UNIVERSITÉ DE LA RÉUNION

**UFR SANTÉ**

Année : 2020 N° : 2020LARE007M

THÈSE POUR LE DIPLÔME D'ÉTAT DE DOCTEUR EN MÉDECINE

# Étude descriptive de la maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de santé de leurs patients, à l'Île de la Réunion en 2019.

Présentée et soutenue publiquement le 27 février 2020 à 19h00 à la Réunion

**Par Monsieur Léo LAVAUD**

Né le 11 janvier 1990 à PARIS XIVe

**Directeur de Thèse :** Monsieur le Docteur Michel BOHRER

**Rapporteur de thèse :** Madame le Docteur Jessica DUMEZ

**Membres du jury**

– Monsieur le Professeur Jean-Marc FRANCO : Président du jury

– Monsieur le Docteur Bernard-Alex GAÜZÈRE : Assesseur

– Monsieur le Docteur Sébastien LERUSTE : Assesseur

# Table des matières

# Abréviations

| | |
|---|---|
| ANSII : | Agence Nationale de la Sécurité des Systèmes d'Information |
| ASIP Santé : | Agence des Systèmes d'Information Partagés de Santé |
| CNIL : | Commission Nationale de l'Informatique et des Libertés |
| CNOM : | Conseil National de l'Ordre des Médecins |
| CPS : | Carte de professionnel de santé |
| DMP : | Dossier médical partagé |
| DPS : | Données personnelles de santé |
| HAS : | Haute Autorité de Santé |
| IC : | Intervalle de confiance |
| MSS : | Messagerie sécurisée de santé |
| OS : | *Operating System* / Système d'exploitation |
| RGPD : | Règlement général sur la protection des données |
| URML-OI : | Union Régionale des médecins libéraux de l'océan Indien |

# I. Introduction

En 2017, 96 % des médecins généralistes déclaraient disposer d'un logiciel informatique pour la gestion des patients et considéraient que la perte de confidentialité est le principal risque associé aux technologies numériques (89 %). Ce risque était jugé plus important que l'inégalité d'accès aux soins (72 %) et que la déshumanisation de la relation médecin-patients (71 %) (1).

Les possesseurs d'un logiciel médical ont sous leur responsabilité les données personnelles de santé (DPS) de leurs patients. Ils sont tenus de prendre toutes précautions utiles pour préserver la sécurité de ces données. Ces précautions visent à empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (2).

Ces DPS sont des données dites « sensibles ». La loi informatique et liberté interdit leur collecte ou leur traitement sans autorisation de la Commission Nationale de l'Informatique et des Libertés (CNIL) et sans consentement de la personne concernée (2). Sont également jugées sensibles la collecte des informations relatives à son appartenance ethnique ou à son orientation sexuelle (2).

Trois évènements sont particulièrement redoutés : un accès illégitime au dossier (risque de rupture du secret médical, risque d'utilisation détournée), la modification non désirée des données (risque d'accusation à tort d'un délit, risque d'erreur médicale) et la disparition des données (risque d'erreur médicale). Ces évènements sont causés par différentes menaces. Ce sont surtout les supports de données qui peuvent être : utilisés de manière inadaptée, modifiés, perdus ou volés, observés, détériorés ou surchargés (3).

En 2014 et 2015, des chercheurs en sécurité informatique avaient déjà souligné le fait que les DPS étaient devenus la cible de choix des cybercriminels (4,5). Depuis, plusieurs affaires ont été révélées : un cas d'accès illégitimes au dossier médical avec l'affaire Quintile en 2017 (6), deux cas de destruction des DPS avec la propagation des rançongiciels Locky en 2016 (7) et WannaCry en 2017 (8). Plus récemment, ce sont les données personnelles de 1,5 millions d'habitants de Singapour (plus d'un quart de la population) qui ont été dérobées. Les ordonnances de 160 000 patients, ainsi que le dossier médical du premier ministre, ont également été volées (9). Au Portugal, un hôpital a été sanctionné, en janvier 2019, pour violation du principe de limitation d'accès aux données, suite à la dénonciation d'un collectif de médecins (10).

L'Australie a expérimenté la mise en place d'un système équivalent au Dossier Médical Partagé (DMP), nommé « My Health Record ». Ce système a été sujet à plusieurs

controverses. L'une concernait l'accès aux données par les forces de l'ordre et par le service des impôts sans nécessité d'une décision judiciaire (11,12). Un premier audit en sécurité avait recommandé que les médecins généralistes ayant accès au fichier australien soient dotés d'un accès sécurisé de niveau militaire et d'une formation adéquate (13). Cette dernière recommandation n'aurait pas été appliquée faute de budget.

