L'hygiène numérique en cabinet dentaire : évaluation des pratiques professionnelles

Marie Thiam Ndiaye

université de BORDEAUX

U.F.R. D'ODONTOLOGIE

Année 2024 Thèse n°82

THESE POUR L'OBTENTION DU

DIPLOME D'ETAT de DOCTEUR EN CHIRURGIE DENTAIRE

Présentée et soutenue publiquement

Par THIAM NDIAYE Marie Juliette Carla

Née le 15 novembre 1999 à Troyes, FRANCE

Le 21 octobre 2024

L'HYGIÈNE NUMÉRIQUE AU CABINET DENTAIRE

Evaluation des pratiques professionnelles

Sous la direction de : Mathilde LEVRIER

Membres du jury :

Mr NAVEAU Adrien	Professeur des Universités	Président
Mme LEVRIER Mathilde	CCU-AH	Directrice
Mr DECAUP Pierre-Hadrien	Maître de Conférence des Universités	Rapporteur
Mme ARRIVE Elise	Maître de Conférence des Universités	Assesseur

UNIVERSITE DE BORDEAUX

01/09/2024

Président	M. LEWIS Dean
Directeur de Collège des Sciences de la Santé	M. DUBUS Pierre

COLLEGE DES SCIENCES DE LA SANTE
UNITE DE FORMATION ET DE RECHERCHE DES SCIENCES

Directrice	Mme BERTRAND Caroline	58-01
Directeur Adjoint à la Pédagogie	M. DELBOS Yves	56-01
Directeur Adjoint – Chargé de la Recherche	M. CATROS Sylvain	57-01
Directeur Adjoint – Chargé des Relations Internationales	M.SEDARAT Cyril	57-01

ENSEIGNANTS DE L'UFR

PROFESSEURS DES UNIVERSITES

Mme	Caroline	BERTRAND	Prothèse dentaire	58-01
Mme	Marie-José	BOILEAU	Orthopédie dento-faciale	56-01
M.	Sylvain	CATROS	Chirugie orale	57-01
M.	Raphaël	DEVILLARD	Dentisterie restauratrice et endodontie	58-01
M.	Emmanuel	D'INCAU	Prothèse dentaire	58-01
M.	Bruno	ELLA NGUEMA	Sciences anatomiques et physiologiques - Biomatériaux	58-01
M.	Jean-Christophe	FRICAIN	Chirurgie orale	57-01
Mme	Elsa	GAROT	Odontologie pédiatrique	56-01
M.	Adrien	NAVEAU	Prothèse dentaire	58-01

MAITRES DE CONFERENCES DES UNIVERSITES

Mme	Elise	ARRIVÉ	Prévention épidémiologie – Economie de la santé – Odontologie légale	56-02
Mme	Audrey	AUSSEL	Sciences anatomiques et physiologiques	58-01
M.	Etienne	BARDINET	Orthopédie dento-faciale	56-01
M.	Michel	BARTALA	Prothèse dentaire	58-01
M.	Cédric	BAZERT	Orthopédie dento-faciale	56-01
M.	Christophe	BOU	Prévention épidémiologie – Economie de la santé – Odontologie légale	56-02
M.	Jacques	COLAT PARROS	Sciences anatomiques et physiologiques	58-01
M,	Jean-Christophe	COUTANT	Sciences anatomiques et physiologiques	58-01
M.	François	DARQUE	Orthopédie dento-faciale	56-01
M.	François	DE BRONDEAU	Orthopédie dento-faciale	56-01
M.	Pierre-Hadrien	DECAUP	Prothèse dentaire	58-01
M.	Yves	DELBOS	Odontologie pédiatrique	56-01
Mme	Mathilde	FENELON	Chirurgie Orale	57-01
Mme	Hélène	FRON-CHABOUIS	Dentisterie restauratrice et endodontie	58-01
M.	Dominique	GILLET	Dentisterie restauratrice et endodontie	58-01
Mme	Olivia	KEROUREDAN	Dentisterie restauratrice et endodontie	58-01
M.	Jean-François	LASSERRE	Prothèse dentaire	58-01
Mme	Léa	MASSE	Prothèse dentaire	58-01
M.	Philippe	POISSON	Prévention épidémiologie – Economie de la santé – Odontologie légale	56-02

M.	Patrick	ROUAS	Odontologie pédiatrique	56-01
M.	François	ROUZÉ L'ALZIT	Prothèse dentaire	58-01
M.	Johan	SAMOT	Biologie Orale	57-01
Mme	Maud	SAMPEUR	Orthopédie dento-faciale	56-01
M.	Cyril	SEDARAT	Parodontologie	57-01
Mme	Rawen	SMIRANI	Parodontologie	57-01
Mme	Noélie	THEBAUD	Biologie Orale	57-01

PRATICIENS HOSPITALIER-UNIVERSITAIRE

Mme	Virginie	CHUY	Prévention épidémiologie – Economie de la santé – Odontologie légale	56-02
Mme	Julia	ESTIVALS	Odontologie pédiatrique	56-01

AUTRES ENSEIGNANTS

M.	Patrick	BONNE	CDD 2e degré Santé publique	56-02
M.	Pierre-Marc	VERDALLE	CDD 2e degré Parodontologie	57-01
Mme	Anais	CAVARE	MCU associé ODF	56-01
Mme	Laurie	FUCHS	Surnombre Odontologie pédiatrique	56-01

CCU-AH (Chefs de Clinique Universitaires - Assistant des Hôpitaux)

M.	Adrien	AMELINE	Orthopédie dento-faciale	56-02
M.	William	AUMAILLEY	Prothèse dentaire	58-01
M.	Rémi	BAGNARIOL	Dentisterie restauratrice et endodontie	58-01
M.	Baptiste	BERGES	Prothèse dentaire	58-01
Mme	Diane	DELADRIERE	Dentisterie restauratrice et endodontie	58-01
M.	Mathieu	DELOLME	Parodontologie	57-01
M.	Quentin	DESPERIEZ	Prothèse dentaire	58-01
Mme	Laurie	FUCHS	Odontologie pédiatrique	56-01
M.	Joran	GARDIN	Parodontologie	57-01
M.	Paul	GIRARDEAU	Sciences anatomiques et physiologiques	58-01
M.	Pierre-André	GUILLAUD	Parodontologie	57-01
M.	Jean-Benoit	HOCKE	Orthopédie dento-faciale	56-01
M.	Louis	HUAULT	Sciences anatomiques et physiologiques	58-01
Mme	Sarah	KAWCHAGIE	Prothèse Dentaire	58-01
Mme	Claire	LAFOURCADE	Dentisterie restauratrice et endodontie	58-01
M.	Adrien	LARAN	Prothèse dentaire	57-01
M.	Clément	LEBRET	Chirurgie Orale	57-01
M.	Quentin	LEGENDRE	Chirurgie Orale	57-01
Mme	Mathilde	LEVRIER	Prothèse dentaire	58-01
Mme	Léa	MASSE	Prothèse dentaire	58-01
Mme	Chiara	PASCALI	Prothèse dentaire	58-01
Mme	Imane	RAMDANI	Dentisterie restauratrice et endodontie	58-01
Mme	Ana	RIBEIRO MAGALHES	Odontologie pédiatrique	56-01
Mme	Mathilde	SAINT-JEAN	Biologie Orale	57-01
M.	Florian	SAYSSET	Prothèse dentaire	58-01
Mme	Aurore	VENENCIE	Dentisterie restauratrice et endodontie	58-01

Remerciements

A notre Président de thèse

Monsieur le Professeur Adrien NAVEAU

Professeur des Universités – Praticien Hospitalier

Directrice de l'UFR des Sciences Odontologiques

Section Prothèse 58-01

Merci pour la fraicheur de votre enseignement et votre implication à l'Université. Vous êtes une figure de respect et un exemple.

A notre Directrice de thèse

Madame la Docteure Mathilde LEVRIER

Cheffe de Clinique Universitaire – Praticienne des hôpitaux

Section Prothèse dentaire 58-01

Merci pour l'accompagnement dans la rédaction de cette thèse. Merci d'avoir accepté de traiter un sujet qui sortait de l'ordinaire. Merci pour toute la bienveillance et la gentillesse dont vous avez fait part. Je suis reconnaissante d'avoir croisé votre chemin. Merci pour tous les enseignements dispensés.

A notre Rapporteur de thèse

Monsieur le Docteur Pierre-Hadrien DECAUP

Maître de Conférences des Universités - Praticien Hospitalier

Section Prothèse 58-01

Merci pour la relecture rapide de ce travail. Merci pour l'accompagnement au début de mon expérience clinique à l'hôpital Pellegrin. Merci d'apporter une nouvelle vision de la pratique en prothèse.

A notre Assesseur

Madame la Docteure Elise ARRIVE

Maître de Conférences des Universités – Praticien Hospitalier

Section Prévention épidémiologique - Economie de la santé - Odontologie légale 56-02

Merci pour l'accompagnement depuis la genèse de cette thèse. Vous m'avez énormément aiguillé dans mes choix et la réalisation de ce travail. Je vous en suis reconnaissante.

REMERCIEMENTS PERSONNELS

Au Docteur Laurent BOURMAUD, pour la transmission de la passion du métier depuis mon stage de 3ème.

À Isabelle, ma maman, pour le soutien et les sacrifices qui m'ont permis d'en arriver là. Merci d'être mon exemple au quotidien. Merci pour ton courage et ta résilience.

À Jean-Hubert, mon beau-père, merci pour les efforts et les encouragements. Merci d'avoir été présent et prêt à me rendre service toutes ces années.

À ma grand-mère Josianne et mon grand-père Daniel, merci pour votre soutien sans failles et votre amour depuis ma naissance.

À mon papa, merci pour tes encouragements et ton amour.

À Mamie Fatime, merci pour ton soutien. Merci de m'inspirer depuis que je suis toute petite.

À Luka, mon acolyte de promotion depuis la PACES, à coté de moi à chaque étape.

À Noémie, ma soeur d'une autre mère, merci de faire partie de ma vie. Merci d'être là depuis ma première année à Bordeaux. Félicitations pour ta petite myrtille.

À mes amies, Thaïs, Severine, Margaux, Soha, merci d'avoir cru en moi.

À Miley, pour sa présence et son soutien moral à chaque étape depuis tant d'années.

TABLE DES MATIÈRES

Introduction

Depuis les années 1980, le monde connaît une informatisation et une transition numérique dans la plupart des secteurs, dont celui de la santé. Les cabinets dentaires sont passés progressivement du papier aux ordinateurs, apportant de nombreux avantages en termes de stockage, d'accessibilité et de communication. L'arrivée de la carte vitale a été une révolution importante dans l'intégration de l'informatique sur les lieux d'exercice. Cette transition a permis d'améliorer la recherche des dossiers patients, facilitant leur compréhension et les démarches avec les organismes, comme la télétransmission informatique des feuilles de soins.

Néanmoins, ces nouvelles technologies ont apporté de nouveaux dangers. Les praticiens se sont équipés d'outils qu'ils maîtrisent parfois peu et qui sont difficiles à maîtriser. La cybercriminalité n'est pas un phénomène nouveau. En effet, les premiers méfaits remontent aux années 80, mais ils ont connu une croissance exponentielle ces dernières années, totalisant près de 9000 milliards de dollars par an (1)(2).

Malheureusement, les chirurgiens-dentistes semblent être peu sensibilisés aux pratiques malveillantes et aux risques de piratage des appareils numériques présents dans leurs cabinets. La protection des données des patients est pourtant essentielle pour respecter le secret médical. Les différents scandales révélés dans les médias ont permis une prise de conscience des risques liés à l'utilisation des données personnelles et médicales (3).

Nous pouvons prendre comme exemple, le « scandale Cambridge Analytics » qui a été révélé au public dans le New York Times. En effet, le lanceur d'alerte Christopher Wylie a forcé le patron du réseau social Facebook à avouer avoir volé les données personnelles de plus de 86 millions d'utilisateurs sans leur consentement. Celles-ci étaient alors utilisées à des fins politiques pour cibler les publicités lors des campagnes électorales (4).

Les cyberattaques visant à paralyser le cabinet en bloquant tout accès informatique contre demande de rançon ont vu le jour et ne cessent de faire parler d'elles.
Dans ce contexte, mon travail cherche à faire l'état des connaissances sur le sujet dans la profession et à mettre en lumière les moyens mis en oeuvre pour lutter contre la cybercriminalité dans les cabinets dentaires.
Pour cela, après avoir illustré le contexte actuel de l'informatique dans les cabinets dentaires, je retracerai à travers des entretiens individuels les moeurs d'hygiène numérique. Enfin, je proposerai des recommandations et des solutions pour assurer la confidentialité des données de santé des patients.

1. L'informatique dans les cabinets dentaires

1.1 L'histoire du dossier patient

Voilà plus de 4000 ans que le dossier médical évolue et contribue à améliorer la prise en charge des soins donnés aux patients. Les médecins de Babylone, 4000 ans avant Jésus Christ, étaient soumis à des règles professionnelles regroupées dans le code d'Hammourabi (5). Celui-ci prévoyait des sanctions pour les médecins maladroits et incompétents. On retrouve également dans l'Antiquité égyptienne, la notion de « registres salutaires » dans lesquels sont synthétisés les symptômes et les thérapeutiques des patients (6).

