Revue de l'Infirmier Congolais
Article Original e-ISSN: 3006 - 2187 p-ISSN: 2520 - 0844

Le Dossier Médical Informatisé et le défi de la protection des données individuelles des patients

The Electronic Medical Record and the challenge of protecting individual patient data

Frank Nduu Nawej [1,2], Didier Kapinga Kayembe [1], Pascal Nawej Tshimwang jr [1], Joseph Pyana Kitenge [1], Fulgence Mbayo Ilunga [1], Romain Ngoy Shindano [3], Henri Mundongo Tshamba [4,5], Pascal Nawej Tshimwang Sr [1]

[1] *Centre Médical Du Centre ville (C.M.D.C.), Lubumbashi, République Démocratique du Congo.*
[2] *Institut d'études & Recherches pour la Qualité en Santé (IReQS), Lubumbashi. République Démocratique du Congo.*
[3] *Bureau Central de la Zone de Santé de Lubumbashi(BCZS), Lubumbashi. République Démocratique du Congo.*
[4] *Institut Supérieur des Techniques Médicales de Kolwezi(ISTM), Kolwezi. République Démocratique du Congo.*
[5] *Faculté de Médecine de l'université de Lubumbashi, Lubumbashi, République Démocratique du Congo.*

Résumé

Introduction. Le dossier médical informatisé tend à se généraliser au sein de nombreux établissements de santé privés de Lubumbashi. Si ses avantages sont indéniables, il sied de noter toutes fois que le DMI présente des faiblesses liées au risque des pertes ou d'usurpation des données patient qui sont réputées sensibles car relevant du secret médical.

Méthodes. L'étude a consisté en un questionnaire fermé et écrit élaboré sur la base des standards internationaux de sécurité informatique, en l'occurrence le prescrit du Mémento de sécurité informatique pour les professionnels de santé en exercice libéral Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). Sur base d'une participation volontaire, une partie de ce questionnaire a été administrée aux différents professionnels de santé du CMDC utilisant régulièrement le DMI (médecins, infirmiers, techniciens de laboratoire et techniciens d'imagerie) et une autre était destinée aux administrateurs du dit logiciel. Au total 64 personnes ont participé à l'enquête dont 59 utilisateurs et 05 administrateurs du DMI.

Résultats. Les données rapportées au sujet de l'accès aux données patient se trouvant sur le DMI, leur conservation ou encore leur partage, suggère un faible niveau de protection.

Conclusion. Le caractère sensible des données patient impose au CMDC et aux autres établissements des soins de santé d'améliorer les pratiques de leur personnel utilisant le dossier médical informatisé en vue d'une sécurité optimale dans l'enregistrement, le traitement et la conservation des informations dont la nature relève du secret médical.

Mots-clés : *Dossier médical, dossier Médical papier, dossier Médical informatisé, données patient.*

Abstract

Introduction. The computerized medical record tends to become generalized in many private health establish ments in Lubumbashi. While its advantages are undeniable, it should always be noted that the DMI has weakne-

Correspondance:
Frank Nduu Nawej, Centre Médical Du Centre Ville (C.M.D.C), Lubumbashi, République Démocratique du Congo.
Téléphone: +243 998 189 012 - Email: frankduu@yahoo.fr
Article reçu: 27-10-2021 **Accepté**: 03-01-2022
Publié: 11-01-2022

Pour citer cet article: Nawej FN, Kayembe DK, Tshimwang jr PN, Kitenge P, Ilunga FM, Shindano RN, Tshamba HM, Tshimwanga Sr PN. Le Dossier Médical informatisé et le défi de la protection des données individuelles des patients. Revue de l'Infirmier Congolais. 2022;6(1):1-9. https://doi.org/10.62126/zqrx.2022611

sses linked to the risk of loss or theft of patient data which is deemed to be sensitive because it falls under medical confidentiality.

Methods. The study consisted of a closed and written questionnaire drawn up on the basis of international IT security standards, in this case the prescription of the IT security guide for health professionals in private practice General Information Systems Security Policy of Health (PGSSI-S). On the basis of voluntary participation, part of this questionnaire was administered to the various CMDC health professionals who regularly use the DMI (doctors, nurses, laboratory technicians and imaging technicians) and another was intended for administrators of the said software. A total of 64 people participated in the survey, including 59 users and 05 administrators of the DMI.

Results. Data reported about accessing, retaining or sharing patient data on the DMI suggests a low level of protection.

Conclusion. The sensitive nature of patient data requires the CMDC and other healthcare establishments to improve the practices of their staff using the computerized medical record with a view to optimal security in the recording, processing and conservation of information whose nature is a matter of medical confidentiality.