Les médecins généralistes français semblent pour le moment avoir été épargnés d'une attaque massive des DPS de leurs patients. En 2007, une étude portant sur 149 médecins généralistes avait toutefois montré que 24 % avaient déjà été victimes d'un virus informatique. Trente-et-un pour cent avaient déjà expérimenté des pertes de données toutes causes confondues (14).

En 2017, 85 % des Français se disaient préoccupés par la protection de leurs données personnelles en général (15). La France est en tête des demandes pour faire valoir le droit à l'oubli sur internet (16). On peut donc supposer que les patients attendent une protection efficace de leurs données de santé.

En 2018, la téléconsultation est devenue remboursée en France. Les logiciels de téléconsultation agréés utiliseront le DMP pour stocker les données de la consultation (17).

En France, la centralisation de données sensibles via le DMP se verra probablement dotée d'un haut niveau de sécurité (18). On peut néanmoins craindre que ce soient les utilisateurs, dont feront partie les patients eux-mêmes, mais aussi les médecins généralistes, qui seront à l'origine des principales failles de sécurité (19).

Pour se prémunir de ces différentes menaces, la CNIL encourage la prise de précautions élémentaires. Ces précautions ont été revisitées lors de la mise en vigueur du nouveau Règlement Général sur la Protection des Données (RGPD) (20).

Le RGPD répond surtout à l'enjeu que représente le traitement des données personnelles par les géants du secteur numérique en Europe. Mais dans le même temps, il édicte des recommandations qui se veulent plus précises et plus adaptées à chaque situation et à chaque entreprise stockant des données personnelles. Il est envisageable, en cas de problème de perte, vol ou divulgation des données de santé, que la justice compare les moyens qui ont été employés par les médecins avec les moyens recommandés par le RGPD.

L'objectif de ce travail était de décrire la maîtrise des médecins généralistes libéraux de la Réunion en 2019 quant à la sécurité des données personnelles de santé de leurs patients.

# II. Matériels et méthodes

## 2.1 Étude

Il s'agissait d'une étude déclarative, transversale, quantitative, dont le recueil a été effectué de mai à septembre 2019.

## 2.2 Population

La population étudiée était les médecins généralistes libéraux installés et exerçant seuls, en groupe ou en pôle de santé, à l'Île de la Réunion.

Critères d'inclusion : les médecins généralistes libéraux installés en cabinet, seuls, en groupe ou en pôle de santé, à la Réunion.

Critères d'exclusion : les médecins généralistes n'exerçant pas en libéral, les médecins généralistes remplaçants ou non installés.

## 2.3 Déroulement de l'étude et recueil de données

Un questionnaire informatisé anonyme et confidentiel a été envoyé une première fois via la lettre d'information de l'URML-OI en mai 2019, à l'intention des médecins généralistes libéraux, installés en cabinet de groupe ou non, à la Réunion. Une relance sur le même format a été effectuée en juin 2019. Les médecins ont répondu aux questions sur la base du volontariat.

Le questionnaire (cf Annexe I) a été élaboré en transposant les conseils du guide de la CNIL sur la sécurité des données personnelles 2018 (3) au contexte du cabinet du médecin généraliste.

Ce questionnaire a été préalablement testé auprès de plusieurs médecins généralistes volontaires. À la fin du questionnaire, les freins à la mise en œuvre des consignes de sécurité ont été recherchés.

Les participants ont été encouragés à faire part de leurs remarques dans des champs libres ajoutés au bas de chaque page du questionnaire.

Il était annoncé aux participants que leurs réponses donneraient suite à l'élaboration d'une fiche d'aide à la sécurisation des données des patients qui leur serait transmise à la fin de

l'étude. Pour recevoir cette fiche, il était demandé aux participants d'envoyer un courriel en ce sens.

## 2.4 Analyse statistique

L'analyse statistique a été réalisée de façon descriptive, et la marge d'erreur a été calculée à posteriori, grâce à une formule de calcul de taille de l'échantillon (21). Avec une taille de population de 757 médecins et une taille d'échantillon de 49 médecins, nous avons obtenu, pour un niveau de confiance de 95 %, une marge d'erreur située entre 14 % et 15 %. Les données du questionnaire ont été analysées grâce au logiciel de statistiques *R – version 3.6.1 (2019-07-05)* qui a permis le calcul des intervalles de confiance.