D'après « Le savoir vagabond » de Patrick Berche (7) , un tournant s'est produit au 18ème siècle à Berlin et à Paris où de nombreux fichiers dactylographiés de médecins rapportaient des analyses et des données cliniques pour chacun de leurs patients.

Dans la même période à l'hôtel Dieu à Paris a été créé un registre pour répertorier des informations propres à chaque patient, mais son contenu restait succinct. En ville, l'oralité restait le mode dominant de transmission des données de santé (8).
Dans le même temps mais cette fois ci au Danemark, le médecin Christopher Detlev Hahn a systématisé, dans son cabinet médical en 1766, le répertoriage des dossiers en latin inhérents aux visites de ses patients. Ceux-ci contenaient leurs diagnostics ainsi que leurs traitements. Plus de 2000 de ses dossiers ont été reliés en 27 volumes et conservés dans les archives du musée médical de Copenhague (9).

Le dossier médical qui au départ possédait seulement un rôle éducatif et de transmission d'informations, a assumé, par la suite, d'autres rôles tels que l'assurance ou les procédures juridiques (10). À partir de la deuxième moitié du 20^{e} siècle, le dossier médical commence à être encadré par des textes de loi. En France, la réglementation impose un premier modèle de dossier médical par l'arrêté du 24 juin 1970 (11). Très vite, les avancées numériques ont engendré un passage des dossiers papier aux dossiers numériques.

1.2 Du papier à l'ordinateur

Le progrès massif et rapide des technologies au cours de la deuxième partie du XXème siècle a amené les chirurgiens dentistes à faire évoluer la manière de gérer les données de santé de leurs patients. L'arrivée du numérique dans la profession a été plutôt rapide, en voici quelques dates clés.

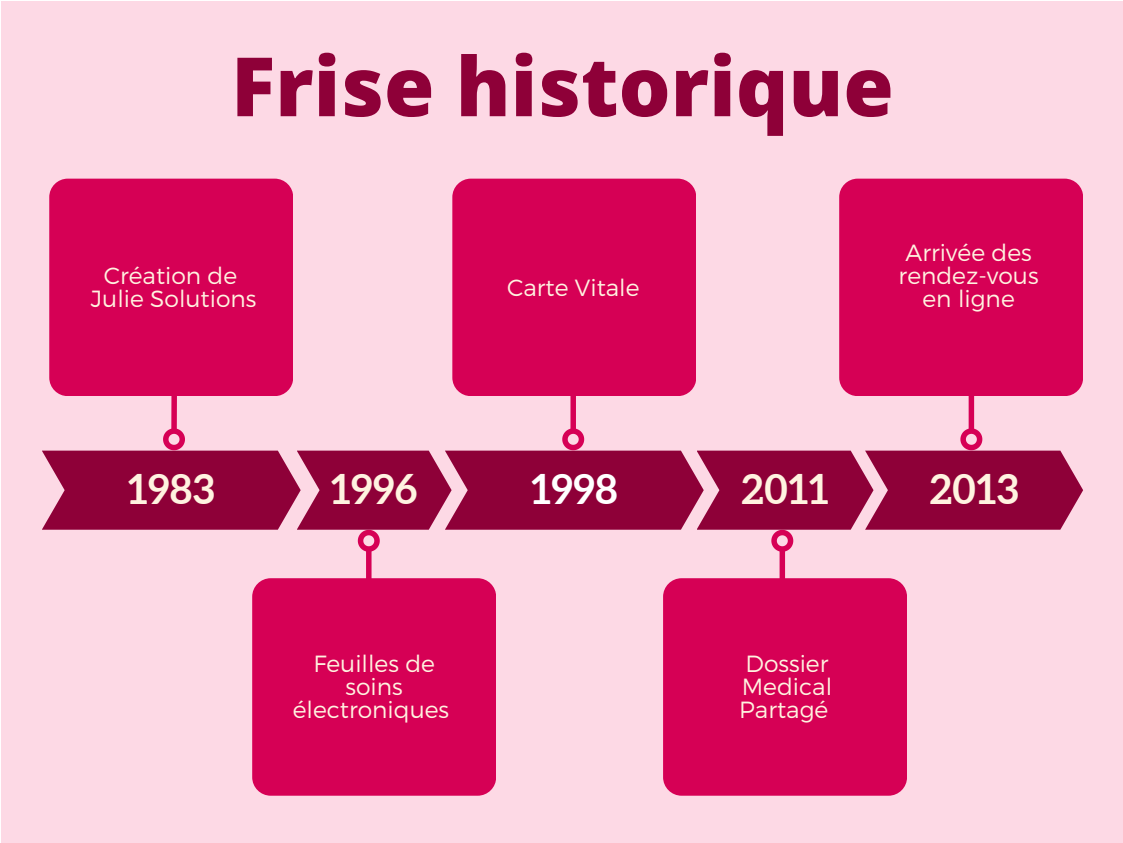


Figure 1 : Fresque historique réalisée selon la frise historique de Julie solutions (12)

Dès 1983, la société Julie Solutions fondée par Arturo Pandolfo & Jaime Oliver, informaticiens passionnés, a créé l'un des premiers logiciels de gestion de cabinet dentaire.

Ils ont également été à l'origine du premier logiciel capable de gérer un capteur radiologique numérique en 1988. Julie solutions a été un acteur essentiel du numérique dans la profession ainsi que dans l'organisation d'un cabinet dentaire avec plus de 140000 utilisateurs en France en 2024 (12).

La société s'est développée au fil des années en proposant de nouvelles fonctionnalités numériques comme l'intégration des sms de rappel de rendez-vous, la mise en place d'un agenda en ligne ou la prise de rendez-vous en ligne par le patient (13).

La société a même collaboré avec l'Etat à l'occasion du Ségur de la santé en 2021 dans le cadre d'activités de recherche et d'aide au développement de nouveaux concepts numériques tels la dématérialisation de la carte vitale, la prescription numérique ou encore la messagerie sécurisée de santé (14).

En 1993, une autre société de logiciel de gestion de cabinets dentaires s'est créée sous le nom de Logos. Elle est maintenant bien connue du grand public.

La même année, le réseau GIE SESAM-Vitale a été missionné par l'Assurance maladie pour sécuriser et moderniser le système de facturation et de remboursement des frais de santé.
Il devient, à l'époque, et est toujours aujourd'hui un acteur majeur du numérique de santé (15).

En 1996, l'article 8 des ordonnances dites Juppé dispose que, « le 31 décembre 1998 au plus tard, les professionnels, organismes ou établissements dispensant des actes ou des prestations remboursables par l'assurance maladie doivent être en mesure, chacun pour ce qui le concerne, d'émettre, de signer, de recevoir et de traiter des feuilles de soins électroniques ou documents assimilés conformes à la réglementation » (16).
Les praticiens sont alors contraints de se moderniser pour télétransmettre les feuilles de soins qui deviennent électroniques.

Deux ans plus tard, en 1998, la Carte Vitale, une carte électronique individuelle d'assuré social est créée pour permettre cette dématérialisation des feuilles de soins (17).

En 2011, le dossier médical partagé, appelé dossier médical personnel avant 2015, est lancé par le service public français afin de créer un dossier médical en ligne, gratuit et sécurisé. Il se nomme depuis fin décembre 2022 « Mon Espace Santé » et permet de stocker les informations médicales. Il est aussi possible de les partager avec les professionnels de santé qui soignent un même individu en respectant son consentement.

L'Etat devient donc un acteur engagé de la numérisation de la santé.

En 2013, la société Doctolib est créée et survient alors l'avènement des rendez-vous médicaux en ligne. À partir de 2016, *Julie Solutions* propose cette option à ses utilisateurs afin de faciliter la prise, le rappel et l'organisation des rendez-vous.

L'utilisation au quotidien de la CCAM dans les cabinets dentaires rend indispensable l'accès à l'informatique. Bien qu'il n'y ai aucune réglementation en vigueur, il semble compliqué de pouvoir exercer sans un ordinateur et un logiciel métier.

L'informatique est donc omniprésente dans le quotidien du cabinet que ce soit dès l'arrivée du patient jusqu'à sa sortie de la structure.
La création d'un dossier médical, l'enregistrement ou la rédaction d'ordonnances, l'acquisition de radiographies (panoramiques ou rétroalvéolaires), la cotation des actes, le recueil de l'anamnèse, la facturation, la télétransmission ou encore l'accessibilité aux données de comptabilité sont tant d'actions centralisées et optimisées grâce au numérique.

1.3 La transformation digitale

En plus de toutes ces évolutions, des innovations technologiques ne cessent d'émerger. Bien qu'elles cherchent à toujours plus optimiser l'expérience numérique du praticien, celui-ci ne semble pas encore tout à fait aguerri sur la sécurisation des fonctionnalités de base.

Il est aujourd'hui possible d'avoir recours au « cloud computing » permettant un stockage des données à distance de son ordinateur. Cela soulève alors une nouvelle question de sécurité à propos des données de santé qui quitteraient de façon digitale le cabinet.

En novembre 2022, le lancement international de ChatGPT a propulsé l'intelligence artificielle sur le devant de la scène. Ce « chatbot » utilise le processus du langage naturel et le traite pour répondre à l'humain de manière conversationnelle. Ce nouvel outil permet de faciliter de nombreuses tâches. Il est notamment utilisé comme support dans les décisions cliniques car il peut aider au diagnostic, à la prise de rendez-vous, à l'écriture des courriers ou encore à la traduction pour communiquer avec les patients étrangers. Il existe notamment une version d'aide à l'analyse des radiographies panoramiques qui permet la détection de restaurations dentaires déjà présentes et le dépistage des anomalies dentaires et maxillo-faciales (18)(19).

Ainsi le praticien peut s'appuyer sur des aides numériques qui lui font gagner en optimisation et en temps. Cependant, il doit rester vigilant quant aux différents risques liés à cet outil et notamment le risque de failles dans la sécurité des données patients et plus largement dans la sécurité informatique du cabinet.

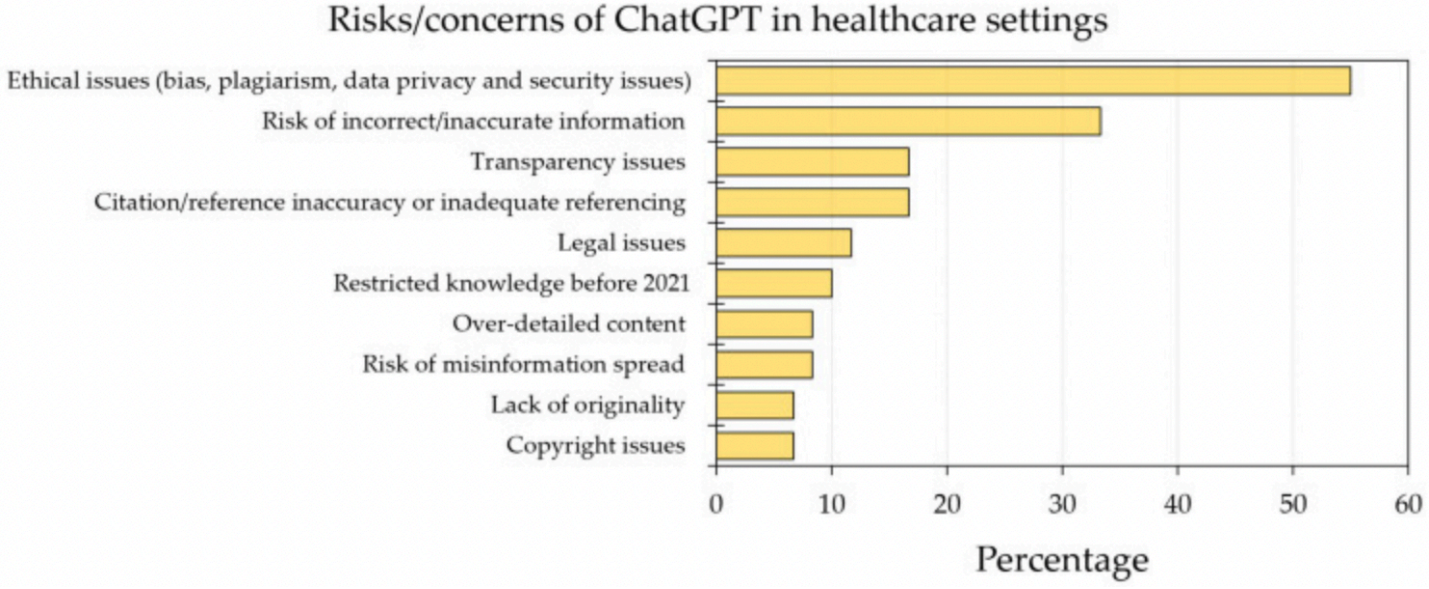


Figure 2 : Résumé des différents risques à propos de l'utilisation de ChatGPT dans le cadre médical selon Sallam M. 2023 (20)

2. La législation

2.1 Le secret professionnel

Le secret professionnel est à la base de la confiance que les patients ont envers leur praticien. Cette notion a été introduite à la création du Serment d'Hippocrate au Vème siècle avant J-C. Elle figure dans la traduction du texte original en grec :
« Tout ce que je verrai ou entendrai au cours du traitement, ou même en dehors du traitement, concernant la vie des gens, si cela ne doit jamais être répété au-dehors, je le tairai, considérant que de telles choses sont secrètes. » (21).

