RMOS

Publié le 22/06/2025

Article original / Original article

Revue Méditerranéenne d'Odonto - Stomatologie

« Gestion numérique des services de santé bucco-dentaire en Tunisie : enjeux et considérations éthiques »

«Digital management of oral health services in Tunisia: issues and ethical considerations»

Sarra Nasri [1,2], Khaoula Sliti[3], Rim Kallala[1,2], Sihem Hajjaji[1,4], Zohra Nouira[1,2], Jilani Saafi[1,2], Belhassen Harzallah[1,2], Mounir Cherif[1,2]

1- Department of Fixed Prosthodontics, Faculty of Dental Medicine of Monastir, Tunisia
2- University of Monastir, Faculty of dental Medecine, ,Research Laboratory of Occlusodontics and Ceramic Prostheses LR16ES15, 5000, Monastir, Tunisia
3- Doctor of Dental Medecine and Public Health consultant, 1000,Tunis, Tunisia
4- University of Sousse, Research Laboratory: LR 12SP10: Functional and Aesthetic Rehabilitation of Maxillary,Tunisia

Résumé :
Les systèmes de santé font l'objet de réformes et de modernisations dans de nombreux pays, et la question de la numérisation occupe une place prépondérante dans les politiques publiques, les plans nationaux stratégiques et les travaux de recherche.
En explorant les perspectives d'évolution et de contribution de la technologie dans le domaine de la dentisterie surtout grâce à des technologies facilitatrices telles que l'intelligence artificielle et le machine learning etc… il devient évident que la gestion numérique des services de santé bucco-dentaire est un prérequis essentiel. Sa mise en œuvre réussie devient une condition sine qua non pour pouvoir suivre le rythme de l'évolution technologique, favoriser le développement et améliorer la qualité des services.
Mots-clés : digitalisation, système de santé, santé bucco-dentaire, santé publique, management, éthique

Abstract
Health systems across many countries are undergoing reforms and modernization, with digitization playing a central role in public policies, national strategic plans, and research efforts. Exploring the evolving perspectives and contributions of technology in the field of dentistry, particularly through enabling technologies such as artificial intelligence and machine learning, highlights the necessity of digital management in oral health services. Effective implementation of these digital solutions is a prerequisite to keeping pace with technological advancements, fostering development, and enhancing the quality of services.
Keywords: digitalization, health system, oral health, public health, management, ethics

« Gestion numérique des services de santé bucco-dentaire en Tunisie : enjeux et considérations éthiques »

Sarra Nasri [1,2], Khaoula Sliti[3], Rim Kallala[1,2], Sihem Hajjaji[1,4], Zohra Nouira[1,2], Jilani Saafi[1,2], Belhassen Harzallah[1,2], Mounir Cherif[1,2]

E-mail adress : Sarra.Nasri@fmdm.u-monastir.tn

nssarra@gmail.com

ORCID ID: https://orcid.org/my-orcid?orcid=0000-0001-6740-6644

Introduction:

La santé numérique est devenue un axe stratégique majeur du Plan National Stratégique de « la Tunisie Digitale 2020 », soutenant ainsi l'ambition de réforme du système de santé. (1)

Le Ministère de la Santé en Tunisie a mis en place plusieurs programmes stratégiques de soutien au développement de la santé numérique. Ces programmes comprennent notamment la mise à niveau des systèmes d'information hospitaliers, la numérisation des systèmes de gestion et d'administration des établissements de santé, la sécurisation du circuit du médicament, la numérisation des archives médicales, le développement des télé-services et des approches territoriales de l'e-santé. (2)

Outre les difficultés logistiques et budgétaires, peu d'articles se concentrent sur les défis que rencontrent les établissements relatifs à la gestion du changement et le rôle des leaders de ce domaine ainsi que les enjeux éthiques qui se lèvent avec ce Aussi, la gestion numérique des services de santé bucco-dentaire, reste un domaine peu exploré dans le contexte de la digitalisation et du déploiement de l'e-santé.

A travers cette revue, on cherche à fournir des réponses en abordant à la fois les prérequis à un tel changement et les enjeux éthiques qui lui sont associés.