## 2.5 Critères éthiques

Ce questionnaire était anonyme et ne récoltait pas de données personnelles. Il n'a donc pas fait l'objet d'une déclaration à la CNIL (cf Annexe III).

Afin de préserver l'anonymat, il a été demandé aux médecins souhaitant recevoir la fiche d'aide à la sécurisation d'envoyer un courriel directement à l'enquêteur. Ce système a été mis en place afin de ne pas stocker leurs adresses de courriel sur le même serveur que les questionnaires. Cela a permis de limiter le risque de ré-identification. De même, les adresses IP des participants n'ont volontairement pas été stockées. Le service de formulaire utilisé (*Framaforms.org*) émanait d'un organisme européen soumis au RGPD et qui se conforme à une charte éthique stricte concernant les données récoltées (22). À la fin de l'étude, les données ont été supprimées de ce service.

# III. Résultats

Au 1er janvier 2018, 757 médecins généralistes libéraux étaient installés à la Réunion (23). Lors de l'étude, 700 d'entre eux étaient inscrits à la lettre d'information de l'URML. Les questionnaires ont été envoyés via les lettres d'information de mai et juin 2019.

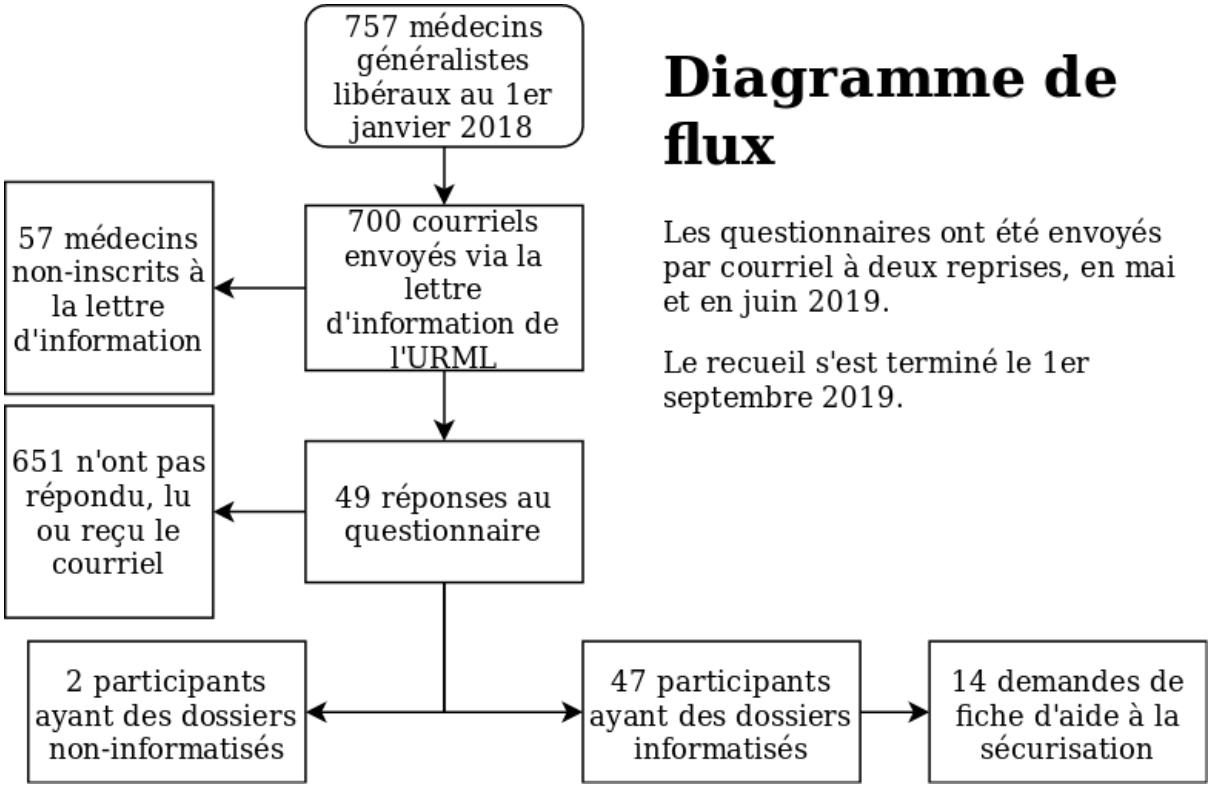


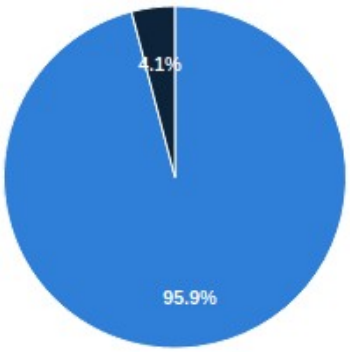