Hippocrate est considéré comme le « père de la médecine ». Ce philosophe grec est à l'origine d'une méthode d'observation clinique et a créé des règles éthiques pour les professionnels de santé (22).

Le secret médical est toujours un des fondements de la médecine du 21ème siècle et est inscrit dans le code de déontologie. Il est également appelé le secret professionnel, et se définit maintenant comme « le droit d'un patient au respect de sa vie privée et au secret des informations le concernant » (23).

La première phrase de l'article R. 4127-206 du Code de la santé publique rappelle que : « le secret professionnel s'impose à tout chirurgien- dentiste, sauf dérogations prévues par la loi »
Le praticien est donc tenu de filtrer l'accès aux données personnelles de ses patients (24).

Deux autres articles du Code de la Santé Publique concernent le secret professionnel :
L'article R.4127-207 rapporte que « Le chirurgien-dentiste doit veiller à ce que
les personnes qui l'assistent dans son travail soient instruites de leurs obligations en matière de secret professionnel et s'y conforment. »
Et l'article R.4127-208 précise que « En vue de respecter le secret professionnel, tout chirurgien-dentiste doit veiller à la protection contre toute indiscrétion des fiches

cliniques, des documents et des supports informatiques qu'il peut détenir ou utiliser concernant des patients. »
Par exemple, lorsqu'il utilise ses observations médicales pour des publications scientifiques, il doit faire en sorte que l'identification des patients soit impossible (25).

Le secret professionnel englobe donc plus que les données médicales mais aussi toutes les autres informations qui concernent la vie privée du patient. Il doit être rigoureusement respecté sous peine d'entraîner des sanctions pénales, civiles et professionnelles (26).

Toutes les données concernant le patient, qu'elle soit des données de santé (antécédents, traitements, motif de consultation, diagnostics etc) ou non (adresse, liens de parenté, numéro de téléphone etc) relèvent du secret médical. Qu'elles soient conservées sous forme informatique ou non, qu'elles concernent un patient nominativement ou permettent de le reconnaître, elles relèvent de sa vie privée et leur protection est, en vertu du secret professionnel, sous la responsabilité du chirurgien-dentiste les détenant.

2.2 La loi Informatique et Liberté

La France a été, en 1978, le 3eme pays d'Europe après l'Allemagne (en 1971) et la Suède (en 1973) à se doter d'une Loi « Informatique et Liberté » (LIL). Cette loi a pour but de garantir que l'informatique serve les intérêts des citoyens et ne porte pas d'atteinte à leurs droits et leurs libertés.

Cette loi du 6 janvier 1978, modifiée le 31 janvier 2017, encadre l'utilisation des données à caractère personnel et comprend les données numériques. L'article 64 de cette loi s'occupe des traitements de données à caractère personnel dans le domaine de la santé.

Cet article rapporte que « Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique » (27).

Le texte de loi LIL définit les cinq droits fondamentaux en informatique pour garantir aux Français la maitrise de leurs données. Les différents droits des citoyens sont : le droit à l'information, à l'accès, à la rectification, à l'opposition et à l'oubli.

Cette loi a du être complètement remaniée suite à l'adoption du Règlement Général de Protection des Données dit RGPD en 2018. La loi originelle est modifiée afin de la conformer au RGPD applicable dans tous les pays européens à travers l'ordonnance du 12 décembre 2018 qui est la réécriture complète de la LIL.

2.3. Le RGPD

Le RGPD, Règlement Général de Protection des Données, adopté par l'Union européenne le 14 avril 2016, vise à apporter un niveau élevé et cohérent de protection pour les données. Il est mis en oeuvre le 15 mai 2018 et bouleverse le monde de l'informatique. En effet, les grands groupes tout comme les petits sites internet ont dû s'adapter au RGPD en un peu plus de deux ans. De ce fait, l'État français a dû remanier entièrement la loi informatique et liberté en supprimant la quasi-totalité de ses articles pour y transposer ce règlement.

Figure 3 : Montant des amendes que peut prononcer la CNIL selon le RGPD du 17 avril 2016 et la loi du 20 juin 2018 (28)

Le RGPD modifie substantiellement la réglementation en matière de protection des données à caractère personnel et ce dans toute l'Union Européenne. Ce règlement s'applique à tous les pays membres et permet de diminuer les disparités entre règlements nationaux sur la protection des données.

Le règlement prévoit aussi une notion de sécurité par défaut et la nécessité d'un consentement positif et explicite aux stockages des données patients. Mais ces nouvelles obligations sont, en principe, déjà mises en oeuvre par les professionnels de santé habitués à gérer les données de santé recueillies dans le respect du secret professionnel.
Le RGPD crée un nouveau droit à la portabilité. Celui-ci permet à un citoyen le transfert de ses données personnelles pour sa propre utilisation ou celle d'un organisme pour lequel il aura donné son consentement.

Le règlement impose également que soient notifiées à l'Autorité Nationale de Protection (ANP) toute fuite de données (article 33). Ceci a pour but d'identifier les organismes dont la sécurité informatique est défaillante et sensibiliser sur la manière de protéger les données personnelles. Cela devrait participer à un processus global de sensibilisation sur l'importance de bien garantir la sécurité des données.

3. Les menaces informatiques

3.1 Définitions

Les attaques informatiques sont communément appelées « cyberattaques ». Celles-ci sont réalisées par des « hackers ».

Cyberattaque

D'après IBM, International Business Machines, les cyberattaques sont des tentatives indésirables de voler, d'exposer, de modifier, de désactiver ou de détruire des informations via un accès non autorisé aux systèmes informatiques. Ces atteintes réalisées dans un but malveillant sont orchestrées par des hackers (29).

Hacker

D'après le Larousse, un hacker est une personne qui par jeu, gout du défi ou souci de notoriété cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou réseau informatique (30).

Il existe plusieurs façons pour les hackers de pirater une infrastructure et pour ce qui nous intéresse : un cabinet dentaire.

3.2 Différents types d'attaques

L'hameconnage « phishing »

Il est un type d'attaque commun distribué sous la forme d'un émail frauduleux déguisé en tiers de confiance (banque, administration, fournisseur d'accès).
Le mail contient souvent un lien ou une pièce jointe. Il suffit alors au destinataire de cliquer dessus pour télécharger sans son consentement et en toute discrétion un logiciel malveillant. Ce genre de mails peut aussi contenir un lien clickable qui dirige sur un site pour récolter des informations personnelles.

Cette technique est donc utilisée afin de récupérer des données sensibles auprès d'un utilisateur.
La plateforme « Signal Spam » en collaboration avec la CNIL permet de signaler les mails suspects reçus. Ils sont examinés par un comité d'experts qui travaille contre les cybercriminels à l'échelle nationale avec les autorités publiques et les services de messagerie (31).

Le logiciel rançonneur « ransomware »
Cette technique est un type particulier de logiciel malveillant. Il entraine un chiffrage complet des données de l'ordinateur sur lequel il est téléchargé. Les fichiers sont alors rendus inaccessibles. L'appareil peut être touché de différentes façons. Un clic sur un lien ou une pièce jointe suffit aussi pour être infecté. Cela peut aussi survenir lors d'une navigation sur un site compromis ou à la suite d'une intrusion dans le système informatique. L'étape suivante est un chantage aux victimes afin d'obtenir de l'argent en contre partie de la récupération de leur données. Les ravisseurs peuvent insister sur le fait de rendre les informations publiques. La rançon réclamée peut s'élever jusqu'à des millions d'euros. Elle est souvent demandée sous forme de monnaie virtuelle type bitcoins, monero ou encore ethereum. L'utilisation de ces cryptomonnaies permet de garder l'anonymat des pirates et complique le travail des autorités pour les retrouver. Les victimes ne sont jamais sures de récupérer leurs données en payant la rançon.
Celle-ci peut alors être augmentée ou d'autres versements peuvent être réclamés. Il est fortement déconseillé de la payer.

En 2020, le site de la cybermalveillance du gouvernement français atteste dans son rapport d'activité que l'attaque par *ransomware* est la principale menace à laquelle les professionnels d'une manière générale ont été confrontés dans le secteur public comme privé. En revanche, les particuliers étaient touchés à moins d'1% (32).

Le piratage de la messagerie et/ou des réseaux sociaux
Cette manœuvre permet d'usurper l'identité de la personne piratée afin d'escroquer ses contacts.

L’attaque par piratage du système informatique

Elle consiste en l’intrusion d’un tiers non autorisé sur un ordinateur ou un appareil électronique. L’objectif du pirate est de contrôler la ressource et d’en dérober les informations à des fins malveillantes.

Le pirate revend la plupart du temps les données sur le dark web.

Le terme de piratage est souvent utilisé dès qu’il y a de la malveillance informatique mais il n’est que véritablement bien utilisé s’il y a eu l’intrusion non autorisé. L’hameçonnage par exemple évoqué précédemment est un vecteur de piratage mais n’en est pas directement un (33).

La défiguration de site internet

Elle permet de modifier l’apparence d’un site web. Celui-ci n’est pas utilisable durant l’attaque et porte souvent, après l’action des hackers, un message ou logo mentionnant le hacking. Les pirates peuvent en retirer les informations sensibles telles les données personnelles, médicales ou encore bancaire et montrent publiquement qu’ils ont le pouvoir d’accéder à ces données (34).

3.3 Echelle Mondiale

Devant la multiplication des cyberattaques, la cybersécurité est devenue un sujet de préoccupation majeur.

Dès 2016, le professeur Clemens Scott Kruse, de l’université du Texas, avait réalisé une revue systématique de littérature sur les menaces informatiques ciblées contre les données de santé (35). Il a mis en lumière l’impact de l’avènement informatique dans le domaine de la santé sur l’échange électronique des données patient.

Les résultats vont dans le sens d’une augmentation statistiquement significative de la vulnérabilité des établissements de santé aux cyberattaques.

En 2017, ce même professeur a réalisé une seconde revue systématique de littérature concernant les menaces modernes et tendances qui pèsent sur la cybersécurité dans le domaine de la santé (36). Après une analyse de 31 articles, l’étude a conclu en un retard de sécurité dans l’industrie de la santé par rapport à d’autres secteurs. Il manque en santé des procédures de protection numérique.

Il conclut par établir que l'industrie de la santé est une cible principale pour les voleurs de données médicales et qu'il est impératif d'investir du temps et de l'argent pour maintenir et assurer une protection efficace des données patients confidentielles contre les accès non autorisés.

Plus récemment, en 2022, Ramo Sendelj, professeur de l'Université du Montenegro, a rédigé un article à propos des challenges de la cybersécurité dans le domaine de la santé (37). On y retrouve notamment quelques statistiques collectées de 2016 à 2022 dans le système de santé américain. Celles-ci montrent que presque 30% des incidents informatiques majeurs avaient pour cible des institutions de la santé. Le tableau ci-dessous nous montre également l'augmentation manifeste au fil des ans du nombre d'attaques résultant de failles dans la protection des données.

Table 1. Healthcare Data Records Breached and Healthcare Data Breaches 2016–2022 [2] [6] [7]

Year	No. of Data Breach Event	No, of Data Breached Records
2016	115	13.429.721
2017	148	3.513.380
2018	164	9.992.440
2019	312	38.429.532
2020	416	26.424.309
2021	521	43.096.956
6 months of 2022	347	20.214.270

Figure 4 : Comparaison entre 2016 et 2022 du nombre de rapports de fuites de données dans le domaine médical selon Ramo Sendlj (37)

Cet article énonce également les raisons pour lesquelles l'industrie de la santé est une des plus grosses cibles des cyberattaques. S'intéresser à celles-ci permet de mieux comprendre pourquoi la cybersécurité est importante dans les établissements de santé et notamment dans nos cabinets dentaires.

Ainsi, différentes causes sont mise en évidence :

- Les données de santé ont une grande valeur sur le marché noir.
- La volonté de protéger les données de santé est sans limite pour les institutions.

- Le matériel médical numérique (pompe à insuline, appareils d'imagerie radiologiques, moniteurs cardiaques etc) est vulnérable et est une porte d'entrée facile pour les attaques.
- La nécessité de transmettre des informations entre professionnels de santé (parfois via leurs appareils personnels) représente une faille facile à l'intrusion malveillante.
- Le niveau inadéquat de connaissances en cybersécurité dans le milieu médical.
- Le manque de budget en sécurité informatique, notamment dans les petites structures de soin.

Dans le même sens, l'entreprise Checkpoint Software France rapporte, dans son bilan annuel, qu'en 2022, les cyberattaques ont augmenté de 38% dans le monde. Le secteur de la santé fait partie des trois secteurs les plus attaqués avec les administrations publiques et le secteur de l'éducation (38).

L'Europe n'échappe pas aux tendances mondiales avec une augmentation de 26% entre 2021 et 2022. L'entreprise déclare également qu'en 2023 les chiffres ne risquent pas de diminuer avec l'arrivée de l'Intelligence Artificielle (IA).