1- Le DES au cœur de la mutation numérique : défis logistiques et budgétaires

La mise en place de DES (Dossier de santé électronique) représente un véritable défi pour les organisations de soins de santé, car elle peut entraîner des pertes de ressources, des frustrations chez les professionnels de santé, un manque de confiance chez les patients et des risques en matière de sécurité des patients.

Pour élaborer, mettre en œuvre et maintenir l'utilisation des DSE, il est indispensable de disposer de fonds suffisants et de mobiliser une multitude de personnes, notamment des cliniciens, des informaticiens, des éducateurs et des consultants (3).

Des défis relatifs aux budgets alloués à l'implémentation des systèmes de DSE ont été rapportés. Il ne suffit pas de prévoir le budget nécessaire à l'achat et à la mise en place des DSE. Des exigences budgétaires doivent être considérées et qui doivent inclure des budgets pour planification des achats et mises à jour futures

de logiciels, le temps du personnel et des coûts supplémentaires pour les déplacements aux conférences des fournisseurs, les coûts des formations... etc (4).

2- *Les enjeux éthiques de la mise en œuvre des DSE et législation en Tunisie :*

- *Confidentialité :*

Il est impératif de respecter la confidentialité des informations d'un patient en ne les communiquant à des tiers qu'avec son autorisation ou si la loi l'autorise. Dans le cas où le patient est dans l'incapacité de donner son consentement en raison de son âge ou d'une incapacité mentale, les décisions concernant le partage d'informations doivent être prises par son tuteur légal. Les informations échangées lors d'une interaction clinique sont considérées comme confidentielles et doivent être protégées (5).

Afin de garantir le bon fonctionnement des DSE, il est essentiel que les établissements de santé, les compagnies d'assurance et d'autres entités aient accès aux données nécessaires.

Cependant, il est primordial de préserver la confidentialité des informations en ne permettant l'accès qu'aux individus autorisés, ce qui requiert une autorisation des utilisateurs.

Les privilèges d'accès des utilisateurs sont déterminés en fonction de leur rôle et l'administrateur doit identifier l'utilisateur, déterminer le niveau d'information à partager et attribuer des noms d'utilisateurs et des mots de passe. Il est important que les utilisateurs soient conscients de leur responsabilité quant à l'utilisation et la mauvaise utilisation des informations consultées, tout en ayant accès aux informations nécessaires pour remplir leurs tâches. En somme, l'attribution des privilèges d'utilisateur est un élément clé de la sécurité des dossiers médicaux(5).

Toutefois, le simple contrôle d'accès aux informations de santé ne suffit pas à garantir la confidentialité. Des politiques de confidentialité et de sécurité solides sont indispensables pour protéger efficacement les informations des patients.

- *Failles de sécurité :*

Les failles de sécurité peuvent menacer la vie privée des patients lorsque des informations de santé confidentielles sont mises à la disposition d'autres personnes sans le consentement ou l'autorisation de l'individu.

Il est nécessaire de mettre en place des mesures de sécurité telles qu'un pare-feu qui présente un système de sécurité de réseau informatique limitant le trafic

Internet entrant et sortant à l'intérieur d'un réseau privé, des logiciels antivirus et des logiciels de détection d'intrusion, ayant pour objectifs de détecter des activités malicieuses sur la cible qu'ils surveillent.

Pour assurer la confidentialité et la vie privée des patients, il convient d'établir des politiques et des procédures spécifiques. Par exemple, les employés doivent s'abstenir de partager leur identifiant avec quiconque, se déconnecter systématiquement lorsqu'ils quittent leur poste et utiliser leur propre identifiant pour accéder aux dossiers numériques des patients (6).

Il convient aussi de désigner un responsable de la sécurité chargé de travailler avec une équipe d'experts en technologies de l'information de santé.

Afin de s'assurer que la politique de l'établissement de santé est respectée, il est nécessaire de mener des audits aléatoires régulièrement. Les audits permettent de suivre toutes les activités du système, notamment grâce à des listes détaillées de contenu, de durée et d'utilisateurs, ainsi qu'à la génération de la date et de l'heure des entrées et des journaux de toutes les modifications apportées aux DSE.

Ceci garantit une traçabilité permettant l'identification de n'importe quelle activité inhabituelle ou suspicieuse.