*Figure 1 : diagramme de flux*

## 3.1 Description de l'échantillon

Tableau I : Caractéristiques de la population étudiée (n=49)

| | | | |
|---|---|---|---|
| *Période d'installation* | *Avant 1980* | 2 | 4 % |
| | *Entre 1980 et 1990* | 9 | 18,3 % |
| | *Entre 1990 et 2000* | 10 | 20,5 % |
| | *Entre 2000 et 2010* | 13 | 26,6 % |
| | *Entre 2010 et 2015* | 6 | 12,2 % |
| | *Après 2015* | 8 | 16,4 % |
| | *Ne sait pas* | 1 | 2 % |
| *Modalité d'installation* | *Cabinet de groupe* | 33 | 67,3 % |
| | *Seul* | 16 | 32,7 % |

## 3.2 Informatisation des dossiers médicaux

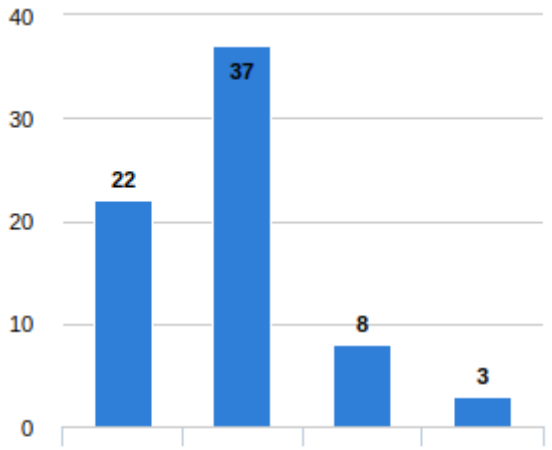



| | |
|---|---|
| Oui | 47 |
| Non | 2 |

*Figure 2 : Vos dossiers médicaux sont-ils informatisés ? (n=49)*

## 3.3 Réponses des participants informatisés

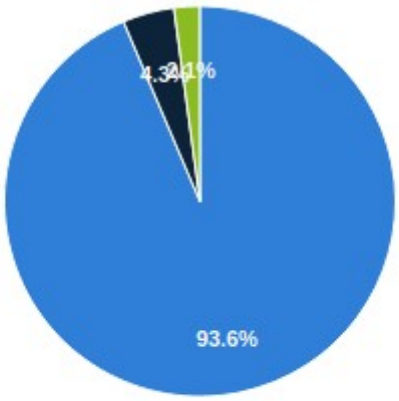
Les questions qui suivent ont été posées aux participants ayant répondu « Oui » à la question « Vos dossiers médicaux sont-ils informatisés ? » (n=47).




| | |
|---|---|
| Vous-même | 22 |
| Un informaticien | 37 |
| Votre associé | 8 |
| Votre secrétariat | 3 |

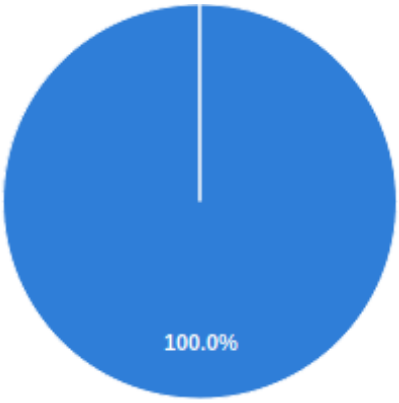
*Figure 3 : Qui se charge habituellement de votre matériel et de la maintenance des logiciels informatiques ?*