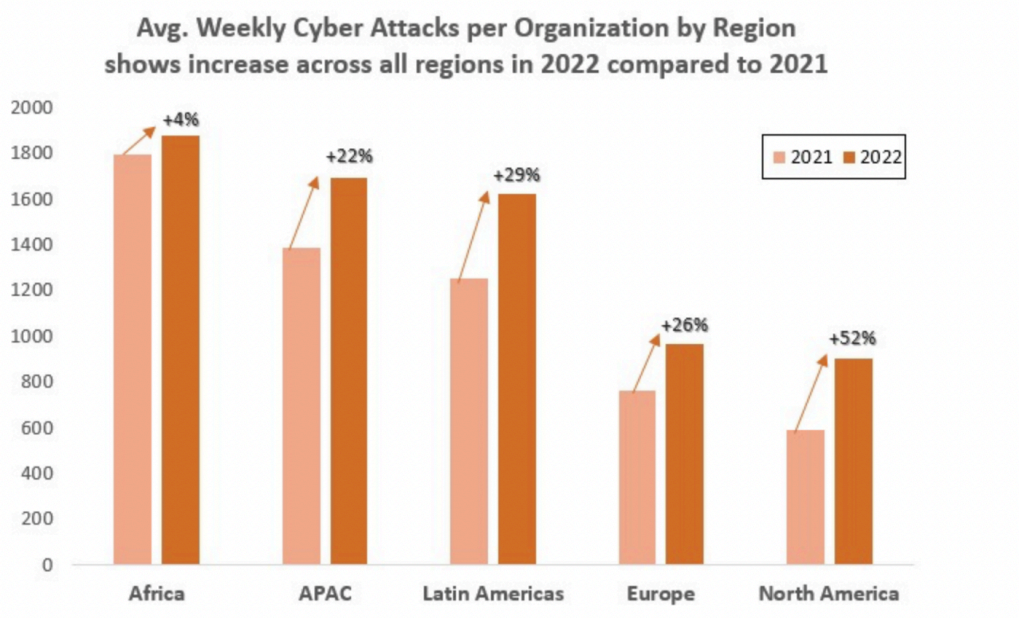


Figure 5 : Comparaison entre 2022 et 2021 du nombre de cyberattaques hebdomadaires classées par régions du monde par Checkpoint (38)

3.4 Echelle Nationale

A l'échelle de la France, plusieurs statistiques vont dans le sens de l'augmentation de cybercriminalité dans le domaine de la santé.

Le médecin généraliste et directeur des systèmes d'information et du numérique de santé des armées françaises, Didier Mennecier, a associé les données de santé à un "nouvel El Dorado" pour les hackers (39).

Les numéros de Sécurité Sociale auraient pour valeur monétaire plusieurs centaines de dollars chacun contre seulement quelques dollars pour un numéro de carte bancaire. Aussi, le système de ransomware serait de plus en plus utilisé pour attaquer les structures hospitalières et les dispositifs médicaux tels que les pompes à insuline, les pompes à perfusion et les stimulateurs cardiaques seraient une porte d'entrée pour la hacking.

En France, en 2021, l'Agence Numérique de la Santé (ANS), a relevé au moins une cyberattaque par semaine (40). Corbeil-Essonnes, Beuzeville, Arles, Oloron Sainte-Marie, Dax, Villefranche-sur-Saone sont, entre autres établissements, une liste de structures de soin victimes de piratage informatique en 2022 (41).

L'Agence du Numérique de la Santé rapporte également qu'en 2022, les établissements médicaux ont déclaré 30% d'incidents de cybersécurité de plus qu'en 2021 (42).

Xavier Duros, expert chez CheckPoint Software France, le leader mondial dédié à la sécurité des entreprises, déclare lui aussi une augmentation de 38% des cyberattaques par semaine sur les réseaux d'entreprises en 2022 par rapport à 2021. Les attaques par ransomware continuent de croitre. Checkpoint Software France rapporte 644 cyberattaques hebdomadaires en moyenne pour les entreprises du secteur de la santé en France en 2022 soit 191% de plus qu'en 2021.

Le secteur de la santé serait le 7ème secteur français le plus attaqué. Les petits hôpitaux seraient particulièrement vulnérables car leurs ressources en matière de sécurité informatique sont insuffisantes. L'aspect lucratif des données de santé et la notoriété apportée suite à l'attaque d'un hôpital attirent les pirates (38).

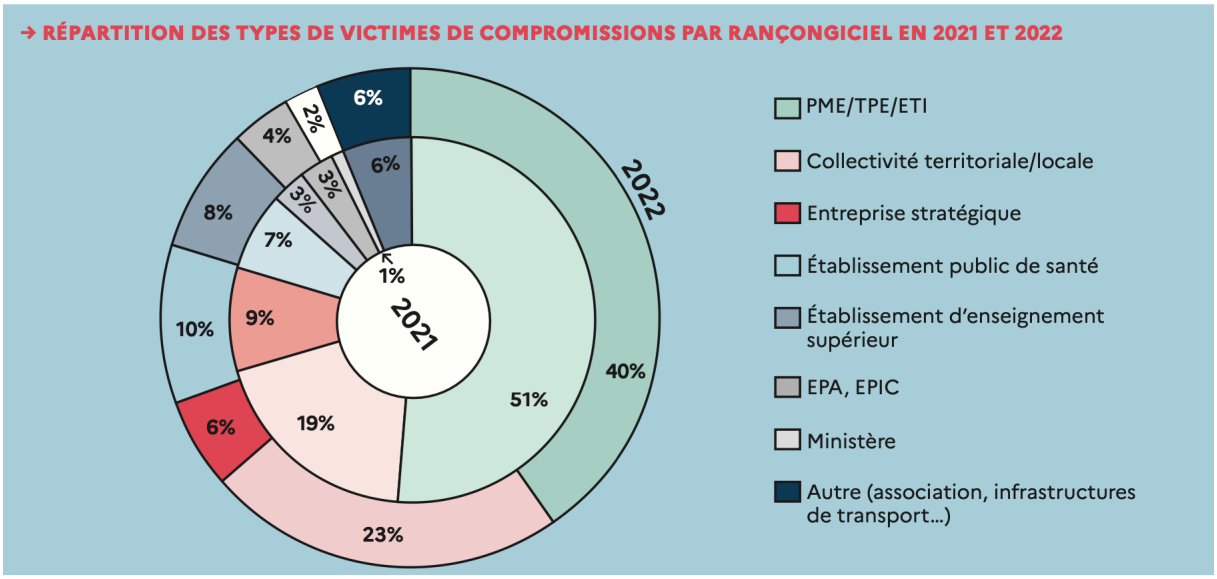


Figure 6 : Répartition des types de victimes de compromissions par rançongiciel en 2021 et 2022 par l'ANSSI (43)

L'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) enregistre également une multiplication des attaques par rançongiciels depuis l'été 2022 particulièrement ciblée sur les établissements de santé (43).

Force est de constater que la menace informatique est réelle, notamment dans les petites structures de santé. Il est donc facile d'imaginer à quel point les cabinet dentaires sont une cible idéale pour les pirates.

3.5 Echelle de la profession

Dans la région par exemple en novembre 2021, une dizaine de cabinets dentaires de Gironde ont été victimes d'une attaque informatique. Cette attaque a paralysé l'ensemble des cabinets touchés qui se sont vus demander une rançon par les hackers (44).

D’après les différents témoignages, une technique en particulier semble privilégiée par les cyberattaqueurs ; celle du logiciel rançonneur (44) (45).

En effet, Docteur Patricia Cabanie a constaté le matin du piratage de son cabinet que l’ensemble des données informatiques nécessaires au fonctionnement de celui-ci avait disparu. La praticienne n’avait jamais imaginé qu’une telle attaque aurait pu toucher sa petite structure. Le hacker lui a demandé une rançon en cryptomonnaie, il s’agit d’une technique ransomware. Après dix jours passés sans solution, la praticienne a fini par céder. Par chance, après avoir payé la rançon, elle a pu récupérer ses données et améliorer sa sécurité numérique (44).

Docteur Durietz, chirurgien dentiste à Saint Quentin, a lui aussi été victime d’un piratage informatique le 23 mars 2020. Malheureusement, celui-ci a eu lieu lors de la période d’arrêt de travail pour cause de la crise sanitaire du covid. Cela lui a complexifié la démarche pour récupérer les données.
Le praticien raconte avoir, à la suite d’une tentative d’installation d’un logiciel de prise en main à distance, reçu des mails dans une langue étrangère contenant des liens sur lesquels il a cliqué. Quelques jours plus tard, toutes les données de son logiciel professionnel avaient disparues. Il s'agissait, dans cette situation aussi, d'un logiciel ransomware. Celui-ci avait crypté toutes les données du praticien et le pirate informatique réclamait 1500 dollars pour les remettre à disposition. Le docteur Durietz disposait d'un système de sauvegarde externe mais n'avait pas enregistré ses données depuis un mois et demi. Il n'a pas payé la rançon et a ainsi perdu un mois et demi de données (45).

Ici, les deux praticiens, bien qu'équipés d'un système de sauvegarde externe, n'ont pas réalisé les sauvegardes assez fréquemment. Cela a fait d'eux des proies faciles à la cyberattaque et surtout à la demande de rançon pour récupérer les données.
La méconnaissance de ces attaques donnent lieu à un relâchement de la rigueur de l’hygiène numérique dans les cabinets dentaires.
Il est donc important d’adopter des pratiques d’hygiène numérique au quotidien pour se protéger de ce type d’attaques.

4. Evaluation des pratiques d'hygiène numérique dans les cabinets dentaires

4.1. Objectifs

L'objectif principal de cette étude était de déterminer si les praticiens avaient bien connaissance des lois concernant le respect des données personnelles et leur protection ainsi que d'appréhender leurs habitudes d'hygiène numérique au sein du cabinet.
Les objectifs secondaires consistaient à demander aux chirurgiens dentistes d'estimer leurs connaissances sur les risques encourus et le niveau de sécurité des moyens employés pour lutter contre la cybercriminalité.

4.2 Méthodes

4.2.1 Design de l'étude

Il s'agit d'une étude qualitative basée sur des entretiens semi-dirigés individuels avec des chirurgiens-dentistes libéraux.

Chaque discussion a suivi un plan classique basé sur un guide d'entretien (annexe 1).
Le guide d'entretien avait pour but d'orienter les interlocuteurs vers des réponses fiables qui relatent leur expérience dans le domaine. Les questions posées regroupent une partie juridique, une partie exécutive ainsi qu'une partie ouverture sur le sujet.Les entretiens semi-dirigés ont d'abord été retranscrits à l'écrit, puis, après avoir lu l'ensemble du corpus, des thèmes ont été identifiés pour classer les verbatim par thèmes et par nombre d'occurrences.

4.2.2 Nombre de sujets nécessaires

Le nombre de sujets à inclure dans une étude qualitative est défini par le seuil de saturations des concepts d'après Dr Baker (46). Ici il est d'environ 7 à 10 sujets.

4.2.3 Critères d'inclusion et d'évaluation

Les critères d'inclusion se résument aux chirurgiens-dentistes d'accord pour participer.
Les critères d'exclusion regroupent les chirurgiens-dentistes dans l'incapacité physique ou psychique à participer à l'entretien au moment de l'étude.

Le but était d'interroger des profils de praticiens assez différents en terme d'âge et de genre mais aussi en terme de structures de santé. Du praticien seul en campagne au cabinet pluri-praticiens de ville, les profils ont été diversifiés au maximum afin d'avoir une vision la plus élargie possible de cette étude.

Pour des raisons d'ordre pratique, les praticiens visités étaient répartis entre les régions de la Gironde et du Lot-et-Garonne dans les villes de Lauzun, Marmande, Bordeaux et Libourne.

4.2.4 Déroulement de l'étude

La période d'enquête s'est déroulée de Octobre 2023 à Décembre 2023, soit sur 3 mois. Pour chaque chirurgien-dentiste rencontré, l'entretien a été mené par une seule investigatrice et de façon à ne pas influencer les réponses.
Aucun questionnaire n'a été envoyé par e-mail ou par téléphone.
Si le praticien n'était pas disponible au moment de la visite, un nouveau rendez-vous était programmé.
Les chirurgiens-dentistes n'avaient pas accès aux questions avant l'entretien et la rédaction des réponses était sous la responsabilité du thésard.
Chaque entretien a duré entre 10 et 20 minutes et les données ont été traitées via un tableur Excel.

4.3 Résultats

4.3.1 Descriptif du panel de l'étude qualitative

Le panel utilisé pour l'étude a inclus dix chirurgiens-dentistes. Les femmes chirurgiens-dentistes étaient au nombre de cinq. Les praticiens exerçant en ville étaient au nombre de cinq également contre cinq praticiens de campagne. Enfin, cinq des dix participants faisaient partie d'un cabinet de groupe, soit une structure comprenant plus de deux chirurgiens-dentistes. La moyenne d'âge des participants était de 39 ans et demi, composée de quatre participants de la tranche d'âge 25-35 ans, trois de la tranche d'âge 35-45 ans et enfin trois dans la tranche 45 ans et plus.