Keywords : *Medical record, paper medical record, computerized medical record, patient data.*

Introduction

Le dossier médical désigne un ensemble comprenant en gros deux parties, l'une administrative et l'autre médicale. La première est un recueil des données personnelles du patient relatives à son identité : noms, sexe, âge, adresse physique, contacts, statut marital, etc. La seconde partie comprend les informations recueillies par les prestataires des soins (médecins, infirmiers, nutritionnistes, anesthésistes, psychologues cliniciens, physiothérapeutes, etc.) ; données qui se rapportent aux consultations, aux diagnostics, aux explorations, aux différents traitements et aux suivis.

L'article 33 de la Loi n° 18/035 du 13 décembre 2018 fixant les principes fondamentaux relatifs à l'organisation de la Santé Publique en République Démocratique du Congo précise même le contenu du dossier médical : « (…) toutes les pièces concernant le patient, notamment l'anamnèse, le résultat de l'examen clinique, des analyses effectuées, l'évolution de la situation du patient, les soins proposés et ceux effectivement administrés, avec l'indication de l'auteur et de la date de chaque inscription» [1].

Outre ce contenu, la loi française du 4 mars 2002 relative aux droits des malades y ajoute également « tous les échanges écrits entre les professionnels de santé» [2].

L'importance du dossier médical est tel que la loi congolaise précitée dispose même à l'article 32 que tout professionnel de santé pratiquant à titre dépendant ou indépendant doit en tenir un pour chaque patient [1]. Par ailleurs, aussi longtemps qu'ils présentent un intérêt pour la santé du patient, les éléments constitutifs de son dossier doivent être conservés pendant au moins dix ans à dater de l'ouverture du dossier [1].

Le passage du dossier médical papier à celui informatisé tend à se généraliser dans l'environnement hospitalier de Lubumbashi, en particulier au sein des établissements des soins privés. L'adoption du Dossier Médical Informatisé (DMI), encore désigné Dossier Médical Electronique(DME) découle des avantages qu'il présente par rapport à son pendant papier ; en l'occurrence, la réduction considérable du volume de stockage des dossiers patients, la facilité d'accès et du transfert des données par le biais des réseaux de l'information (comme Internet par exemple) du fait de leur dématérialisation, la facilitation de la coordination des soins entre les différents professionnels de santé ou encore une meilleure lisibilité des informations.

Les données personnelles du patient, autrement appelées données de santé ou encore données patient, désignent des « données individualisées recueillies auprès des professionnels de santé et relatives à leurs prescriptions et à leurs pratiques médicales.» [3]. Elles ont un caractère confidentiel et leur traitement, en particulier leur communication à autrui, est régie par les dispositions du Code pénal relatives au secret professionnel [1]. En effet, du fait de leur qualité sensible, ces données « sont protégées par le secret médical. « Dès qu'elles sont collectées et stockées, ces informations font l'objet d'une protection

https://doi.org/10.62126/zqrx.2022611

particulièrement sécurisée, qui malheureusement n'est pas sans faille » [3].
Le législateur congolais a, dans le souci de garantir une protection de ces données après la cessation d'activités d'un établissement ou d'un prestataire indépendant, prévu que « Le professionnel de santé qui cesse son activité en informe ses patients. Il remet leurs dossiers à son successeur. En cas d'indisponibilité ou d'incapacité permanente avérée ou de décès du professionnel de santé, les dossiers qu'il détient sont placés sous la responsabilité de la direction de l'établissement ou l'institution de santé qui l'emploie. Les dossiers des patients sont transmis au bureau central de la zone de santé en cas de fermeture de l'établissement ou l'institution de santé » [1].
Les données personnelles du dossier médical papier sont relativement faciles à sécuriser du fait de la matérialité de leur support. En revanche, avec l'avènement du DMI « la dématérialisation des données patient modifie le rapport à l'information médicale. Ces données sensibles, hétérogènes et multidomaines deviennent à présent massives (notion de bigdata) et potentiellement accessibles de façon ubiquitaire » [4].
Comment, dès lors, dans un tel contexte de risque lié au DMI, profiter de manière optimale des avantages qu'offre l'informatisation, tout en assurant et en garantissant la protection des données individuelles des patients ?
La visée de cette étude était de recueillir des informations relatives à la sécurité des données personnelles du patient contenues dans le DMI en vue de déterminer si leur protection était assurée de manière optimale ou s'il y avait une marge de progression à réaliser par l'institution afin de la rendre plus sûre.