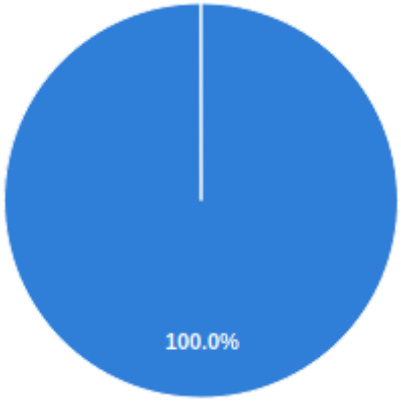
*Question à choix multiple (n=47)*




| | |
|---|---|
| Microsoft Windows | 44 |
| Apple MacOS | 2 |
| Je ne sais pas | 1 |

*Figure 4 : Quel système d'exploitation (OS) utilisez-vous ? (n=47)*



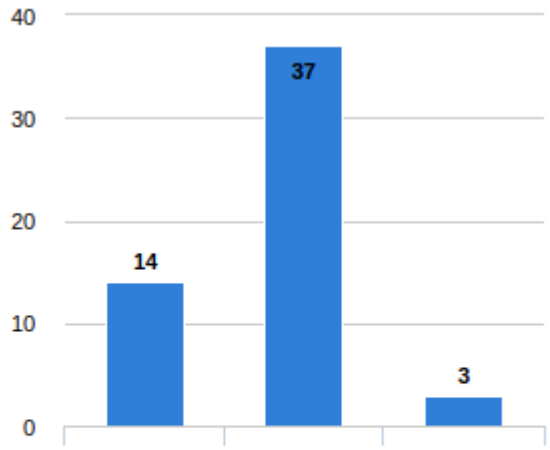




| | |
|---|---|
| Windows 7, 8 ou 10 | 44 |

| | |
|---|---|
| OS X Yosemite, El Capitan, Sierra ou High Sierra | 2 |

*Figure 5 : Quelle version de Microsoft Windows / Apple MacOS utilisez-vous ?*

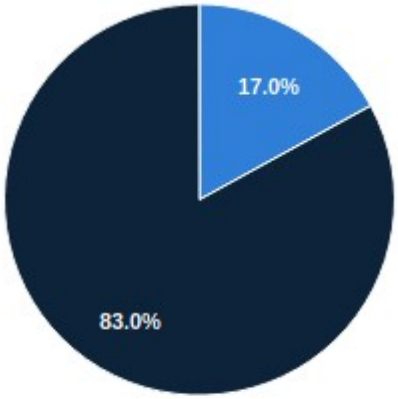
*Question posée aux participants ayant répondu « Microsoft Windows » ou « Apple MacOS » à la question « Quel système d'exploitation (OS) utilisez-vous ? » (n=46)*




| | |
|---|---|
| Ordinateur portable | 14 |
| Ordinateur fixe | 37 |
| Téléphone intelligent (smartphone) | 3 |

*Figure 6 : Quelle(s) machine(s) utilisez-vous pour accéder au dossier médical ? (n=47)*

*Question à choix multiple*




| | |
|---|---|
| Oui | 8 |
| Non | 39 |

*Figure 7 : Emportez-vous parfois une de ces machines hors du cabinet médical ? (n=47)*

Tableau II : Wi-Fi

| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Votre poste de travail est-il connecté à internet en Wi-Fi ? (n=47)* | 22 (46,8 %) | 23 (48,9 %) | 2 (4,3 %) |
| *Si oui, proposez-vous à vos patients de se connecter au même réseau Wi-Fi que le vôtre ? (n=22)* | 0 (0 %) | 22 (100 %) | 0 (0 %) |
| *Si oui, l'accès à votre réseau Wi-Fi est-il protégé par un mot de passe ? (n=22)* | 20 (90,9 %) | 0 (0 %) | 2 (9,1 %) |
| *→ Si oui, votre mot de passe Wi-Fi est-il noté sur un papier de manière à être visible depuis votre poste de travail ? (n=20)* | 2 (10 %) | 18 (90 %) | 0 (0 %) |
| *→ Si oui, votre mot de passe Wi-Fi fait-il au moins 12 caractères ? (n=20)* | 14 (70 %) | 3 (15 %) | 3 (15 %) |
| *→ Si oui, votre Wi-Fi utilise-t-il le chiffrement WPA/WPA2-PSK ? (n=20)* | 5 (25 %) | 1 (5 %) | 14 (70 %) |