4.3.2 Thèmes identifiés et classement des verbatim par nombre d'occurrences

1) Quelle est la place de l'informatique actuellement dans votre cabinet dentaire ?

Parmi les chirurgiens-dentistes interrogés, neuf ont déclaré considérer la place de l'informatique au cabinet dentaire comme « indispensable ».
Un seul a jugé qu'elle était, à un degré inférieur, importante.

« Je n'utilise l'informatique que pour télétransmettre à la Sécurité sociale et je remplis encore tous mes dossiers au format papier ».

2) Connaissez vous la loi RGPD ?

Concernant la loi RGPD, cinq praticiens interrogés ont répondu par la négative. L'idée qui ressort des entretiens est donc que la moitié des participants ne connaissait pas cette loi.

« Non je n'en ai jamais entendu parlé » « De nom cela me dit quelque chose mais je ne sais plus à quoi correspond l'acronyme »

3) Si oui, comment se passe la mise en pratique de la RGPD dans votre cabinet ?

Les chirurgiens-dentistes qui ont répondu qu'ils avaient connaissance de la loi RGPD ont décrit les actions qu'ils mettent en place pour la respecter.

« Je connais la loi RGPD et j'associe cela au secret médical mais pour tous ce qui concerne l'informatique au cabinet. » « La loi RPDG est connue et obligatoire. » « Sa mise en pratique est réalisée à travers l'utilisation de logiciels sécurisés qui garantissent la sécurité des informations. »

Ils sont conscients des spécificités techniques que cette loi requiert.

« La télétransmission à la Sécurité sociale, elle, est réalisée à l'aide d'un réseau indépendant privé sécurisé qui nécessite un abonnement spécifique. »
« La partie la plus délicate reste l'échange par mail avec les patients. Ceux-ci sont réalisés sur des messageries sécurisées et des précautions sont prises, comme ne pas utiliser de nom, prénom ou d'informations personnelles dans leur contenu. »

4) Avez-vous embauché un sous traitant informatique ?

Pour cette question, sept praticiens ont répondu par la négative.

« Non je n'ai embauché personne qui s'occupe exclusivement de la sécurité informatique du cabinet ».

Trois chirurgiens-dentistes interrogés ont embauchés un sous traitant informatique.
Ils préfèrent déléguer à une personne compétente dans le domaine.

« La sécurité informatique du cabinet est réalisée par un sous-traitant qualifié. » « J'ai embauché un informaticien qui s'occupe de tout ça » « Il existe également des sociétés spécialisées qui réalisent des tests pour tenter de pirater le cabinet afin de tester réellement l'efficacité des moyens déployés. »

5) Est ce que chaque membre du personnel du cabinet a accès aux outils informatiques ?

Neuf praticiens ont répondu positivement à cette question. Une exception est soulignée chez un seul praticien qui donne l'accès informatique à ses secrétaires mais pas à ses assistantes.

« Seules mes secrétaires ont accès aux outils informatiques au secrétariat. Mes assistantes sont au fauteuil avec moi ou en stérilisation, elle ne s'occupe pas de l'informatique. »

Un chirurgien-dentiste a répondu par oui mais a souhaité préciser que sa technicienne de surface, membre du personnel, n'avait pas accès à l'ordinateur.

« Chaque membre du personnel, excepté la technicienne de surface, a accès aux outils informatiques. »

6) Les différents membres du cabinet ont-ils des identifiants et code d'accès personnalisés pour pouvoir utiliser les logiciels ?

Une majorité de praticiens, soit six, possède un mot de passe personnalisé.
Il ressort que trois secrétaires et trois assistantes ont leur propre mot de passe.
L'idée majoritaire est qu'au quotidien, elles utilisent celui de leur praticien.

« C'est un mot de passe par praticien, les assistantes et secrétaires utilisent le même que le chirurgien-dentiste ».

Certains cabinets, quatre, ne différencient pas les mots de passe en fonction des utilisateurs.

« C'est un mot de passe par ordinateur, il ne change pas en fonction de qui l'utilise. »

Trois cabinets ont décidé de choisir un mot de passe différent pour chaque membre du personnel.

« Les mots de passe ont une base commune adaptée aux différents logiciels, comportent plus de 8 caractères, des chiffres, des lettres, et un caractère spécial.
Ils sont personnalisés pour les praticiens et les deux secrétaires. Ils sont communs pour les assistantes qui agissent sous l'autorité du praticien auquel elles sont affectées. »

7) A quelle fréquence les mots de passe sont-ils renouvelés ?

Un grand nombre de praticiens ne renouvelle pas les mots de passe, soit 8 praticiens.

« Jamais » « On ne change pas les mots de passe » « On ne les a pas renouvelé depuis la création du cabinet »

Deux chirurgiens-dentistes ont répondu qu'ils étaient renouvelés régulièrement.

« Les mots de passe sont changés régulièrement tous les 2 mois » « Nous changeons de mots de passe toutes les fins de mois » « Les mots de passe sont régulièrement renouvelés, particulièrement ceux permettant d'accéder au planning et à la messagerie. »

8) Dites moi en plus sur votre système de sauvegarde de données au cabinet ? Son mode de fonctionnement, sa fréquence, l'opérateur qui en est à l'origine.

Pour cette question, on a pu observé que tous les praticiens avaient une ou plusieurs techniques de sauvegarde.
La sauvegarde par disque dur externe est revenue en grand nombre chez 7 chirurgiens-dentistes.

La sauvegarde double ou triple a été décrite chez un cabinet.

« Concernant le système de sauvegarde, deux disques durs externes sont utilisés. Une sauvegarde quotidienne est effectuée. L'une reste au cabinet, l'autre est stockée au domicile du praticien. Une sauvegarde hebdomadaire est, aussi, réalisée sur un troisième disque dur situé chez les secrétaires »

Une sauvegarde externe au cabinet est conservée chez quatre des praticiens interrogés.

« Je réalise une sauvegarde chaque soir que je ramène à mon domicile »

Le cloud est une option assez peu choisie mais est tout de même utilisée chez un praticien.

« Je suis passé au cloud il y a deux ans, je trouve cela plus pratique que le disque dur à transporter »

Il peut arriver de seulement conserver les données sur l'ordinateur du cabinet. Un seul praticien a décrit réaliser une sauvegarde unique sur l'ordinateur du cabinet.

« Je sauvegarde chaque jour sur l'ordinateur du secrétariat, c'est tout »

9) Que savez vous à propos des cyberattaques dans la profession ?

La majorité des praticiens ne connaissent pas les risques de cyberattaques dans la profession. Ils ont été six à a avouer ne rien connaître sur le sujet.

« Je ne savais pas que les cabinets dentaires étaient des cibles » « Avant votre demande d'entretien, je n'y avais jamais réfléchi ni entendu parlé »
Quatre praticiens interrogés sont conscients de la menace cybercriminelle mais se sentent impuissants en cas d'attaques.

« Les cyberattaques sont un sujet connu du cabinet. Je connais des confrères touchés. La conscience de la menace est là, mais je me sens impuissant si jamais une attaque devait se produire. »

10) Que pensez-vous de l'importance de la menace cyber criminelle aujourd'hui dans la profession ?

Les chirurgiens-dentistes interrogés sont pour la plupart pas très concernés par le sujet et ne pensent pas que ce soit un véritable risque.

« Je pense que mon cabinet de campagne n'est pas prêt d'être concerné » « Ce sont des problématiques de cabinet de ville » « Selon moi, c'est rare, ce n'est pas chose courante »

11) Que pensez-vous de votre niveau de formation sur le sujet ? Pensez-vous avoir besoin de conseils en la matière ?

La majorité des praticiens estime leurs connaissances sur le sujet comme insuffisantes. Sept d'entre eux ont indiqués ne pas en savoir assez.
Trois ont fait part de leur demande de formation supplémentaire sur la cybersécurité.

« On nous en parle très peu, il devrait y avoir plus de congrès à ce sujet » « Je ne m'y connais pas assez pourtant c'est intéressant d'en savoir plus pour mieux se protéger » « Le niveau de formation et communication sur le sujet mériterait d'être relevé. Je ne sais pas vers quels organismes me tourner. Il y a des lois mises en places mais pas de réel accompagnement pour les appliquer correctement. »

Un praticien isolé a jugé ses connaissances suffisantes.

« Je me protège en faisant mes sauvegardes et changeant mes mots de passe, ça devrait suffire »

Un autre cas a fait part de la non nécessité d'en apprendre plus sur le sujet (N=1).

« Je ne pense pas avoir besoin d'en savoir plus, je ne me sens pas concerné »

4.4 Discussion

4.4.1 Analyse thématique

Cette enquête avait pour but d'évaluer le niveau de connaissances des praticiens sur la menace cybercriminelle au cabinet dentaire et leurs pratiques quotidiennes d'hygiène numérique.

4.4.1.1 La place de l'informatique au cabinet

La grande majorité des chirurgiens-dentistes interrogés considère l'informatique comme indispensable au cabinet dentaire. Néanmoins, seulement la moitié d'entre eux a connaissance de la loi RGPD. Pour rappel, le Règlement Général de Protection des Données est en vigueur depuis le 25 mai 2018. Le chirurgien-dentiste doit informer ses patients qu'il collecte et traite des données personnelles. Il oblige les chirurgiens-dentistes à informer leurs patients de la collecte et du traitement de leurs données personnelles et à assurer la sécurité de ces données (47). Il convient de s'interroger sur la diffusion de l'information et le faible niveau de sensibilisation des professionnels du la santé bucco-dentaire à cette loi.

Bien que la plupart des praticiens interrogés considère l'informatique au cabinet comme indispensable, seulement quelques-uns ont embauché un sous-traitant informatique qualifié pour s'occuper de cette partie cruciale.
Cela dénote un possible manque de prise de conscience des dangers liés à l'informatique. Manier ces installations demande des connaissances spécifiques, qui appartiennent à un métier à part entière dans le domaine de la cybersécurité.

4.4.1.2 Les pratiques d'hygiène numérique

Il est possible de constater qu'un certain nombre des cabinets dentaires interrogés n'a pas recours aux mots de passes personnalisés. Chirurgien-dentiste, assistante et secrétaire utilisent le même au sein de la structure. Il n'y a donc aucun moyen d'identifier les différents utilisateurs et leurs connexions.
La majorité des cabinet a un mot de passe personnalisé par praticien pour les différencier. Peu d'assistantes et secrétaires ont en revanche un mot de passe personnalisé. Dans un soucis de traçabilité et de sécurité, il est ainsi primordial que chaque membre du personnel ayant accès à l'informatique ait ses propres identifiants et codes personnalisés.
L'enquête a également révélé que peu de chirurgiens-dentistes renouvellent leurs mots de passe régulièrement. La majorité d'entre eux ne renouvelle jamais leur mot de passe. La statistique montre que ce n'est pas un évènement anecdotique.

Un des conseils de base en cybersécurité est de renouveler les mots de passe régulièrement. Ceci n'est pas appliqué en pratique. C'est un axe d'amélioration évident à mettre en lumière afin d'augmenter la prévention contre la cybercriminalité. Cela interroge encore sur le manque de prise de conscience et de sérieux de la part des praticiens concernant l'hygiène numérique.

Pour ce qui est des méthodes de sauvegarde, la plupart a recours au disque dur externe. Or, le disque dur externe reste un élément fragile qui peut être endommagé, volé ou piraté. Il est important de faire plusieurs sauvegardes et de les conserver dans des lieux différents. Seulement un seul des praticiens double ou triple ses sauvegardes. Un seul d'entre eux, également, sauvegarde uniquement sur l'ordinateur même. Il n'y a donc aucune protection ni garantie si celui-ci est compromis ou simplement victime d'une panne. Un certain nombre possède une sauvegarde externe au cabinet, ce qui est conseillé. Il est important de désigner une personne responsable des sauvegardes et que celles-ci soient régulières : journalières ou hebdomadaires.

Un praticien de l'étude a également recours au Cloud. Cela semble pertinent mais périlleux car à risque de hacking.
Enfin, la dernière partie de l'entretien portait sur une auto-évaluation du praticien concernant ses connaissances sur la menace cybercriminelle dans la profession. La majorité admet avoir un niveau de formation insuffisant dans le domaine. Mais peu sont en demande de formation sur le sujet. Cela interroge à nouveau sur l'importance que les praticiens donnent à ce danger pour leur cabinet.

Il est alarmant de constater que de nombreux cabinets dentaires ne prennent pas les mesures nécessaires en matière d'hygiène numérique. Il est nécessaire de prendre au sérieux la menace cybercriminelle et de se conformer à la loi RGPD pour protéger les données sensibles des patients.
Il est également important de sensibiliser et de former le personnel sur les risques de cyberattaques et sur les mesures de sécurité à mettre en place. Il est crucial de mettre en place des formations et des organismes spécialisés pour aider les praticiens à renforcer leur sécurité numérique et à respecter la législation en vigueur.

4.4.2 Limites de l'étude

Cette étude qualitative comporte néanmoins des limites.