Méthodes

Nous avons réalisé une étude descriptive du 31 juillet 2020 au 14 août 2020 au Centre Médical Du Centre ville (C.M.D.C.), Lubumbashi-RD Congo.

L'étude a consisté en un questionnaire fermé et écrit élaboré sur la base des standards internationaux de sécurité informatique, en l'occurrence le prescrit du Mémento de sécurité informatique pour les professionnels de santé en exercice libéral Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) [5].

Sur base d'une participation volontaire, une partie de ce questionnaire a été administrée aux différents professionnels de santé du CMDC utilisant régulièrement le DMI (médecins, infirmiers, techniciens de laboratoire et techniciens d'imagerie) et une autre était destinée aux administrateurs du dit logiciel.

Ont été exclus, les utilisateurs non impliqués directement dans les soins de santé et dans la gestion du logiciel DMI.

Au total 64 personnes ont participé à l'enquête dont 59 utilisateurs et 05 administrateurs du DMI.

Le premier groupe comprenait 39 infirmiers (66,11%), 10 techniciens de laboratoire (16,95%), 8 médecins (13,56%) et 02 techniciens d'imagerie (3,39%). 64% étaient de sexe féminin contre 36% de sexe masculin. L'âge moyen dans ce groupe était de 37,5 ans pour un écart-type de 6,7.

Le second groupe était constitué de 5 informaticiens, tous de sexe masculin. L'âge moyen y est de 36,4 ans pour un écart-type de 6,0.

Les données recueillies ont été saisies à l'aide du logiciel Excel. L'analyse et l'interprétation ont utilisé le calcul de la proportion.

Résultats

98,31% des professionnels de santé interrogés disent utiliser un ordinateur collectif contre 1,69% disposant d'un ordinateur personnel.

18,64% d'utilisateurs disent accéder à l'ordinateur à l'aide d'un mot de passe.

Tous les utilisateurs du DMI disposent d'un mot de passe personnel leur permettant d'accéder à leur compte.

Les mots de passe de 47,46% d'utilisateurs sont une combinaison de caractères alphanumériques (chiffres et lettres) et de caractères spéciaux.

Les mots de passe de 91,53% d'utilisateurs du DMI ont moins de 8 caractères contre ceux de 8,47% qui en ont davantage.

Pour tous les utilisateurs, aucun changement périodique de mot de passe n'a été opéré au cours de six derniers mois voire davantage.
15,25% d'utilisateurs du DMI utilisent un même mot de passe pour toutes les autres applications auxquelles ils accèdent (E-mail, session, logiciel de gestion….) contre 84,75% qui ont un mot de passe différent.
Environ 4 utilisateurs de DMI sur 10 (44,07%) incluent dans leurs mots de passe des données personnelles tel le nom d'un proche ou une date de naissance.

