COURS D'INFORMATIQUE

Master IMSD

M. OUEDRAOGO Boukary,
MD, MPH , PhD

Mail: ouedbouks@gmail.com

SECURITE DES SYSTEMES D'INFORMATION

I. Maîtriser la sécurité du Système d'Information (SI) – Comment ?

II. Définition de la sécurité du Système d'Information dans les établissements de santé

SECURITE DES SYSTEMES D'INFORMATION

I. Maîtriser la sécurité du Système d'Information (SI) – Comment ?

II. Définition de la sécurité du Système d'Information dans les établissements de santé

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1 - LES OBJECTIFS DE LA SECURITE DU SYSTÈME D'INFORMATION (SI)

Trois grands objectifs sont fixés à la démarche de sécurité du SI.

1.1 - Objectif 1 : Garantir l'intégrité de l'information en évitant toute altération ou perte de données

Réduire le risque de perte ou d'altération des données du SI est l'un des objectifs principaux.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Pour atteindre cet objectif, l'une des actions prioritaires doit porter sur **la mise en œuvre d'un plan de sauvegarde des données du SI.** L'expérience montre que ce plan n'est jamais efficace à moins d'être testé régulièrement (sauvegardes incomplètes, restauration impossible, absence de procédures de reprise des données non sauvegardées, etc.) ; ces tests sont **exécutés avec la collaboration des utilisateurs du SI** de l'établissement.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1.2 - Objectif 2 : S'assurer de la continuité des services en cas de défaut grave de l'informatique

Elaborer un plan de continuité d'activité pour s'assurer qu'en toutes circonstances, les activités vitales de l'établissement ne seront pas arrêtées.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1.3 - Objectif 3 : Garantir la confidentialité des données à caractère personnel

Un établissement traitant des données à caractère personnel sont qualifiées de sensibles par la loi « informatique et libertés »: santé+++

SECURITE DES SYSTEMES D'INFORMATION

I. Maîtriser la sécurité du Système d'Information (SI) – Comment ?

II. Définition de la sécurité du Système d'Information dans les établissements de santé

Définition de la sécurité du Système d'Information dans les établissements de santé

1 - LA SECURITE DU SYSTEME D'INFORMATION

Le système d'information (SI) ne se réduit pas à l'informatique ; il regroupe l'ensemble des moyens humains, techniques et organisationnels visant à assurer le traitement, le stockage et l'échange d'informations nécessaires aux activités de l'établissement.

Définition de la sécurité du Système d'Information dans les établissements de santé

2 -LES NOTIONS FONDAMENTALES DE LA SECURITE (DICPAhA: DISPONIBILITE, INTEGRITE, CONFIDENTIALITE, PREUVE, AUTHENTIFICATION, AUTORISATION)

La sécurité regroupe 6 notions fondamentales : la disponibilité (D), l'intégrité (I), la confidentialité (C), la preuve ou Non-Répudiation (P/NR), l'Authentification (Ah), et l'Autorisation (A).

Définition de la sécurité du Système d'Information dans les établissements de santé

2.1 - La disponibilité (D) : un niveau contextualisé selon l'usage du SI (financier, médical, gestionnaire …).

La disponibilité des SI permet de garantir en permanence la communication et l'échange des données, sans défaut y compris pendant les heures non ouvrées.

La disponibilité des SI qui aident à la production doit être au centre des préoccupations sécuritaires des établissements.

Une panne entraîne l'arrêt du DPI – *Etablissement de la région du Limousin* « La panne d'un serveur dont le contrat de maintenance est arrivé à échéance, entraine l'arrêt du DPI. Plus aucun dossier patient n'est accessible »

Un virus bloque la production – *Etablissement de la région du Limousin* « Un virus non détecté par le logiciel anti-virus se propage, rendant inutilisables les postes de travail jusqu'à l'intervention d'un technicien spécialisé »

?

Définition de la sécurité du Système d'Information dans les établissements de santé

2.2 - L'intégrité (I) : une fiabilité maximale des données (santé, financières…)

L'intégrité est l'objectif d'exactitude et de fiabilité des données et des traitements.

Les SI doivent garantir que les informations sont identiques et inaltérables dans le temps et l'espace et certifier leur exhaustivité, leur validité et leur cohérence. En ce sens, la sécurité du SI contribue aux actions d'identito-vigilance.

Une défaillance provoque des erreurs des dys-fonctionnements – *Etablissement de la région Nord Pas de Calais*

« Une mise à jour de l'application DPI (Dossier Patient Informatisé) a provoqué une modification de tous les numéros d'identification des patients, ayant failli entraîner une erreur de prescription médicamenteuse. »

« Des éléments de calcul ont été involontairement modifiés et cela a provoqué des erreurs de paie massives »

?

Définition de la sécurité du Système d'Information dans les établissements de santé

2.3 - La confidentialité (C) : un accès modulable aux données sensibles.

La confidentialité permet de réserver l'accès aux données aux seules personnes autorisées. Les données confidentielles sont les suivantes :

- Les informations protégées par le secret (justice médicale)
- Les informations privées des collaborateurs,

Définition de la sécurité du Système d'Information dans les établissements de santé

2.3 - La confidentialité (C) :

- Les informations de toute autre nature soumises à une obligation légale ou règlementaire de confidentialité (marchés publics par exemple)
- Les informations stratégiques dont la divulgation interne ou externe peut nuire à la réputation ou au fonctionnement de l'établissement.

Des cas divers de divulgation – *Région Nord Pas de Calais*

« Des personnels accèdent aux dossiers médicaux de leur collègue »

« Des personnes extérieures pénètrent dans des bureaux et consultent des dossiers patients »

« L'assistante a laissé par inadvertance des documents de direction sur l'imprimante »

« Un prestataire informatique intervient dans l'établissement et fait la copie de tous les DPI de l'établissement pour disposer de données de test »

?

Définition de la sécurité du Système d'Information dans les établissements de santé

2.3 - La preuve (P) : Assure le fait qu'une personne ou entité ne puisse nier avoir effectué une activité.

La preuve permet l'investigation en cas de dysfonctionnement et d'incidents d'identifier le responsable.

Dans le domaine du courrier électronique, la non-répudiation est utilisée pour assurer que le destinataire ne pourra nier avoir reçu l'information, et assurer que l'expéditeur de la source de l'information ne peut nier avoir envoyé l'information.

Définition de la sécurité du Système d'Information dans les établissements de santé

2.3 - La preuve (P) : la conservation de traces à valeur de preuve

Les SI doivent pouvoir fournir la preuve d'un évènement donné et permettre la vérification du bon déroulement des traitements informatiques réalisés par les applications.

Les mécanismes généralement employés sont la génération de traces informatiques et un système d'imputabilité qui permet d'associer une action à son auteur.

L'absence de preuve sur l'auteur d’un document dont la lecture aboutit à une erreur médicale, ne permet pas d'imputer l'erreur à la personne réellement en cause et de trouver la source des erreurs.

Définition de la sécurité du Système d'Information dans les établissements de santé

2.3 – L' Authentification (Ah) : Assure l'identification de l'origine de l'information

2.3 – L' Aurisation (A) : concerne le type d'activité ou d'information qu'une personne ou entité est autorisé à effectuer ou accéder

Conclusion

Les pertes **d'intégrité**, de **disponibilité**, de **confidentialité** et **de traçabilité** de l'information, peuvent engendrer des conséquences importantes dans tous les domaines de traitement de l'information, ainsi que des répercussions possibles sur la notoriété de l'établissement.

Ces conséquences seront considérées comme des manquements graves aux obligations éthiques et aux engagements de l'établissement

MERCI