Tout d'abord, concernant notre panel. Celui-ci est constitué de seulement 10 praticiens répartis dans 2 régions de la France. Il aurait été intéressant d'élargir l'enquête à d'autres régions. En effet, j'ai eu l'occasion d'interroger plus de chirurgiens-dentistes en milieu rural qu'en milieu urbain. J'ai pu remarquer que les praticiens de ville semblent un peu plus sensibilisés à ce sujet que les praticiens de campagne.

Cela aurait été également pertinent de comparer les résultats de cette enquête qualitative à une enquête quantitative portant sur le même sujet. Un questionnaire similaire mais diffusé à un plus grand nombre de participants afin d'affirmer ou de questionner les résultats de cette étude qualitative.

Concernant le questionnaire, les questions ouvertes n'étaient pas toujours très claires pour les praticiens interrogés, particulièrement les questions 3 et 9. Il a fallu parfois préciser et poser des questions plus ciblées afin d'avoir des réponses.
Après quelques entretiens, la pertinence de certaines questions s'est révélée absente. Le questionnaire a donc été modifié. Les questions concernant la traçabilité numérique et l'expérience personnelle du praticien dans le domaine de la sécurité informatique ont été supprimées.

Également, il aurait été intéressant d'avoir parmi les chirurgiens-dentistes interrogés, des praticiens ayant eu l'expérience d'une activité cybercriminelle. Malheureusement, l'expérience est désagréable et traumatisante, ce qui peut rendre difficile d'en parler. J'ai contacté à cet effet plusieurs praticiens ayant été précédemment victimes d'attaques par ransomware, mais aucun d'entre eux n'a souhaité répondre à mes questions malgré la garantie de l'anonymat.

5. Guide pour la lutte contre la cybercriminalité

5.1 Fiche pratique ludique

Des recommandations simples et utiles ont été regroupées sous forme de fiche pédagogique. Le but de cette fiche réalisée par mes soins est d'être diffusée aux professionnels de santé afin de sensibiliser aux risques de la cybercriminalité.

Figure 7 : Fiche récapitulative des 5 conseils simples pour se protéger de la cybercriminalité

5.2 Analyse d’impact

L’analyse des risques se nomme aussi dans le domaine : Analyse d’Impact relative à la Protection des Données (AIPD). D’après la CNIL, celle-ci se définit par l’étude qui doit être menée lorsqu’un traitement de données personnelles est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes concernées.

C’est l’une des actions importantes à effectuer régulièrement. Elle permet d’évaluer l’efficacité des moyens mis en oeuvre contre la cybercriminalité et de mettre en lumière les failles et les points à améliorer. Les AIPD ne sont pas obligatoires mais fortement recommandées.

La CNIL fournit un logiciel qualifié de « prêt à l’emploi » pour créer son AIPD selon une méthode testée et validée. Il y a principalement 3 grands risques mis en exergue par les analyses d’impact : l’accès illégitime aux données, leur modification non désirée et enfin leur disparition.

La CNIL met également à disposition une grille d’auto-évaluation pour évaluer le niveau de sécurité des données personnelles.

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

	FICHES	MESURE	
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manière sécurisée	☐
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	☐
		Prévoyez les conditions de restitution et de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

Figure 8 : Grille d'auto-évaluation fournie par la CNIL pour créer son AIPD

5.3 Sécurité informatique

5.3.1 Les serveurs

Les serveurs sont le centre regroupant toutes les données du cabinet.
Il est recommandé de limiter les accès Internet et les flux réseaux au strict nécessaire en bloquant les services non nécessaires.

5.3.2 Le réseau Wifi

Chiffrer les réseaux Wi-Fi et séparer le réseau invité du réseau interne.
Ne pas utiliser de réseau wifi avec chiffrement Wired Equivalent Privacy (WEP) mais plutôt du Wifi Protected Access (WPA2) ou WPA2-PSK.

WEP, WPA2 ou WPA2-PSK sont des protocoles de sécurité Wi-Fi qui assurent la sécurité des connexions sans fil. Leur rôle est de masquer les données et de protéger les communications pour empêcher les pirates d'accéder aux réseaux. Le WEP est le plus courant et ancien protocole de sécurité. De nombreuses failles à son propos ont été découvertes depuis 1999. En 2003, le WPA a été lancé pour pallier aux vulnérabilités du WEP. Le WPA chiffre les données à une vitesse de 256 bits, alors que le WEP peut aller jusqu'à 128 uniquement (48).

Il est important d'utiliser des protocoles de sécurité du courrier électronique. Il se produit régulièrement des échanges entre les patients, autres professionnels de santé ou les fournisseurs. Il faut sécuriser ces échanges.
Pour cela on peut utiliser différents protocoles de sécurité.

Le Simple Mail Transfer Protocol (SMTP) est utilisé pour chiffrer les échanges de messages entre les clients et les serveurs. Il fonctionne comme l'HTTPS c'est à dire qu'il utilise le Transport Layer Security (TLS) pour chiffrer les flux du trafic réseau. Il n'est pas invoqué directement dans le courrier électronique mais est utilisé pour le trafic web et chiffre donc la messagerie web.

L'Internet Message Access Protocol (IMAP), quant à lui, permet d'accéder aux courriers électroniques sans les télécharger ou les stocker sur l'ordinateur d'après Microsoft (48).

5.3.3 L'utilisation d'un VPN

Un Virtual Private Network (VPN) est un réseau privé virtuel qui permet de chiffrer le trafic Internet avant que celui-ci soit renvoyé au fournisseur d'accès internet. Ainsi, les données proviennent du serveur VPN et non directement de notre serveur, renforçant ainsi la confidentialité.
Utiliser un protocole de sécurité du type WPA2 combiné à un VPN permet de protéger efficacement le réseau local du cabinet contre les intrusions et les failles.

Il est également possible d'utiliser des systèmes de détection d'intrusion pour être prévenu des attaques.

5.3.4 La séparation locale des réseaux

Un réseau informatique peut se cloisonner.
Pour faciliter la compréhension du principe on peut comparer cela à une chaine avec des maillons. Le cabinet possède plusieurs chaines, soit plusieurs ordinateurs. Donc, quand un maillon, un ordinateur, est infecté par un virus, ce virus reste dans le réseau local de l'ordinateur. Le cloisonnement des réseaux permet aux autres ordinateurs de ne pas être touchés par le virus.

Cette méthode est technique à mettre en place, surtout au sein d'un cabinet dentaire. Il faut obligatoirement communiquer avec le serveur fourni par le prestataire du LGO. Il est donc conseillé de faire appel à un professionnel de la sécurité informatique pour sécuriser le réseau, plutôt que d'avoir des ordinateurs reliés entre eux sans fractionnement (49).

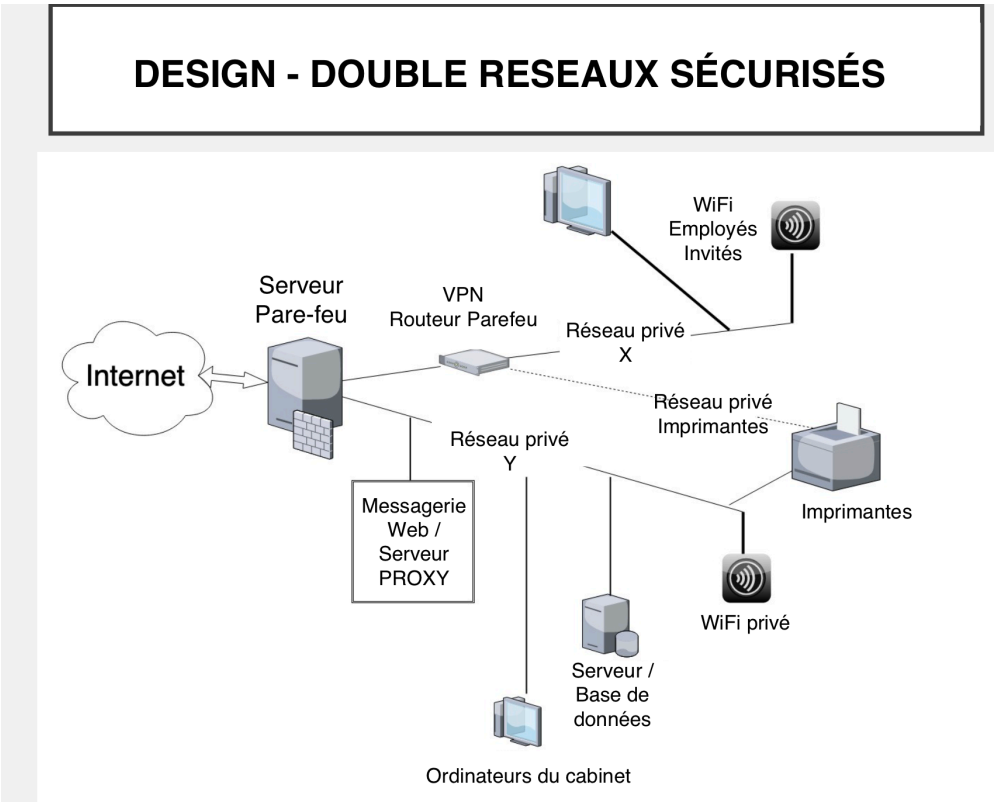


Figure 9 : Représentation du fractionnement d'un réseau informatique sécurisé traduite depuis le congrès de la sécurité informatique des bureaux mené à San Diego en septembre 2019 (49)

5.3.5 Les antivirus

Un antivirus est un logiciel capable de détecter les virus informatiques et de les éliminer d'après Le Robert (50). Il est un indispensable pour une structure de santé. Il existe globalement six grands éditeurs d'antivirus qui possèdent 60% du marché, dont Norton et Avast. C'est au praticien de comparer, en termes de tarifs et de services par rapport à la structure de son cabinet, quelle formule lui conviendrait le plus. Il n'y a pas de grandes différences d'efficacité entre les différents antivirus. Cependant, il faut être vigilant car les antivirus peuvent parfois détecter des faux positifs et bloquer, par exemple, un logiciel qui n'est pourtant pas un virus. Ce genre d'erreurs arrive régulièrement pendant les mises à jours.Cela constitue une faille car l'utilisateur désactive momentanément l'antivirus pour effectuer une mise à jour, par exemple, laissant la porte ouverte à une attaque malveillante.

Le plus simple est d'établir une liste blanche accessible par le biais des réglages, dans laquelle on répertorie les fichiers et logiciels que l'on veut exclure de l'analyse de l'antivirus. Cette faille sera alors bien moins importante que la désactivation complète de l'antivirus pendant la mise à jour (51).

5.3.6 Les systèmes d'exploitation

Les systèmes d'exploitation obsolètes sont à bannir, il est important d'adapter son système d'exploitation aux besoins du métier. Microsoft Windows ou Apple OS sont défectueux, les hackers ont déjà écrit des programmes pour exploiter ces systèmes qui sont les plus utilisés. Linux n'est pas plus sécurisé mais comporte moins d'utilisateurs et serait donc statistiquement moins attaqués (51).

Il est conseillé d'installer un pare-feu sur le routeur et chaque poste de travail.
Il convient également d'effectuer régulièrement les mises à jours des logiciels et des navigateurs car ils sont exposés au web. Il existe des analyses de vulnérabilité sous forme d'audits car les virus sont souvent basés sur des failles de sécurité des systèmes d'exploitation.

5.3.7 Les mises à jour

Les recommandations sont les suivantes :

- Programmer et automatiser les MAJ qui peuvent être longues.
- Harmoniser les logiciels et les versions de ceux-ci sur l'ensemble du parc informatique.
- Limiter les installations et utilisations d'applications, ainsi que la navigation sur Internet.
- Toute action sur le système informatique doit être expliquée et documentée dans des référentiels auxquels le membre du personnel puisse se référer.

5.3.8 La charte informatique

Il convient de rédiger une charte informatique pour rappeler les règles élémentaires.

Cette charte doit permettre de rappeler comment utiliser les ressources informatiques aux utilisateurs et comment éviter la fraude cybercriminelle avec l'application interne de la loi RGPD.
Celle-ci doit être lisible et compréhensible, donner des définitions claires et précises, et être signée par les protagonistes du cabinet.
Elle doit mentionner les éléments suivants : son objet et sa portée, les usages permis des moyens informatiques, les règles de sécurité en vigueur, les mesures de contrôle prises par l'employeur ainsi que les sanctions encourues en cas de non-respect de la charte.
En complément, il est important de former les utilisateurs à l'aide d'une sensibilisation récurrente pour les faire adhérer aux mesures de base.

5.4 Education des utilisateurs et leur sensibilisation

5.4.1 Sensibilisation

Il faut sensibiliser le personnel du cabinet à l'importance du caractère personnel des données manipulées au quotidien, qui sont liées aux libertés et à la vie privée des patients. On peut réaliser des séances de sensibilisation sous forme de réunions, faire des rappels et envoyer de la documentation par mail.

En parlant de documentation, il est important de tenir à jour et de rendre accessible aux utilisateurs un manuel regroupant les procédures d'exploitation. Toute action touchant à des données à caractère personnel doit être expliquée simplement à travers des fiches que le personnel peut consulter dès qu'il en ressent le besoin.
La charte informatique intervient à ce moment là. C'est un document qui reprend les droits et les obligations du personnel quant à l'utilisation du matériel mis à sa disposition. C'est le premier rempart dans la protection des données dans une entreprise. Elle définit les limites entre vie privée et vie professionnelle et décrit les modalités d'utilisation des réseaux sociaux.