https://doi.org/10.62126/zqrx.2022611

13,56% d'utilisateurs du DMI notent leurs mots de passe sur un support pour pouvoir se les rappeler au moment de s'en servir.
76,27% d'utilisateurs de DMI rapportent que leurs ordinateurs se mettent en mode veille lorsqu'ils restent inutilisés après un certain temps. 37,78% d'entre eux doivent rentrer à nouveau un mot de passe pour pouvoir accéder à leurs données patients. 62,22% d'utilisateurs n'ont pas besoin de mot de passe pour accéder à leurs ordinateurs après une phase de veille.
13,56% utilisateurs du DMI ont reconnu avoir réutilisé des anciens mots de passe.
35,59% d'utilisateurs disent avoir recours à l'approche mnémotechnique pour se souvenir de leurs mots de passe sans jamais les inscrire sur un support accessible par un tiers.
Lorsque le navigateur internet leur propose la mémorisation de leurs mots de passe, environ un utilisateur de DMI sur deux (49,15%) refuse systématiquement.
Pour 88,14% d'utilisateurs de DMI, l'accès aux données de santé de patients est limité aux stricts besoins liés à leur prise en charge. 11,86% d'utilisateurs ont en sus des besoins liés à la prise en charge des patients, d'autres motivations.
Pour 91,53% d'utilisateurs, l'échange des données de santé entre professionnels de santé se fait exclusivement avec ceux devant intervenir dans la prise en charge des patients.
45,76% d'utilisateurs de DMI sont d'avis que leurs équipements informatiques sont placés en un endroit difficile d'accès pour le public (patients et accompagnants) contre 54,24% qui ont une opinion contraire.
Tous les utilisateurs du DMI reconnaissent qu'il n'existe aucun dispositif de verrouillage automatique du compte après trois essais de mots de passe infructueux.
Pour 50,85% d'utilisateurs de DMI, l'antivirus sur leur poste de travail n'est pas régulièrement mis à jour.
Tous les administrateurs du DMI sont unanimes à reconnaitre qu'aucun tiers, en l'occurrence le fournisseur de leur logiciel, ne dispose d'accès aisé aux données de patients.
Pour 60% d'administrateurs, tous les accès d'utilisateurs aux données patient ne sont pas retracés.
60% d'administrateurs affirment qu'ils font des sauvegardes régulières des données concernant les patients sur un support autre que le disque dur de leur ordinateur (serveur).
Pour ceux qui affirment faire des sauvegardes périodiques, 33,33% disent utiliser des clefs USB comme support de sauvegardes tandis que 66,67% évoquent un ordinateur autre que le serveur hébergeant le DMI.
66,67% d'administrateurs disant effectuer les sauvegardes reconnaissent que les supports de sauvegarde ne sont pas conservés en lieu sûr (coffre fort ou armoire fermant à clé) contre 33,33% qui affirment le contraire.
A la question de savoir si les administrateurs effectuent des essais de restauration des données sauvegardées pour vérifier leur validité, 66,67% de ceux qui disaient faire des sauvegardes répondent par l'affirmative contre 33,33% qui ne reconnaissent pas cette pratique.
Aucun administrateur ne reconnait avoir déjà eu à faire à une perte des sauvegardes contenant des données patients informatisées.
Pour la totalité des administrateurs, aucun compte utilisateur n'a le même droit d'accès que le compte administrateur.
Tous affirment également qu'aucun compte administrateur n'a le même mot de passe que le compte utilisateur.
40% des administrateurs estiment que le mot de passe du compte administrateur n'est pas consigné. Pour les administrateurs ayant affirmé que le mot de passe du compte administrateur était consigné, seuls 33,33% estiment que la feuille sur laquelle il est consigné se trouve gardée en un endroit sûr (coffre fort par exemple ou une armoire fermant à clé).
80% d'administrateurs affirment qu'en cas de cessation d'activités de la part d'un administrateur, son successeur a la possibilité de modifier le mot de passe.
Ils sont également 80% à affirmer qu'en cas d'absence prolongée ou de départ d'un utilisateur (agent), son compte DMI est désactivé.
60% d'administrateurs affirment que les postes de travail des utilisateurs disposent de pare – feu. 100% de ceux-ci estiment même que ce pare-feu est mis à jour.
Tous les administrateurs affirment que les logiciels utilisés sont des originaux.
60% d'administrateurs affirment qu'il leur arrive d'utiliser simultanément une double connexion filaire et Wifi au réseau.

Discussion

Le caractère sensible des données patient impose aux établissements des soins de santé de disposer d'une sécurité optimale dans l'enregistrement, le traitement et la conservation des informations dont la nature relève du secret médical. Et comme l'écrit Stéphane de Saint Albin, « Les hôpitaux " intelligents"» c'est-à-dire ceux utilisant le numérique, sont attrayants pour les pirates informatiques et les incidents de sécurité sont en constante augmentation. Le secteur de la Santé est reconnu comme étant le plus vulnérable aux cyber

https://doi.org/10.62126/zqrx.2022611

attaques, en raison de la grande valeur de ses données sensibles. Il est la cible idéale des attaques par ransomware ou « logiciels de rançon ». Le secteur doit être mieux armé pour détecter rapidement les cyber attaques et les déjouer» [6].

La quasi-totalité des ordinateurs utilisés au CMDC est collective, avec plusieurs utilisateurs se relayant sur une même machine. C'est ce qui explique, en partie, le faible taux des machines accessibles par mot de passe (18.64%).

Pour l'accès au DMI en revanche, chaque utilisateur dispose de son propre compte et de son propre mot de passe ce qui évite l'accès à des données patient au travers d'un compte d'un utilisateur tiers. Les administrateurs du DMI affirment d'ailleurs qu'aucun compte utilisateur n'a le même droit d'accès que le compte administrateur et qu'aucun compte administrateur n'a le même mot de passe que le compte utilisateur.

Dans une étude similaire BRAMI Grégory [7] a trouvé que 66% des médecins utilisant le DMI avaient un mot de passe pour accéder à leur ordinateur et seulement 79% pour leur logiciel de données patients.

Pour accéder à leurs comptes de données patient, 52,54% d'utilisateurs du CMDC avaient des mots de passe n'ayant pas une combinaison de caractères alphanumériques et de caractères spéciaux. Et seulement 8,47% d'utilisateurs possédaient des mots de passe ayant au moins 8 caractères. Dans l'étude de Bramy, 54% de mots de passe n'utilisaient pas de caractères alphanumériques et 81% n'utilisaient pas plus de 8 caractères.