Dans un monde ou les données ont de plus en plus de la valeur, et tous les moyens sont permis pour collecter plus de données, les informations de santé des patients n'échappent pas à ces risques. Plusieurs accidents ont été rapportés dans ce sens. A titre d'exemple et selon des informations publiées par la FBI (Federal Bureau of Investigation, FBI est le principal service fédéral de police judiciaire et un service de renseignement intérieur aux États-Unis), une ancienne employée de l'hôpital de l'université Howard est condamnée pour avoir vendu des informations personnelles sur les patients de l'hôpital, en effet, Napper, âgée de 33 ans a plaidé coupable en juin 2012 devant le tribunal de district des États-Unis pour le district de Columbia pour avoir divulgué de manière illégale des informations de santé individuellement identifiables. Cette accusation constitue une violation de la Loi sur la portabilité et la responsabilité de l'assurance maladie. Le juge a soumis Napper à une période de probation de trois ans. (7)

D'où l'importance des lois et des cadres législatifs qui organisent et réglementent l'utilisation et l'exploitation des données des patients.

- *Inexactitude des données :*

Bien que les DSE aident à améliorer la précision et à réduire les marges d'erreurs, des préoccupations ont été soulevées concernant l'exactitude et la fiabilité des données saisies dans le dossier électronique.

Plusieurs facteurs peuvent contribuer à des situations d'inexactitude des données, dans la majorité des cas, il s'agit de problèmes de manipulation des systèmes.
Les techniques de « copier » et « coller » par exemple peuvent induire à l'erreur, bien que ceci peut sembler faciliter les tâches pour les cliniciens ou les utilisateurs du système en général, des recommandations spéciale ont été élaborées pour ne plus autoriser l'utilisation de cette technique(8). De même, des fonctionnalités telles que le menu déroulant qui permet aux utilisateurs de faire un choix parmi une liste déroulante ont été identifiées comme source d'erreurs car elles offrent un nombre de choix limité. Sous la pression du temps, les utilisateurs sont plus susceptibles de commettre des erreurs.
Des améliorations continues doivent être introduites sur le système afin d'optimiser son efficacité et de le rendre le plus « user-friendly », une expression utilisée dans le domaine de l'informatique pour désigner un système convivial et facile à utiliser.

3- *Législation relative à la protection de données en Tunisie* :

En 2002, la Tunisie est devenue le 32e pays à inscrire dans sa constitution le droit à la protection des données personnelles. Depuis lors, plusieurs lois ont été adoptées à cet effet.
Une première loi organique a été adoptée en 2004 ; la loi n°2004-63 du 27 juillet 2004 relative à la protection des données à caractère personnel, dans laquelle la création d'Instance Nationale de la Protection des Données Personnelles (INPDP) a été inscrite.
La mission de cette instance est de veiller au respect des dispositions de la loi relative à la protection des données en mettant en œuvre les moyens nécessaires à l'exercice de son mandat, tels que des manuels de procédures, des formations et des campagnes de sensibilisation (9).
Le 5 décembre 2018, l'Instance nationale de protection des données personnelles (INPDP) a adopté la délibération n°4 du 5 septembre 2018, qui concerne le traitement des données à caractère personnel liées à la santé. Cette délibération vise à renforcer et préciser les principes juridiques de la protection des données personnelles. Ce texte prend en compte les avancées technologiques et aborde notamment la question de l'Internet des objets, en particulier les dispositifs permettant le développement de pratiques médicales telles que les applications liées au mode de vie et les systèmes de consultation et de surveillance personnalisés.

En vertu de la délibération de 2018 et de la loi organique de 2004 des conditions de traitement des données de santé ont été avancées (9)

- Autorisation préalable de l'INPDP
- Charte éthique interne
- Finalité claire et légitime
- Minimisation de la collecte des données
- Information suffisante
- Consentement libre, explicite, éclairé et univoque et preuve du consentement
- Pseudonymisation ou anonymisation des données
- Sécurité des données
- Hébergeur agréé national
- Durée limitée de conservation
- Accès et portabilité des données

➢ *Le cas du Médecin dentiste et technicien de laboratoire de prothèse (prothésiste) :*

La qualité de la relation entre le médecin dentiste et le prothésiste de laboratoire de prothèse est cruciale pour obtenir des résultats satisfaisants des traitements prothétiques. Le numérique a servi l'amélioration de la communication entre le praticien et le technicien prothésiste.
Les données qui peuvent être communiquées sont :

- Photographies (extra et intra buccales) ;
- Vidéos (optionnel) ;
- Radiographie panoramique ;
- Empreintes optiques ;
- Scans du visage (optionnel) ;
- Scans CBCT (Cone beam computed tomography) ;
- Cinématique mandibulaire Modjaw ;
- Antécédents médicaux/questionnaires ;
- Formule dentaire ;
- Traçage parodontal.