La charte doit également posséder un caractère contraignant et prévoir des sanctions en cas de non-respect des règles établies. Elle dispose donc d'une valeur

juridique. Voici quelques règles de sécurité indispensables qui doivent figurer dans la charte du cabinet dentaire et auxquelles le personnel doit se conformer :

- Signaler et informer le service informatique et/ou la direction de toute intrusion, violation ou tentative de violation et dysfonctionnement.
- Ne pas confier ses identifiants et mots de passe à un tiers.
- Ne pas installer de logiciels sans autorisation.
- Verrouiller son ordinateur lorsque l'on quitte son poste de travail.
- Ne pas tenter d'accéder à des données pour son usage personnel.
- Ne pas se connecter et surfer sur le Web pour son usage personnel, y compris les réseaux sociaux.

5.4.2 L'authentification des utilisateurs

L'authentification apporte la preuve de son identité.

Tout d'abord, il y a le tout premier rempart qui est le mot de passe du poste, de l'ordinateur. Celui-ci permet d'allumer et de démarrer le système d'exploitation. Le plus sécurisé est d'avoir deux comptes utilisateurs : un compte utilisateur simple à utiliser au quotidien et un compte administrateur. L'inconvénient est qu'il faut se connecter au compte administrateur lorsque l'on doit effectuer les mises à jour. La grande force est qu'au quotidien, la session de l'utilisateur simple ne lui permet pas de modifier les configurations systèmes ni d'installer un logiciel qui pourrait être espion ou malveillant.

Cette authentification est le plus souvent réalisée à l'aide du couple login/mot de passe. La première étape est la saisie de l'identifiant, le login, qui doit être unique pour chaque utilisateur. Interdire les comptes partagés fait partie des précautions élémentaires recommandées par la CNIL.

Puis il est temps de rentrer son mot de passe qui doit être confidentiel. Il ne faut jamais révéler son mot de passe, ni le laisser accessible à tous. Il doit être unique, c'est-à-dire qu'un même mot de passe ne doit pas servir pour plusieurs logiciels et il faut choisir un mot de passe robuste.

La robustesse d'un mot de passe est sa capacité à résister à une attaque par des moyens permettant de le deviner ou par « force brute ». Il est déconseillé d'utiliser comme mot de passe un mot courant dans les langues les plus utilisées ou un des mots de passe utilisés très couramment comme « azertyuiop ». La CNIL recommande d'utiliser un mot de passe de 12 caractères minimum et 4 types de caractères différents, d'en changer régulièrement, au moins tous les 3 mois, et de ne jamais utiliser 2 fois les mêmes mots de passe.

Le moyen mnémotechnique le plus simple pour créer des mots de passes complexes est de ne conserver que les premières lettres des mots d'une phrase. Par exemple, la phrase *« un Chef d'Entreprise averti en vaut deux »* peut correspondre au mot de passe « 1Cd'Eaev2 ».

Il ne faut pas communiquer son mot de passe à autrui, ne pas noter son mot de passe dans un fichier, sur un post-it ou un papier facilement accessible, ne pas enregistrer les mots de passes sur le navigateur, ni conserver les mots de passe par défaut. Il est recommandé de ne pas utiliser un de mot de passe ayant un lien avec soi-même.

Pour garantir l'authentification des utilisateurs, il est recommandé de définir des règles de connexions et de déconnexions. Les principales sont :

- Ne pas se connecter avec le même code utilisateur sur plusieurs postes en même temps.
- Limiter le nombre de tentatives d'accès : en général, trois essais erronés bloquent l'accès temporairement.
- Activer la déconnexion automatique en fin de traitement par un utilisateur.
- Activer la déconnexion automatique après une période d'inactivité définie.
- Redémarrer conduit à la page d'identification.
- Imposer un renouvellement de mot de passe selon une périodicité pertinente et raisonnable.

- Installer un système d'horodatage participant à la sécurité des comptes en affichant la date et l'heure de la dernière connexion.

5.5 Archivage et Sauvegarde des données

5.5.1 Archivage

Concernant les données médicales, il existe deux méthodes de conservation des dossiers patients. Soit les dossiers sont conservés au sein du cabinet dentaire, soit ils sont dématérialisés et stockés chez un hébergeur agrée. La deuxième option n'est possible que pour les données informatiques. La durée de conservation est de 20 ans à compter de la date de la dernière consultation.

Lorsqu'il s'agit d'un patient de moins de 28 ans, la conservation est prolongée jusqu'à la date du 28ème anniversaire. Enfin, si le patient décède moins de 10 ans après sa dernière consultation, on doit conserver encore 10 ans à compter de la date de décès les données.

Il est donc important de définir une méthode de gestion des archives et de mettre en oeuvre des modalités d'accès à ces archives. Par rapport à la suppression des données, il faut choisir un processus garantissant l'intégralité de la destruction de l'archive. Pour cela, on peut effectuer une destruction physique par écrasement, incinération ou broyages des disques durs, une démagnétisation ou un effacement par réécriture. Il est intéressant d'utiliser des logiciels dédiés à la suppression des données certifiés par l'Agence Nationale de la sécurité des systèmes d'information (ANSSI).

Il faut choisir des supports garantissant une longévité suffisante et choisir un service ou des personnes spécifiques chargées d'y accéder.

5.5.2 Sauvegarde

L'objectif de la sauvegarde des données est leur récupération en cas de contentieux ou d'évènement indésirable. La sauvegarde permet de créer une copie de sûreté des données informatiques à un instant précis. Les sauvegardes servent à restaurer le système avec le moins de perte de données possible afin d'assurer la continuité de l'activité du cabinet malgré une panne. Il est donc indispensable de sauvegarder régulièrement et de stocker ces sauvegardes dans un lieu sécurisé. Il peut être plus facile d'imposer une sauvegarde quotidienne, hebdomadaire ou à un intervalle régulier et de la stocker hors du cabinet. On ne conserve pas les sauvegardes au même endroit que les serveurs. Il faut chiffrer les sauvegardes pour assurer leur confidentialité et vérifier leur intégrité régulièrement.

5.5.3 Traçabilité

La traçabilité est importante. Tracer les accès permet d'identifier plus facilement un accès frauduleux ou une utilisation abusive de données personnelles ou de déterminer l'origine d'un incident. Il est donc important d'enregistrer certaines des actions effectuées sur le système informatique du cabinet.

5.5.4 Prévoir un système de journalisation

Un système de journalisation permet de tracer les activités des utilisateurs, les anomalies et les événements liés à la sécurité sous format de « fichiers journaux », aussi appelés« logs », qui doivent être conserver sans être altérés pour une période de temps raisonnable. En principe, la durée de conservation des données de journalisation est comprise entre six mois et un an afin de trouver un juste équilibre entre l'identification des incidents et le poids du stockage des données.

Ces fichiers journaux contiennent au minimum les accès des utilisateurs, y compris leurs identifiants, la date et l'heure de leur connexion et de leur déconnexion. Dans certains cas, il peut être utile de stocker d'autres données, comme le détail des actions effectuées par l'utilisateur et les types de données consultées.

On peut les comparer à l'historique d'un navigateur web mais valable pour toutes les actions effectuées sur les ordinateurs du cabinet.
Les « fichiers journaux » doivent être régulièrement consultés pour détecter d'éventuelles anomalies ou incidents de sécurité. Ils ne doivent pas être détournés à d'autres fins incompatibles, comme le suivi du temps de travail des salariés, par exemple.

5.5.5 Protéger ce système de journalisation

Ne pas rendre ce système de journalisation accessible aux personnes dont l'activité est enregistrée, afin de ne pas leur donner l'opportunité de supprimer leurs traces.

5.5.6 Informer les utilisateurs

Il est important d'informer et de consulter le personnel quant à la mise en place de ce système.

5.5.7 Procédures pour gérer les incidents

En cas de violation des données, il faut notifier toute violation de données à caractères personnel à la CNIL ainsi qu'aux personnes concernées, pour qu'elles puissent limiter les conséquences. Les alertes doivent remonter rapidement pour pouvoir répondre à l'objectif de sécurisation des données. Il est souvent nécessaire d'automatiser les procédures d'alertes en cas d'utilisation non autorisée ou détournée, afin de réagir le plus rapidement possible. La sécurisation doit donc se faire de manière active.

6. Ouverture / Pistes de réflexion / Perspective

Il est évident que les chirurgiens-dentistes ne sont pas suffisamment informés, formés et sensibilisés à l'hygiène numérique. La plupart d'entre eux utilisent quotidiennement un ordinateur et Internet sans en maitriser tous les aspects.

Pourtant, ils sont légalement responsables de la sécurité des données patients. La sécurité informatique est un domaine à part entière qui requiert du temps et une compréhension technique que tous les praticiens ne possèdent pas. Ils ne sont pas qualifiés pour gérer les détails spécifiques nécessaires à la cybersécurité d'un cabinet.

Il serait intéressant de confier la responsabilité de l'hygiène numérique à des spécialistes informatiques dans l'ensemble des cabinets. Cependant, cela implique des coûts financiers et temporels que toutes les structures ne peuvent peut-être pas supporter, ce qui entrave la mise en place des mesures de cybersécurité efficaces.

Ces éléments expliquent pourquoi, malgré le cadre législatif et les recommandations de l'Europe et du RGPD, les mesures de protection des données numériques dans les cabinets dentaires restent insuffisantes. La priorité devrait être de créer des outils pour former et sensibiliser les chirurgiens-dentistes à cette problématique, ainsi que de réfléchir au financement de l'installation et du maintien des règles de sécurité.

Il serait opportun d'intégrer dans la formation professionnelle continue à l'université un module sur ce sujet, notamment lors des séminaires de 6ème année, afin que les jeunes praticiens soient vigilants et conscients de cette menace croissante et complexe.
En effet, même les chirurgiens-dentistes récemment diplômés, bien que plus enclins à être à l'aise avec les outils informatiques, semblent ne pas être plus au courant que les praticiens en exercice depuis des années. Il y a peu de mention de notions d'hygiène numérique à la faculté.

Conclusion

Cette enquête a permis de dresser un premier état des lieux des connaissances des praticiens concernant les menaces cyber criminelles, mettant en évidence diverses pistes d'amélioration. La cybersécurité est sous-estimée dans la profession, et les chirurgiens-dentistes ne sont pas suffisamment conscients ni sensibilisés sur le sujet.

Les entretiens ont révélé qu'un dentiste sur deux n'était même pas au courant de l'existence de la loi RGPD, qui les oblige pourtant à prendre en charge la protection des données sensibles de leur patientèle. De plus, 80% d'entre eux ont admis ne jamais changer leur mot de passe. Ces statistiques témoignent du relâchement généralisé en matière de mesures d'hygiène numérique.

Il est clair que la cybersécurité est un enjeu majeur auquel les praticiens doivent être sensibilisés et informés. Bien que la CNIL mette à disposition de nombreuses ressources en ligne, telles que des fiches conseils pour l'auto-évaluation de la sécurité des structures, cela semble insuffisant compte tenu de la charge de travail restante. Des formations dédiées et un accompagnement plus soutenu des praticiens dans ce domaine seraient donc bénéfiques.

Pour les professionnels de santé, les services numériques sont devenus des outils essentiels dans leur relation avec les patients. Toutefois, malgré les nombreux avantages qu'ils apportent, il est crucial de veiller à ce qu'ils ne compromettent pas la sécurité numérique du cabinet.

La transformation numérique s'intensifie avec l'avènement de technologies émergentes telles que l'intelligence artificielle, l'analyse des données, les blockchains et le cloud computing. Ces avancées accroissent les risques de failles de cybersécurité. Il est donc primordial de comprendre les menaces qui pèsent sur la sécurité numérique lors de l'adoption de nouvelles technologies, afin de prévenir les activités malveillantes et non autorisées des hackers.

Les praticiens doivent adopter des bonnes pratiques au quotidien pour respecter le RGPD et protéger les données de leurs patients, dont ils sont responsables. Pour cela, la mise en place de protocoles rigoureux, une prise au sérieux de la menace et une vigilance constante sont essentielles.