**NSP pour « Ne sait pas »*

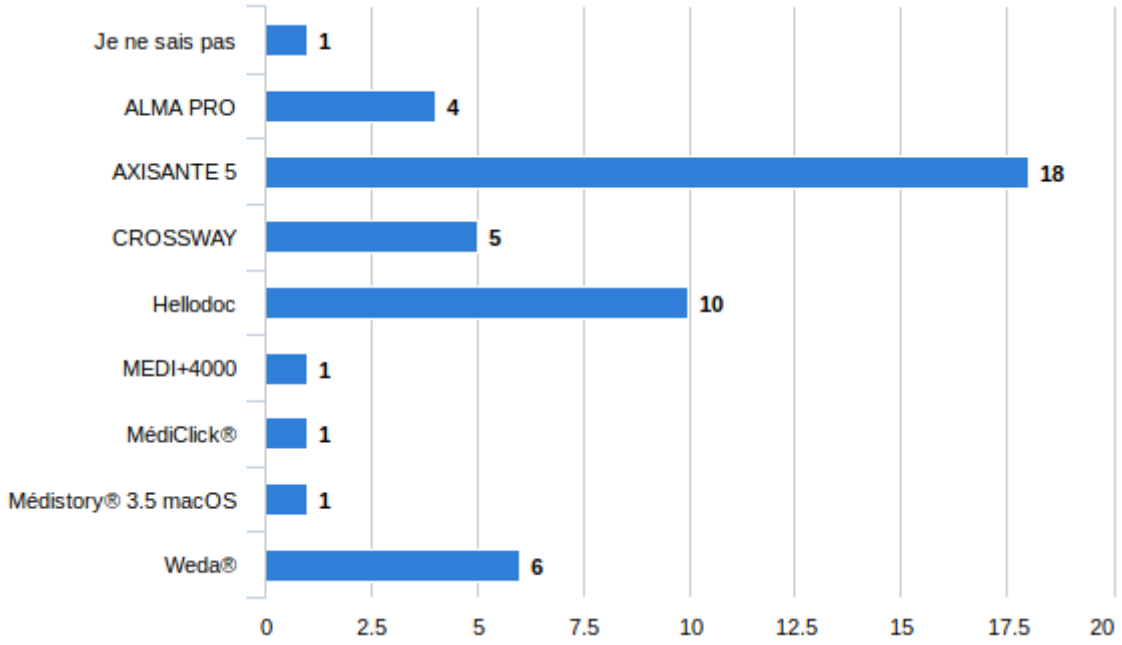
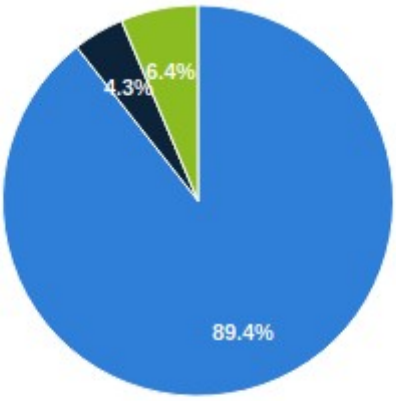



*Figure 8 : Quel logiciel médical utilisez-vous ? (n=47)*




| | |
|---|---|
| Oui | 42 |
| Non | 2 |
| Je ne sais pas | 3 |

*Figure 9 : Utilisez-vous la dernière version de ce logiciel ? (n=47)*

Tableau III : Logiciel métier (n=47)

| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Devez-vous taper votre identifiant à chaque connexion ?* | 18 (38,3 %) | 27 (57,4 %) | 2 (4,3 %) |
| *Utilisez-vous un mot de passe pour y accéder ?* | 34 (72,4 %) | 12 (25,5 %) | 1 (2,1 %) |
| *Votre carte CPS est-elle nécessaire pour accéder aux données du logiciel médical ?* | 14 (29,8 %) | 32 (68,1 %) | 1 (2,1 %) |