Le changement régulier de son mot de passe est réputée une pratique apte à contribuer à sa robustesse. Dans notre étude, aucun utilisateur n'a changé son mot de passe au cours de six derniers mois au moins précédant l'enquête. Ces données sont très proches de celles de Bramy, pour qui 96% d'utilisateurs n'avaient jamais changé leurs mots de passe [7].

Environ 4 utilisateurs de DMI sur 10 (44,07%) incluent dans leurs mots de passe des données personnelles tel le nom d'un proche ou une date de naissance. Ils étaient 26% dans l'étude précitée [7]. Cette pratique rend le mot facile à deviner par un tiers qui pourrait ainsi accéder aux données patient.

Avec 13,56% d'utilisateurs du DMI notent leurs mots de passe sur un support pour pouvoir se les rappeler au moment de s'en servir. Ces données sont un peu plus élevées que celles observées par Bramy et qui étaient de 8%. On pourrait penser que la proportion restante soit 86,44%, a recours à l'approche mnémotechnique pour se souvenir du mot de passe. Pourtant les données ne rapportent que 35,59% d'utilisateurs y ayant recours, ce qui laisse penser qu'il y aurait en réalité davantage d'utilisateurs notant leurs mots de passe sur un support. Avec une telle pratique, il est à craindre qu'un utilisateur tiers puisse retrouver le mot de passe et accéder aux données patient.

15,25% d'utilisateurs du DMI utilisent le même mot de passe pour toutes les applications, une proportion moins élevée que chez Bramy qui est de 45% [7].

Les données rapportées ci-dessus au sujet de la composition et de l'usage du mot de passe dans la gestion des données patient du DMI suggèrent un faible niveau de sécurité. Et pourtant l'utilisation et l'élaboration d'un mot de passe sont des étapes primordiales dans la protection des données informatiques [7]. Pour protéger les données, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne [8]. En vue d'obtenir de mots des passe disposant d'une robustesse appropriée, il est recommandé de:

- fixer à au moins 8 caractères, la longueur du mot de passe et éviter qu'il soit prédictible;
- imposer la combinaison de caractères alphanumériques et de caractères spéciaux ;
- procéder au renouvellement périodique de vos mots de passe (tous les trois mois) :
- interdire la réutilisation des 3 mots de passe précédents ;
- interdire un mot de passe identique au nom du compte ;
- adopter une approche mnémotechnique pour vous souvenir de vos mots de passe, sans jamais les inscrire sur un support accessible par un tiers ;t
- refuser systématiquement la mémorisation de vos mots de passe lorsqu'elle vous est suggérée par votre navigateur Internet [8].
- ne jamais demander à un tiers de créer pour vous un mot de passe ;
- ne pas stocker pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
- ne pas vous envoyer vos propres mots de passe sur votre messagerie personnelle [8].

https://doi.org/10.62126/zqrx.2022611

Si l'on veut une protection optimale, tous les ordinateurs devraient disposer d'un écran de veille et tous devraient être configurés de telle sorte qu'il faille un mot de passe pour le désactiver. Au CMDC, 76,27% d'utilisateurs de DMI rapportent que leurs ordinateurs se mettent en mode veille lorsqu'ils restent inutilisés après un certain temps. Mais seulement 37,78% d'entre eux doivent rentrer à nouveau un mot de passe pour pouvoir accéder à leurs données patient. Dans l'étude de Bramy, 73% d'utilisateurs interrogés disposaient d'un écran de veille et seuls 19% parmi eux utilisaient un mot de passe pour le désactiver.

L'absence d'un dispositif de verrouillage automatique du compte après trois essais de mots de passe infructueux a été rapportée par tous les utilisateurs du DMI, ce qui accroit le risque d'intrusion malveillante d'utilisateurs non autorisés et l'accès à des données patients. Il est possible de mettre manuellement en veille son poste de travail lorsque on s'en éloigne (par exemple sous Windows, le raccourci clavier pour ce faire est le suivant: Touche Windows + L) [7].

L'accès aux données de santé de patients est limité aux stricts besoins liés à leur prise en charge pour 88,14% d'utilisateurs de DMI. 11,86% d'utilisateurs ont en sus, d'autres motivations qui n'ont pu être clairement mises en évidence.