BIBLIOGRAPHIE

1. Romain Charbonnier. (page consultée le 17/09/2024). L'histoire de la cybersécurité. Guardia. 2024. https://guardia.school/boite-a-outils/lhistoire-de-la-cybersecurite
2. Tristan Gaudiaut. (page consultée le 17/09/2024). Le coût de la cybercriminalité dans le monde. Statista. 2024. https://fr.statista.com/infographie/32299/cout-cybercriminalite-dans-le-monde-et-par-pays/
3. Radio Canada. (page consultée le 17/09/2024). Fuite de données : cinq grands scandales des dernières années. 2019. https://ici.radio-canada.ca/nouvelle/1193991/scandale-fuite-vol-renseignements-personnel
4. Pérez Lagos C. Rendre visibles les conséquences de la surveillance numérique. Communication. 2020;37(2).
5. Ludovic Demont. 4000 ans de responsabilité pénale médicale. Revue juridique de l'Ouest. 1999. p. 361-376.
6. Edouard Hu. Etude historique et juridique sur la responsabilité du médecin.Thèse Droit.Paris.1880.p. 2.
7. Berche P. Le savoir vagabond. Paris: Éditions de la Santé; 2013. p. 186-191.
8. Hess V. Formalizing observation: The emergence of the modern patient record exemplified by Berlin and Paris medicine, 1725-1830. Medizinhistoriches Journal. 2010;45(3-4):293-340.
9. Wulff HR, Jungersen K. A Danish provincial physician and his patients; the patient records from the practice of Christopher Detlev Hahn in Aarhus around 1800. Medizinhistoriches Journal. 2005;40(3-4):321-45.
10. Lorkowski J, Pokorski M. Medical Records: A Historical Narrative. Biomedicines. 2022;10(10):2594.
11. Haute Autorité de Santé. (page consultée le 09/06/2023). Le dossier médical en santé au travail (DMST). 2009. https://www.has-sante.fr/jcms/c_757826/fr/le-dossier-medical-en-sante-au-travail
12. Julie Solutions. (page consultée le 14/06/2023). Julie Solutions crée une expérience client personnalisée et unique. Organisation du cabinet. 2022. https://www.julie.fr/

13. Julie Solutions. (page consultée le 14/06/2023). Solutions digitales pour la performance des cabinets dentaires et la qualité des soins. 2022. https://www.julie.fr/
14. Julie Solutions. (page consultée le 14/06/2023). Le numérique en santé : Julie Solutions au service du plan Ma Santé 2022. Information Dentaire. 2020.
15. Sesam-Vitale. (page consultée le 16/05/2023) https://www.sesam-vitale.fr/
16. Juppé A. Ordonnance n° 96-346 portant réforme de l'hospitalisation publique et privée. Legifrance. 1996.
17. Assurance Maladie Améli. (page consultée le 14/06/2023). Notre histoire. 2023. https://www.assurance-maladie.ameli.fr/qui-sommes-nous/histoire
18. Eggmann F, Weiger R, Zitzmann NU, Blatz MB. Implications of large language models such as ChatGPT for dental medicine. Journal of Esthetic and Restorative Dentistry. 2023;35(7):1098-1102.
19. Alhaidry HM, Fatani B, Alrayes JO, Almana AM, Alfhaed NK. ChatGPT in Dentistry: A Comprehensive Review. Cureus. 2023;15(4)
20. Sallam M. ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns. Healthcare (Basel). 2023;11(6):887.
21. Jouanna J. Hippocrate. Paris: Librairie Arthème Fayard; 1992. annexe I.
22. Petit EP. Le Serment d'Hippocrate, source de l'éthique médicale. La Presse Médicale. 2002;31(2):52-96.
23. Code de la Santé Publique. Première Partie. Article L1110-4 modifié par LOI n°2021-1017 - art. 14. 2021.
24. Vassal JP. Le secret professionnel aujourd'hui. Information dentaire. 2017.
25. Code de la Santé Publique. Section 2 : Code de déontologie des chirurgiens-dentistes (Articles R4127-201 à R4127-284). 2021.
26. Markus JP. Secret Professionnel du chirurgien dentiste. EMC Odontologie. 2007.
27. La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 64. Legifrance gouvernement.
28. Vie Publique. (page consultée le 10/06/2023) RGPD : règlement général sur la protection des données, de quoi s'agit-il ? https://www.vie-publique.fr/eclairage/19588-rgpd-reglement-general-sur-la-protection-des-donnees-de-quoi-sagit-il

29. IBM. (page consultée le 31/05/2024). Qu'est ce qu'une cyberattaque ? https:// www.ibm.com/ fr-fr/topics/cyber-attack
30. Larousse. (page consultée le 05/02/2024). Définition de «hacker». https:// www.larousse.fr/dictionnaires/francais/hacker/38812
31. Cybermalveillance.gouv.fr. (page consultée le 14/03/2024). Comment signaler un mail de phishing ou d'hameçonage ? 2021. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actuali tes/comment-signaler-un-mail-de-phishing
32. Cybermalveillance.gouv.fr. (page consultée le 14/03/2024) Qu'est-ce qu'un ransomware ou rançongiciel ? 2022. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-rancongiciel-definition
33. Cybermalveillance.gouv.fr. (page consultée le 14/03/2024). Quels sont les différents types de piratage informatique ? 2022. https://www.cybermalveillance. gouv.fr/tous-nos-contenus/actualites/quels-sont-les-differents-types-de-piratage-informatique
34. Cybermalveillance.gouv.fr. (page consultée le 14/03/2024). Défiguration de site internet, que faire ? 2020. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/ fiches-reflexes/defiguration-de-site-internet
35. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technology Health Care. 2016;24(1):1-9
36. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology Health Care. 2017;25(1):1-10.
37. Sendelj R, Ognjanovic I. Cybersecurity Challenges in Healthcare. Studies Health Technology Informatics. 2022;300:190-202.
38. Coret S. Les cyberattaques mondiales ont augmenté de 38% en 2022. CheckPoint France. 2023.
39. Mennecier D. Cyberattaques et hôpital. Sécurité et hôpital Pandémie Covid-19. 2020;4(4):327-30.
40. Association Dentaire Française. La santé, nouvelle cible des cybercriminels. Dental Tribune, 2023.
41. Union Dentaire. Cyberattaque au cabinet dentaire : agissez vite ! 2022.

42. Les cyberattaques du secteur santé auraient augmenté de 191 % en 2022. Ortho Magazine. 2023;29(164):5.
43. CERTFR 2023. (page consultée le 14/03/2024). ANSSI Panorama de la cybermenace en 2022. https://www.cert.ssi. gouv.fr /uploads/CERTFR-2023-CTI-001.pdf
44. Albo C. Cybercriminalité : des cabinets médicaux de Gironde contraints de payer une rançon à des hackers. Journal France Info. 2022.
45. Durietz D. (page consultée le 14/06/2023). Interview croisée. Julie Solutions. 2020. https://www.julie.fr/temoignage-dr-durietz-masauvegarde-2020/
46. Baker, S. E., & Edwards, R. How many qualitative interviews is enough. 2012.
47. URPS. (page consultée le 14/03/2024). RGPD pour les cabinets dentaires, que dit la loi ? 2022.https://urps-cd-idf.com/rgpd-pour-les-cabinets-dentaires-que-dit-la-loi/
48. Loshin P. What are the most important email security protocols? Tech Target. 2023.
49. Office Network Security. (page consultée le 10/06/2023). How to do it. 2019. https://officenetworksecurity.com
50. Le Robert. (page consultée le 09/03/2024). Dictionnaire. https://dictionnaire.lerobert.com
51. Caruso RD. Personal computer security: part 1. Firewalls, antivirus software, and Internet security suites. Radiographics. 2003;23(5):1329-37.

ANNEXE 1

Le guide d'entretien

Intro présentation de l'étude

Cette étude vise à décrire les pratiques actuelles d'hygiène numérique et de sécurité informatique dans les cabinets dentaires. L'entretien du jour a pour but de recueillir votre témoignage personnel qui sera accueilli sans jugement puis anonymisé dans le cadre de l'écriture de ma thèse. Cet entretien d'une dizaine de minutes sera semi-dirigé à travers des questions ouvertes, neutres et faciles à comprendre. Libre à vous de répondre ou non à une question bien que le plus de transparence observé sera bénéfique à cette étude. Je vous remercie de m'accueillir.

Consentez-vous au recueil des réponses et à l'enregistrement audio ou vidéo des données de cet entretien ? Oui / Non

Trame des questions (11)

1) Quelle est la place de l'informatique actuellement dans votre cabinet dentaire ?
2) Connaissez vous la loi RGPD ?
3) Si oui, comment se passe la mise en pratique de la RGPD dans votre cabinet ?
4) Avez-vous embauché un sous traitant informatique ?
5) Est ce que chaque membre du personnel du cabinet a accès aux outils informatiques ?
6) Les différents membres du cabinet ont-ils des identifiants et code d'accès personnalisés pour pouvoir utiliser les logiciels ?
7) A quelle fréquence les mots de passe sont-ils renouvelés ?
8) Dites moi en plus sur votre système de sauvegarde de données au cabinet ? Son mode de fonctionnement, sa fréquence, l'opérateur qui en est à l'origine.
9) Que savez vous à propos des cyberattaques dans la profession ?
10) Que pensez-vous de l'importance de la menace cyber criminelle aujourd'hui dans la profession ?
11) Que pensez-vous de votre niveau de formation sur le sujet ? Pensez-vous avoir besoin de conseils en la matière ?

université de BORDEAUX

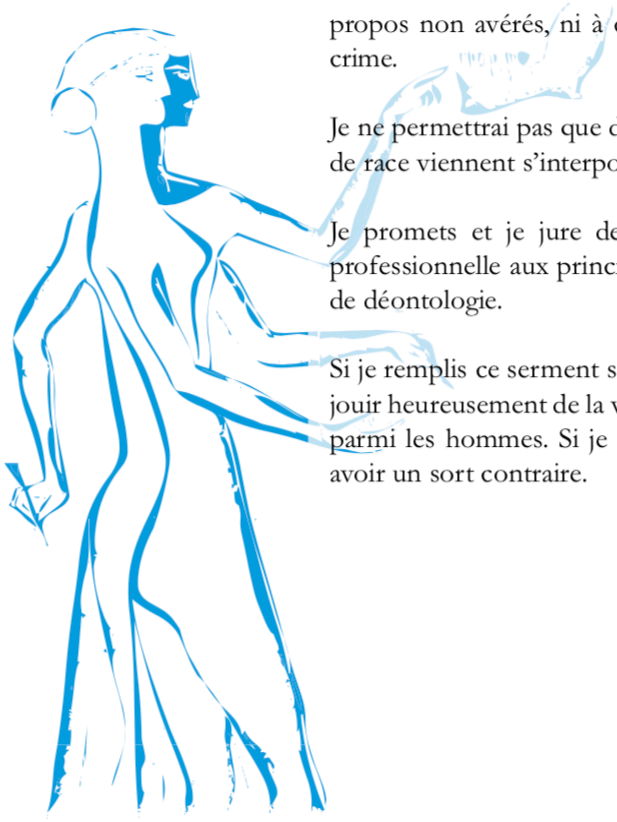
Collège des Sciences de la Santé

UFR des Sciences Odontologiques

Serment

En présence de mes Maîtres et de mes condisciples, je promets et je jure d'être fidèle aux lois de l'honneur et de la probité dans l'exercice de l'art dentaire.

Je donnerai mes soins gratuits à l'indigent et n'exigerai jamais un honoraire au-dessus de mon travail. Ma langue taira les secrets qui me seront confiés. Admis à l'intérieur des maisons, mes yeux ne verront pas ce qui s'y passe.
Mes connaissances et mon état ne serviront ni à diffuser des propos non avérés, ni à corrompre les mœurs, ni à favoriser le crime.



Je ne permettrai pas que des conditions de croyance, de nation et de race viennent s'interposer entre mon devoir et mon patient.

Je promets et je jure de conformer strictement ma conduite professionnelle aux principes et aux règles prescrites par le code de déontologie.

Si je remplis ce serment sans l'enfreindre, qu'il me soit donné de jouir heureusement de la vie et de ma profession, honoré à jamais parmi les hommes. Si je le viole et que je me parjure, puissé-je avoir un sort contraire.

Vu, Le Président du Jury,

Date, Signature :

Vu, la Directrice de l'UFR des Sciences Odontologiques,

Date, Signature :

Vu, le Président de l'Université de Bordeaux,

Date, Signature :

Titre : L'HYGIÈNE NUMÉRIQUE AU CABINET DENTAIRE, évaluation des pratiques professionnelles.

Résumé : Les cabinets dentaires subissent une transition vers le numérique depuis quelques années. Les processus sont de plus en plus informatisés, ce qui laisse la porte ouverte aux hackers qui ciblent plus régulièrement le système de santé. L'attaque la plus courante au niveau des cabinets dentaires est le blocage et le vol des données en échange d'une rançon. Le RGPD rend responsable le chirurgien dentiste de la protection des données patients qui sont considérées comme sensibles. L'objectif était de réaliser une évaluation des pratiques professionnelles afin de rendre compte des moyens mis en oeuvre pour respecter le RGPD et se protéger des cyberattaques. Globalement, un manque de formation et de prévention a pu être constaté. Il serait nécéssaire d'en apprendre plus à la faculté pour les jeunes praticiens et de former plus sérieusement les équipes qui pratiquent déjà.

Mots clés : hygiène numérique, cybersécurité , ransomware

Title: DIGITAL HYGIENE AT DENTAL CLINIC, an evaluation of professional practices.

Abstract: Dental clinics have been transitioning into digital the past few years. Computers are taking part of a lot of processes leading to a new breach for hackers. Medical system is now a frequent target especially by ransomware, one of the most common type of attack. In the law, dentists must protect their patients data. The goal here was to realize an evaluation of professional practices to see how dentists are handling the cybersecurity risks and how they stay digital clean at their office. Results found mostly a lack of knowledge and actions. It will be important to strengthen the prevention, inform the young dentists at the university and do courses to already practitioners.

Keywords: digital hygiene, cybersecurity, ransomware