**NSP pour « Ne sait pas »*

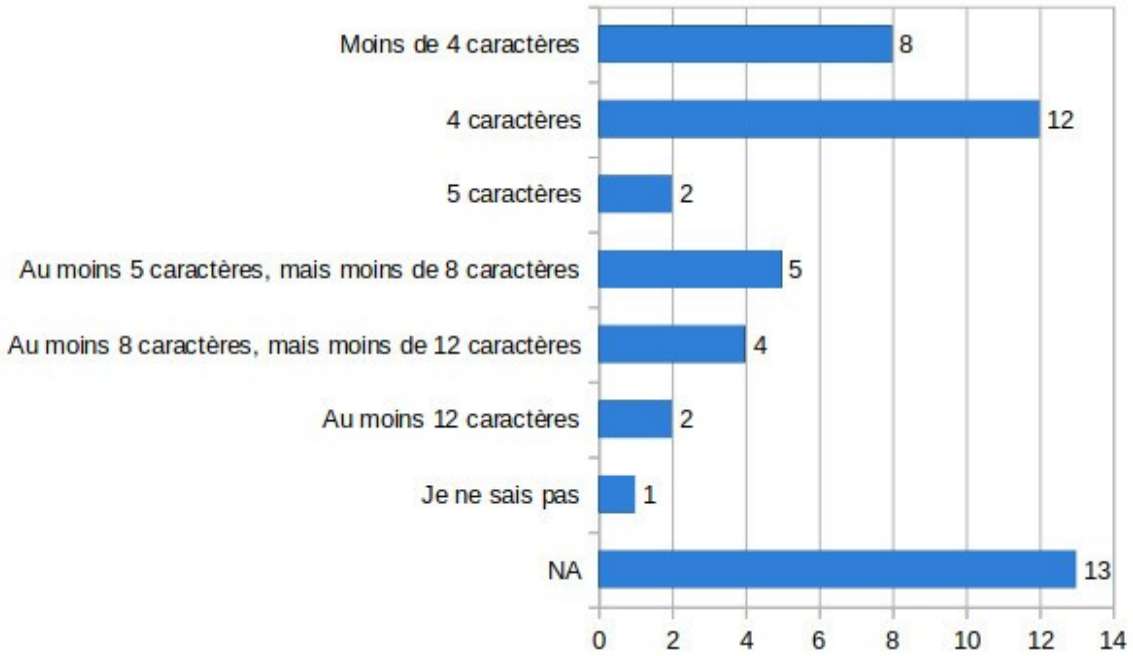



*Figure 10 : Quelle est la longueur de votre mot de passe ?*

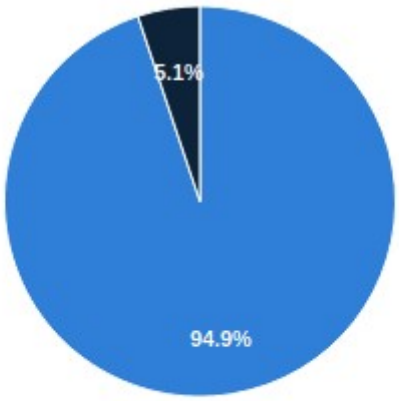
*Question posée aux participants ayant répondu « Oui » à la question « Utilisez-vous un mot de passe pour y accéder ? » (n=34)*

Tableau IV : Force du mot de passe, questions posées aux participants ayant répondu « Oui » à la question « utilisez-vous un mot de passe pour y accéder ? » (n=34)

| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Possède-t-il une majuscule ?* | 9 (26,5 %) | 23 (67,6 %) | 2 (5,9 %) |
| *Possède-t-il une minuscule ?* | 15 (44,1 %) | 17 (50 %) | 2 (5,9 %) |
| *Possède-t-il un chiffre ?* | 20 (58,8 %) | 12 (35,3 %) | 2 (5,9 %) |
| *Possède-t-il un caractère spécial ?* | 28 (82,4 %) | 4 (11,8 %) | 2 (5,9 %) |
| *Votre mot de passe est-il noté sur un papier de manière à être visible depuis votre poste de travail ?* | 1 (2,9 %) | 33 (97,1 %) | 0 (0 %) |
| *Renouvelez-vous votre mot de passe tous les ans ?* | 5 (14,7 %) | 29 (85,3 %) | 0 (0 %) |
| *Est-ce que le nombre de tentative d'accès au dossier médical est limité en cas d'erreur de mot passe ?* | 15 (44,1 %) | 6 (17,6 %) | 13 (38,2 %) |

**NSP pour « Ne sait pas »*

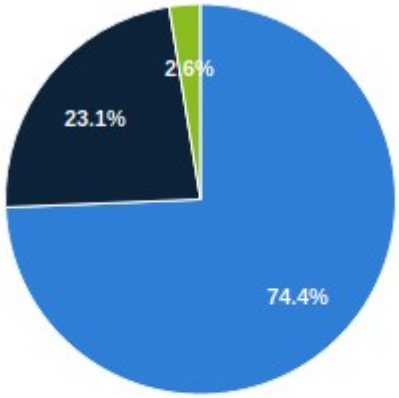
39 participants (82,9 %, n=47) ont déclaré employer au moins un secrétaire. Ces participants ont déclaré employer en moyenne 1,8 secrétaires (avec des réponses allant de 1 secrétaire à 10 secrétaires).