En Tunisie, la pratique de médecine dentaire est organisé par la loi n° 91-21 du 13 mars 1991 relative à l'exercice et à l'organisation des professions de médecin

et médecin-dentiste et le décret n° 73-259 du 31 mai 1973 portant promulgation du code Déontologie Dentaire.

Quant à l'exercice de la profession de prothésiste dentaire, elle est organisée en pratique libérale par le cahier de charge relatif à l'exercice de la profession de prothésiste dentaire de libre pratique.

En termes d'échange de données personnelles, il n'y pas un cadre législatif en Tunisie qui règlemente ce type de trafic de données, cependant des pratiques telles que l'étiquetage des empreintes qui permettent le transfert anonyme des données sont utilisées pour réduire les risques.

L'envoi des empreintes numériques se fait en moyennant de plusieurs outils notamment les logiciels CAO. Plusieurs types de fichiers sont utilisés et leur partage avec les laboratoires de prothèse dentaire reste un défi en absence des outils numériques sécurisés et adéquats.

Le recours à des outils commerciaux et grand public de partage de fichiers est répandu (Drive, Wetransfer, dropbox.) mais ceci est en contradiction avec les conditions avancées par la loi organique de 2004 précédemment évoquée car ces pratiques impliquent le partage des données avec un tiers (la plateforme de partage et ses partenaires) et peut nuire à la sécurité des données. En absence d'alternatifs abordables et démocratisés l'anonymisation des données reste le seul moyen pour diminuer les risques. (10)

Conclusion :

La numérisation de la gestion des services de santé offre de nombreux avantages. Cependant, sa mise en place reste un défi à plusieurs niveaux.

Pour réussir cette transition, il est nécessaire de maîtriser les enjeux organisationnels, notamment la gestion du changement, afin d'assurer une acceptation et une continuité, et de prévenir les échecs ou d'en réduire l'incidence et l'ampleur.

Des défis liés à la sécurité des informations et des échanges se posent avec la numérisation et doivent être anticipés et gérés à l'aide d'outils juridiques et techniques.

Références:

1. Plan National Stratégique Tunisie Digitale 2020. Site du Ministère des technologies de la communication. 2020. https://www.mtc.gov.tn/index.php?id=14#:~:text=Le%20Plan%20National%20Strat%C3%A9gique%20%C2%AB%20Tunisie
2. Benedict M, Hannes Schlieter. Governance guidelines for digital healthcare ecosystems. PubMed. 2015 Jan 1;212:233–40.
3. Bostrom A et al., Electronic Health Record. CIN: Computers, Informatics, Nursing. 2006 Jan;24(1):44–52.
4. Harman L. Ethical Challenges in the Management of Health Information. 2001.
5. Jamshed N, Ozair FF, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. Perspectives in Clinical Research. 2018;6(2):73–6.
6. District of Columbia | District of Columbia [Internet]. www.justice.gov. 2014. Available from: https://www.justice.gov/usao-dc
7. Gelzer R, Hall T, Liette E, Reeves MG, Sundby J, Tegen A, et al. Auditing copy and paste. 2009 Jan 1;80(1):26–22.
8. nstance nationale de protection des données à caractère personnel (INPDP) - Bureau du Conseil de l'Europe à Tunis - www.coe.int [Internet]. Bureau du Conseil de l'Europe à Tunis. 2014. https://www.coe.int/fr/web/tunis/inpdp
9. Anne-Christine Lacoste, Frédérique Lesaulnier, Natalia Rusu, Sara Ben Fraj. Sensibilisation à la protection des données à caractère personnel dans le secteur de la santé 2021. Programme d'Appui aux instances indépendantes en Tunisie (PAII-T), Conseil de l'Europe et Union européenne.2021.
10. Sastre T. La dentisterie numérique tout simplement. Paris :ESPACE ID, 2021.