Pour 91,53% d'utilisateurs, l'échange des données de santé entre professionnels de santé se fait exclusivement avec ceux devant intervenir dans la prise en charge des patients. L'entretien directif avec des utilisateurs a permis de noter que des données patient étaient parfois communiquées, à leur demande, aux services en charge de la facturation lors d'établissement des factures pro forma.

L'échange de données de santé entre professionnels de santé doit être subordonné à deux conditions cumulatives à savoir:

- les professionnels de santé doivent tous intervenir dans la prise en charge du patient dont les données de santé sont échangées et
- cet échange doit être limité aux données utiles pour la continuité des soins ou la détermination de la meilleure prise en charge sanitaire du patient [8].

54,24% d'utilisateurs de DMI sont d'avis que leurs équipements informatiques sont placés en un endroit facile d'accès pour le public (patients et accompagnants). Des regards indiscrets pourraient ainsi lire sur les écrans allumés, des données patients. Et plus d'une fois, des équipements informatiques amovibles, en l'occurrence des lap top, ont été volés, alimentant de facto le marché noir des nouvelles technologies (tablettes, ordinateurs portables, téléphones, …) et contribuer aussi à « des faits d'exploitation frauduleuse des données de santé à caractère personnel qu'ils contiennent, par exemple pour alimenter des campagnes ciblées de courriers électroniques de vente de médicaments d'origine douteuse » [7].

Autant que possible, les équipements informatiques doivent être dans un lieu difficile d'accès par le public (patients, accompagnants, visiteurs, …) et ceux qui ne sont pas sous surveillance directe doivent bénéficier des mesures adéquates de protection physique en l'occurrence une protection renforcée des ouvertures permettant l'accès au lieu d'exercice (portes et fenêtres) et si possible, mettre en place un système d'alarme voire une caméra de surveillance. Les équipements amovibles tels les lap top et autres tablettes, peuvent être protégés à l'aide d'un câble antivol et d'autres comme les CD, les disques durs externes ou les clés USB ; être placés dans un coffre ou une armoire fermant à clé.

L'intégrité des données patients face aux attaques virales mérite une attention particulière lorsqu'on sait que seuls 49,15% d'utilisateurs de DMI estiment que l'antivirus sur leur poste de travail est régulièrement mis à jour. Parmi les utilisateurs de chez Bramy, 80% faisaient des mises à jour régulières de leur logiciel anti-virus.

Outre les anti-virus, le pare-feu est un logiciel qui protège également les données d'un ordinateur contre des logiciels espions. Au CMDC, 60% d'administrateurs du DMI interrogés ont affirmé que les postes de travail des utilisateurs disposaient de pare – feu et même qu'il était mis à jour.

Le traçage numérique désigne les informations qu'un dispositif numérique enregistre sur l'activité ou l'identité de ses utilisateurs au moyen de traceurs tels que les cookies, soit automatiquement, soit par le biais d'un dépôt intentionnel. Le traçage permet d'identifier la personne ayant accédé aux données patient et de vérifier à postériori les motivations de l'utilisateur. 60% d'administrateurs du DMI du CMDC ont reconnu que les accès aux données patient n'étaient pas tracés. Même parmi ceux ayant affirmé le contraire, 50% ont reconnu que le traçage n'était possible qu'à condition que l'utilisateur ait modifié des données. Sans traçage adéquat des utilisateurs à des informations aussi sensibles que les données patient, il est à craindre pour leur intégrité.

https://doi.org/10.62126/zqrx.2022611

Face au risque des pertes des données, la sauvegarde se révèle être une pratique essentielle à la restauration des données patients. Au CMDC, 60% d'administrateurs du DMI interrogés ont affirmé que cette pratique était régulière. 33,33% d'entre eux citent des clefs USB comme support de sauvegardes tandis que 66,67% évoquent un ordinateur autre que le serveur hébergeant le DMI. Par ailleurs 66,67% d'administrateurs disant effectuer les sauvegardes ont admis que les supports de sauvegarde n'étaient pas conservés en lieu sûr (coffre fort ou armoire fermant à clé).

De l'avis de 66,67% d'administrateurs, les essais de restauration des données sauvegardées pour vérifier leur validité s'effectuent régulièrement. Ceux qui admettent le contraire citent comme obstacle le fait que les sauvegardes se font sur un serveur de recours, ayant le même IP que le serveur central, cette opération ne peut se faire car il y a risque de conflit. Dans l'étude de Bramy, il a observé que « même si 85% des généralistes interrogés font régulièrement des sauvegardes de leurs données, 53% n'en ont jamais testé la validité. »

Même si aucune perte des sauvegardes contenant des données patient informatisées n'a été rapportée par les administrateurs du DMI, assurer une sauvegarde régulière de données (mensuelle par exemple), demeure une nécessité. Et pour être optimale, il importe d'observer certaines règles :

- Une fois que la sauvegarde est effectuée, il faut en conserver le support dans un lieu sûr et éloigné de l'ordinateur.
- Vérifier périodiquement (chaque trimestre par exemple) la (validité) lisibilité des données sauvegardées au moyen des tests de restauration.
- Il est préférable que les sauvegardes soient gardées dans un format non chiffré.

