

Fiche repère pour les Représentants des usagers : les critères numériques de la certification qualité HAS

Cybersécurité

protéger les patients et leurs données



Quel est le cadre des actions de cybersécurité ?

- La cybersécurité regroupe l'ensemble des mesures techniques, informatiques et organisationnelles mises en œuvre pour prévenir les incidents de sécurité tels que les fuites de données, pertes accidentelles, accès non autorisés, ruptures de confidentialité, etc.
- Elle contribue à la protection des données des patients et donc du secret médical.
- Le Règlement Général de la Protection des Données (RGPD) édicte des règles de bonne gestion des données qui sont la base de leur protection, et inclus des référentiels pratiques de sécurité qui s'appliquent aux dispositifs médicaux, services de télémédecine, etc.
- Des agences publiques (CNIL, ANSSI, ANS, etc.) interviennent pour soutenir, outiller et financer la cybersécurité, notamment dans les établissements de santé : comme le programme CaRE du Ministère chargé de la santé (750 millions € sur 4 ans).



Comment cela se passe dans les établissements ?

Les établissements de santé sont de plus en plus touchés ces dernières années par les menaces cyber.

Les établissements sont vulnérables pour plusieurs raisons :

- Dans un contexte tendu de financement, les budgets alloués à la sécurité informatique ne font souvent pas partie des investissements prioritaires des établissements. On estime que les établissements dépensent la moitié de ce qui serait nécessaire dans ce domaine.
- Le manque de compétences informatiques touche le domaine de la santé et plus particulièrement les établissements publics, moins attractifs que d'autres secteurs ou employeurs.
- Le nombre d'agents, soignants et administratifs, ayant des accès informatiques est très important et multiplie les portes d'entrée potentielles pour les menaces cyber qui reposent majoritairement sur les erreurs humaines.



Les impacts des cyberattaques sont nombreux sur les établissements :

- Le blocage des systèmes informatiques empêche l'accès aux dossiers des patients, prescriptions médicales, résultats d'examens, etc. et impose le passage au papier. Cela représente des contraintes fortes d'organisation, de continuité et de sécurité des soins. Dans certains cas des services entiers doivent être fermés (urgences, réanimation) avec un impact sur l'accès aux soins sur le territoire.
- Les cyberattaques ont un impact durable (mois voire années) et un coût pour les établissements, jusqu'à plusieurs millions d'euros, pour identifier et résoudre l'origine de l'attaque, reconstruire l'informatique, palier la perte d'activité, etc.



Fiche repère pour les Représentants des usagers : les critères numériques de la certification qualité HAS

Cybersécurité

secret médical

protection

confidentialité



Comment les critères de la certification HAS sont-ils évalués ?

- **Une gouvernance est établie** pour planifier les actions de préparation contre les cyberattaques ;
- **Des exercices de crise / simulations** de cyberattaque sont organisés régulièrement une à deux fois par an ;
- **Des Plans de Continuité et de Reprise d'Activité (PCRA)** sont rédigés et régulièrement mis à jour.

guide HAS en cours de révision



Comment contribuer à cette évaluation ?

Dans les établissements qui ont été touchés par un incident cyber :

- Faire remonter le vécu des représentants des usagers, leur information sur la mise en place des mesures dégradées et les témoignages qui auraient été partagés par les usagers ;
- Faire remonter le vécu des patients impactés, la manière dont ils ont été informés et les mesures éventuelles pour les accompagner.



En amont de la certification, les représentants des usagers peuvent participer à la préparation de la réponse cyber :

- Participer à sensibiliser les soignants en rappelant comment les usagers voient leurs données de santé et l'importance de protéger leur confidentialité.
- Assister ou participer à des exercices de crises / simulation de cyberattaque, pour partager le rôle du représentant des usagers et sa connaissance transversale de l'établissement.
- Discuter les modalités d'information des usagers, sur les efforts de préparation de la réponse cyber pour les rassurer et sur leur information en cas d'incident.
- Demander une présentation annuelle en CDU des mesures de préparation de la réponse cyber mises en place en prévision (formation des professionnels, financements obtenus, actualisation de procédures, renforcement des systèmes, etc.).

