
Quelle place pour le Système d'Information dans la certification des établissements

Chapitre 2
Référence 18

Ressources transversales.
Le système d'information.

18.a

Le système d'information est organisé pour faciliter la prise en charge des patients.

Précisions

- Les bases de connaissance contiennent des recommandations, référentiels d'évaluation, nomenclatures, documents juridiques, etc., utiles à la prise en charge des patients. Les supports possibles sont divers : Internet, intranet, revues, ouvrages de référence, etc.
- Les données nécessaires portent notamment sur les demandes d'examens complémentaires, les rendez-vous, les comptes rendus, etc.

Éléments d'appréciation

- Identification des besoins des secteurs d'activité en termes de SI.
- Mise à disposition des professionnels, des bases de connaissances utiles à la réalisation des différentes activités.
- Communication des données nécessaires à la prise en charge des patients et à sa coordination, en temps utile et de façon adaptée aux besoins.
- Accompagnement et formation des professionnels concernés pour traiter et utiliser les données.

Certification V2

Chapitre 2
Référence 18

Ressources transversales.
Le système d'information.

18.b

Une identification fiable et unique du patient est assurée.

Précisions

- L'identification fiable et unique du patient permet de connaître l'ensemble des informations contenues dans son dossier. Un état des lieux permet d'apprécier les pratiques liées à l'identification du patient et sa fiabilité en termes de création d'identifiant, d'utilisation, de correction d'identité, etc.
- L'existence de procédures permet de contrôler l'identification du patient à toutes les étapes de sa prise en charge et donc la mise en concordance des identités lors des échanges de données (identitovigilance).
- Les procédures de contrôle de l'identification du patient peuvent porter, par exemple, sur l'identité provisoire créée au niveau des urgences, les fusions d'identités, les corrections d'identité, la gestion des doublons, la perte de données, la persistance de l'identité du patient de l'admission jusqu'aux plateaux techniques et jusqu'au service des archives.

Éléments d'appréciation

- Politique d'identification du patient.
- Organisation permettant la diffusion et la mise en œuvre de procédures de contrôle de l'identification du patient.
- Information et/ou formation des professionnels.

18.c

La sécurité du système d'information est assurée.

Précisions

- La définition d'une politique de sécurité couvre :
 - L'organisation et le management de la sécurité, comprenant notamment la désignation d'un responsable de la sécurité du système d'information ;
 - La définition des principes de sécurité à mettre en œuvre pour les applications et les données du système d'information de l'établissement ;
 - L'inventaire et la classification des différentes ressources intervenant dans le système d'information (documents, données, matériels, logiciels, etc.) ;
 - L'évaluation des risques (d'accident, d'erreur, de malveillance) et le choix de mesures constituant une réponse proportionnée ;
 - L'élaboration d'un plan d'actions ;
 - Les conditions d'utilisation de dispositifs de sécurité par le personnel de l'établissement de santé et par les usagers externes (patient, professionnel de santé) ainsi que les services de support et d'accompagnement nécessaires (formation, sensibilisation, hot line, etc.) ;
 - La mesure de l'efficacité des dispositifs de sécurité et leur mise à jour ;
 - Les actions de formation et d'information des utilisateurs.
- Une des composantes de la politique de sécurité est la définition des droits d'accès aux informations dans un établissement et les droits d'écrire et/ou de valider une information. Elle suppose que les personnels de l'établissement soient correctement identifiés et qualifiés. Ceci est facilité par des annuaires tenus à jour.

Éléments d'appréciation

- Politique de sécurité pour assurer l'intégrité, la disponibilité, la confidentialité des données et la traçabilité des accès au SI.
- Contrôle qualité des données (notamment information médicale issue du PMSI).
- Sécurité technique de l'environnement assurée.
- Information des professionnels sur les contraintes liées à l'utilisation des ressources informatiques.
- Mise en œuvre des démarches et formalités prévues par la législation Informatique et libertés.

Certification V2 – Rôle du DSI

- **Dimension fonctionnelle : applications, informations disponibles, bases de connaissances, cohérence du SI dans son ensemble (identité patient, dossier patient, SGL, imagerie...)**
- **Dimension technique : sécurité informatique (serveurs, réseau, salle informatique, support et maintenance...)**

Certification V2 – Rôle du DSI

➤ **Veiller à la cohérence et à l'intégrité du SI ainsi que son utilisation :**

- Charte d'utilisation des ressources informatique
- Unicité de l'identité patient (propagation de l'identité, fusion des identités, procédures de contrôle de cohérence)
- Définition des habilitations et des profils donnant accès aux informations du SI
- Traçabilité des accès

Certification V2 – Rôle du DSI

➤ **Veiller à la sécurité informatique des systèmes en place :**

- Définition d'une politique de sécurisation du système d'information avec cartographie des risques
- Identifier un Responsable de la sécurité informatique
- Salle informatique (secours électrique, codes d'accès, climatisation, sauvegardes, réseau...)
- Sécurité logique (sécurité du poste de travail, virus, firewall...)
- Plan de reprise après incident
- Tests des sauvegardes...

Certification V2 – Point de vue de l'expert-visiteur

➤ **Constats :**

- Forte hétérogénéité des dispositifs en place
- L'exigence ne peut être pas être la même dans un CHU que dans une petite clinique
- Peu d'établissements répondent totalement aux critères
- Peu de compétences informatiques dans les établissements de petite et moyenne tailles
- Très peu de vrais responsables de la sécurité informatique
- Très peu de suivi des habilitations et des droits d'accès
- Risque rarement analysés tant sur la plan fonctionnel que sur le plan technique
- Rares évaluations des dispositifs
- Aucun audit réalisé par consultants spécialisés

Axes d'amélioration

- **Sensibiliser chaque établissement aux conséquences d'une perte de données, d'un vol de données, d'une identité corrompue...**
- **Intégrer dans la fiche de poste du DSI l'obligation de mettre en œuvre les dispositifs garantissant une sécurité**
- **Promouvoir les formations liées à la sécurité informatique**
- **Sensibiliser le corps médical sur les points liés à la traçabilité des accès aux informations médicales**
- **Définir un niveau de sécurité « minimum » auquel chaque établissement devra répondre dans le processus de certification**

Merci de votre attention....

