gestion des identités pour les patients (INS) et de mise en œuvre des bonnes pratiques en matière d'identitovigilance
  - la liste des déclarations d'incidents auprès des autorités compétentes (ANSSI/ARS/CERT Santé, etc)
  - l'attestation des audits sécurité des systèmes d'information
  - le bilan audits sécurité numérique et plan d'actions SSI, actions de remédiation identifiées
  - bilan des exercices cyber: identification des bonnes pratiques et actions d'amélioration, type d'exercice, périodicité

Que cherche l'Expert Visiteur Numérique ?

L'EVN souhaite évaluer 2 fondamentaux dans les visites de certification

- La qualité des pratiques dans l'usage des outils numériques
- Le niveau de sensibilisation, de formation de l'ensemble des professionnels de l'ES, notamment sur l'hygiène informatique et les risques qui sont liés au numérique.

La consultation de la documentation permet de mesurer la maturité du SI de l'établissement vis-à-vis des risques numériques, et son niveau de résilience face aux risques cyber.

Les documents recherchés sont identiques à ceux définis dans les programmes Hop'En, Sun'ES, Care, la feuille de route du Numérique en Santé … + ceux en lien avec les règles d'Identitovigilance, d'échanges entre professionnels, entre professionnel et patients …

L'EVN vérifie la bonne diffusion de la politique, des activités et des actions de l'établissement sur la thématique concernée et sa déclinaison par les professionnels.
Les exercices et simulations sont à conduire annuellement.

La synthèse

- Pas de NA sur les critères numériques

- Une synthèse en fin de chapitre 3 du rapport adressée à l'établissement sur Calista mais qui ne sera pas publiée sur le site internet de la HAS

- La synthèse précise les pratiques qui ne correspondant pas aux attendus du référentiel

- Pas de commentaire sur les risques numériques en séance de restitution générale

Questions/réponses

Agenda

PROCHAIN WEBINAIRE

Mardi 25 juin 2024 de 13h30 à 14h30

Inscription

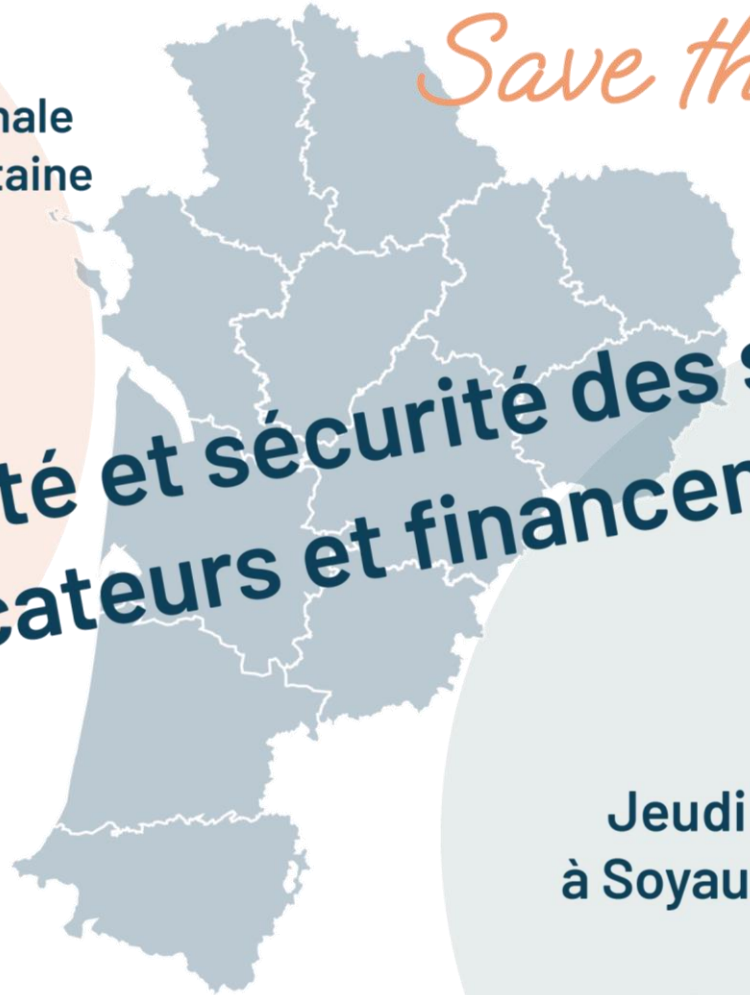
QVCT et Parentalité

Avec l'intervention de Annabelle FERRE-JANICOT et Hassanat MARCHAND (ARS-Nouvelle-Aquitaine) et Catherine POURIN (CCECQA)

CCECQA

Rencontre régionale
de Nouvelle-Aquitaine

Save the date



Qualité et sécurité des soins : indicateurs et financements

Jeudi 20 juin 2024
à Soyaux (Angoulême)

CCECQA
AGISSONS POUR DEMAIN

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

CCECQA

Toute notre actualité

Sur notre site internet

www.ccecqa.fr

Contact

communication@ccecqa.fr

Inscription à la Newsletter mensuelle

https://www.ccecqa.fr/newsletter/

Suivez-nous