La consignation du mot de passe du compte administrateur est indispensable car en cas d'empêchement de celui qui le détient, on peut y accéder en cas de besoin. Mais la feuille sur laquelle il se trouve enregistré doit pouvoir être gardée dans un endroit sûr. Au CMDC, 40% des administrateurs estiment que le mot de passe du compte administrateur n'est pas consigné. En revanche, pour ceux qui affirment le contraire, seuls 33,33% d'entre eux admettent que la feuille sur laquelle le mot de passe est consigné se trouve gardée en un endroit sûr (coffre fort par exemple ou une armoire fermant à clé).

Un administrateur qui cesse ses activités ne devrait plus conserver son mot de passe et en cas d'absence prolongée, son compte devrait être désactivé. Interrogés sur cette possibilité, les administrateurs du DMI ont reconnu à 80% qu'en cas de cessation d'activités de la part d'un administrateur, son successeur avait la possibilité de modifier le mot de passe et qu' cas d'absence prolongée ou de départ d'un utilisateur (agent), son compte DMI était désactivé.

L'usage des copies en lieu et place des logiciels originaux peut être une tentation étant le coût relativement élevé de ces derniers. Malheureusement, cela ne va pas sans risques. Il y a d'abord des risques juridiques, l'usage d'une copie illicite de logiciels étant du piratage ; un acte répréhensible et punissable par la loi. Il y a aussi des risques techniques dans la mesure où l''utilisation d'une copie illicite d'un logiciel ne permet pas de bénéficier des mises à jour et du support technique du produit qui sont indispensables pour la sécurité des logiciels. Par ailleurs « les logiciels « crackés » téléchargeables sur Internet peuvent contenir des virus ou des Troyens » [9].

L'utilisation simultanée d'une double connexion filaire et Wifi au réseau est une pratique courante au CMDC à en croire 60% d'administrateurs du DMI. Elle constitue cependant un risque pour l'intégrité des données. Il est préférable d'utiliser l'une ou l'autre forme de connexion et non les deux simultanément.

Conclusion

Depuis 3 ans, le CMDC est entrain d'expérimenter le dossier médical informatisé (DMI). A l'instar d'autres établissements des soins qui lui ont emboité le pas, ce choix se justifie entre autre par les avantages qu'offre ce type de dossier :

- les professionnels de santé disposent d'un accès direct et immédiat à des informations pertinentes relatives au patient ;
- il est un instrument de travail et d'échanges entre les différents membres de l'équipe soignante ;
- il améliore la coordination entre les professionnels de santé et offre un meilleur partage de l'information nécessaire à la prise en charge du patient ; [10]
- il permet la sécurité et la confidentialité des données patient grâce aux droits d'accès restreints des utilisateurs ;
- il est un outil qui permet au patient de jouir de son droit à l'information, étant entendu que la loi lui reconnait le droit « d'obtenir, à sa demande, un résumé écrit des informations relatives à sa santé.» ; [1]
- le DMI possède en plus un avantage certain lié à sa capacité accrue de stockage (archivage) bien supérieure à celle du dossier papier.

https://doi.org/10.62126/zqrx.2022611

En dépit de ces avantages, le DMI présente des faiblesses liées au risque des pertes ou d'usurpation des données qui sont réputées sensibles car relevant du secret médical.

Dans des environnements aussi complexes que les milieux des soins, l'élaboration et l'appropriation d'un document de politique reprenant les procédures et les bonnes pratiques se révèle être une démarche salutaire pour améliorer ses services [11]. Depuis avril 2018, le CMDC dispose d'un règlement sur l'usage du matériel informatique qui édicte une série des mesures de sécurité devant être observées par les différents utilisateurs d'équipements informatiques. Ce support insiste quasi exclusivement sur la sécurité physique du matériel informatique, celle des données patient, y est, en revanche, à peine effleurée. Au regard des résultats de la présente étude et des standards en la matière, il existe un gap qui mérite d'être comblé pour élever le niveau de sécurité des donnés patient qui sont enregistrées via le DMI.

Conflits d'intérêt : Aucun.

Qu'est ce qui est connu sur ce sujet

- Le DMI est apprécié pour sa facilité de gestion des patients par l'ensemble des intervenants.
- Il faut cependant constater que l'immatérialité des données individuelles des patients les rend vulnérables face à l'intrusion des tierces personnes.

Qu'est-ce que votre étude apporte de nouveau

- Notre étude permet de relever que les pratiques, procédures et attitudes observées dans le chef des utilisateurs et des administrateurs du DMI au Centre médical Du Centre - ville ne permettent pas d'assurer une protection optimale des données patient.
- Cet état de lieu rend primordial rend primordiale la nécessité d'améliorer les pratiques, procédures et attitudes des différents utilisateurs du DMI afin d'optimiser la sécurité des données individuelles des patients.
- Ces recommandations valent aussi pour les autres établissements des soins ayant recours au dossier médical informatisé.

Contributions des auteurs

Frank Nduu Nawej a conçu l'étude, rédigé le manuscrit et élaboré le projet du questionnaire d'enquête. Fulgence Mbayo Ilunga, Pascal Nawej Tshimwang Junior et Romain Ngoy Shindano ont validé le questionnaire d'enquête. Didier Kapinga, Joseph Pyana Kitenge et Henri Mundongo ont analysé les données. Pascal Nawej Tshimwang sénior a encadré l'équipe. Tous les auteurs ont lu et approuvé la version finale du manuscrit.

Remerciements

Les auteurs remercient les autorités et le personnel du CMDC de Lubumbashi pour leur disponibilité.

Références

1. Journal Officiel de la République Démocratique du Congo. Loi n° 18/035 du 13 décembre 2018 fixant les principes fondamentaux relatifs à l'organisation de la Santé Publique. Numéro spécial de la 59ième année. 2018. Kinshasa. Disponible sur : http://extwprlegs1.fao.org/docs/pdf/Cng190586.pdf et consulté le 20 décembre 2019.
2. Légifrance. Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Disponible sur : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000227015 et consulté le 20 décembre 2019.
3. de la Grange P, Lajugie V. Sécurisation des données de santé, protection des droits des patients. 2016. Disponible sur http://www.gf-avocats.com/securisation-des-donnees-de-sante-protection-des-droits-des-patients-_r_30_a_5.html et consulté le 20 décembre 2019.
4. Riou C, Cuggia M. Protection des données de santé lors de leur réutilisation à des fins de recherche au sein des entrepôts de données biomédicaux (EDBM). 15èmes Journées francophones d'informatique médicale (JFIM). 2014. Disponible sur : http://ceur-ws.org/Vol-1379/paper-14.pdf et consulté le 20 décembre 2019.
5. ASIP Santé/DSSIS. Mémento de sécurité informatique pour les professionnels de santé en exercice libéral. 2013. Disponible sur https://www.ordremk.fr/wp-content/uploads/2014/02/Memento_Securite.pdf et consulté le 10 janvier 2020.
6. de Saint Albin S. Hôpitaux intelligents : le défi de la sécurité informatique. Disponible sur :

https://doi.org/10.62126/zqrx.2022611

https://www.maddyness.com/2020/07/01/hopitaux-intelligents-defi-securite-informatique/ et consulté le 02 juillet 2020.

7. Brami G. Protection des données patients informatisées en médecine générale. Thèse pour le Doctorat en Médecine. Faculté de Médecine Université Paris 7. 2007. Disponible sur : http://www.bichat-larib.com/publications.documents/3331-BRAMI-Gregory-THESE.pdf et consulté le 10 janvier 2020.
8. Agence nationale de la sécurité des systèmes d'information. Note technique. Recommandations de sécurité relatives aux mots de passe. 2012. Disponible sur https://www.ssi.gouv.fr/guide/mot-de-passe/ et consulté le 25 août 2020.
9. Conseil informatique. Pourquoi il ne faut jamais utiliser des logiciels piratés ? Disponible sur : http://www.conseil-informatique.com/voici-pourquoi-il-ne-faut-jamais-utiliser-des-logiciels-pirates/ et consulté le 19 septembre 2020.
10. Gonnetan C. Avantages et inconvénients du Dossier Médical Informatisé dans le cadre de l'odontologie médico-légale. Thèse pour le diplôme d'état de docteur en Chirurgie dentaire. 2017. Nantes. Université de Nantes.
11. Nduu F. Politique de qualité santé. Guide pratique à l'intention des établissements des soins de santé - 2ème édition augmentée. 2020. Lubumbashi. Editions Talenta.

https://doi.org/10.62126/zqrx.2022611