| | |
|---|---|
| Oui | 37 |
| Non | 2 |

*Figure 11 : Les secrétaires ont-ils accès au dossier médical ?*

*Question posée aux participants ayant répondu employer au moins 1 secrétaire (n=39)*




| | |
|---|---|
| Oui | 29 |
| Non | 9 |
| Je ne sais pas | 1 |

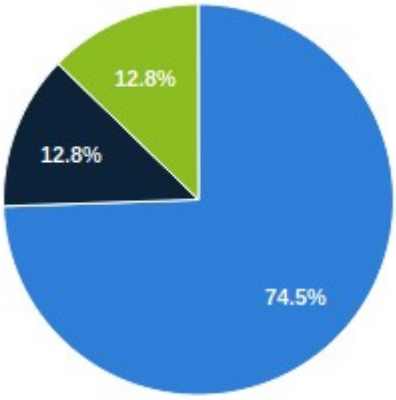
*Figure 12 : Les secrétaires ont-ils connaissance de vos identifiants et mots de passe ?*

*Question posée aux participants ayant répondu employer au moins 1 secrétaire (n=39)*

Tableau V : Remplaçants

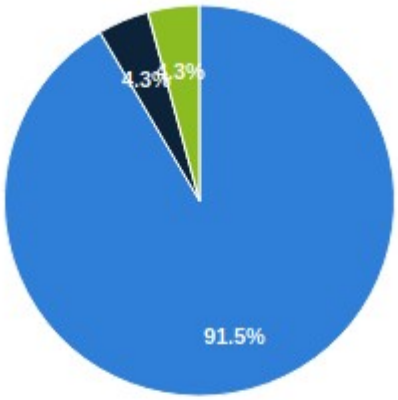
| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Vos remplaçants ont-ils un identifiant spécifique ? (n=47)* | 8 (17 %) | 36 (76,6 %) | 3 (6,4 %) |
| *Si oui, renouvelez-vous cet identifiant à chaque nouveau remplacement ? (n=8)* | 6 (75 %) | 2 (25 %) | 0 (0 %) |
| *Vos remplaçants ont-ils un mot de passe spécifique ? (n=8)* | 6 (75 %) | 2 (25 %) | 0 (0 %) |
| *Si oui, renouvelez-vous ce mot de passe à chaque nouveau remplacement ? (n=6)* | 5 (83,3 %) | 1 (16,7 %) | 0 (0 %) |

**NSP pour « Ne sait pas »*




| | |
|---|---|
| Oui | 35 |
| Non | 6 |
| Je ne sais pas | 6 |

*Figure 13 : Utilisez-vous un logiciel anti-virus ? (n=47)*




| | |
|---|---|
| Oui | 43 |
| Non | 2 |
| Je ne sais pas | 2 |

*Figure 14 : Utilisez-vous un logiciel de dépannage à distance ? (n=47)*

Tableau VI : Logiciels

| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Utilisez-vous un logiciel anti-virus ? (n=47)* | 35 (74,5 %) | 6 (12,8 %) | 6 (12,8 %) |
| *Si oui, votre anti-virus est-il mis à jour automatiquement ? (n=35)* | 29 (82,9 %) | 1 (2,9 %) | 5 (14,3 %) |
| *Utilisez-vous un logiciel pare-feu ? (n=47)* | 27 (57,4 %) | 3 (6,4 %) | 17 (36,2 %) |
| *Utilisez-vous un logiciel de dépannage à distance ? (n=47)* | 43 (91,5 %) | 2 (4,3 %) | 2 (4,3 %) |
| *Si oui, lorsque ce logiciel de dépannage à distance souhaite prendre le contrôle de votre poste, recueille-t-il votre autorisation avec un message de confirmation affiché à l'écran ? (n=43)* | 32 (74,4 %) | 9 (20,9 %) | 2 (4,7 %) |
| *Si oui, lorsque ce logiciel de dépannage à distance est utilisé, êtes-vous prévenu par un message affiché à l'écran ? (n=43)* | 36 (83,7 %) | 4 (9,3 %) | 3 (7 %) |

**NSP pour « Ne sait pas »*

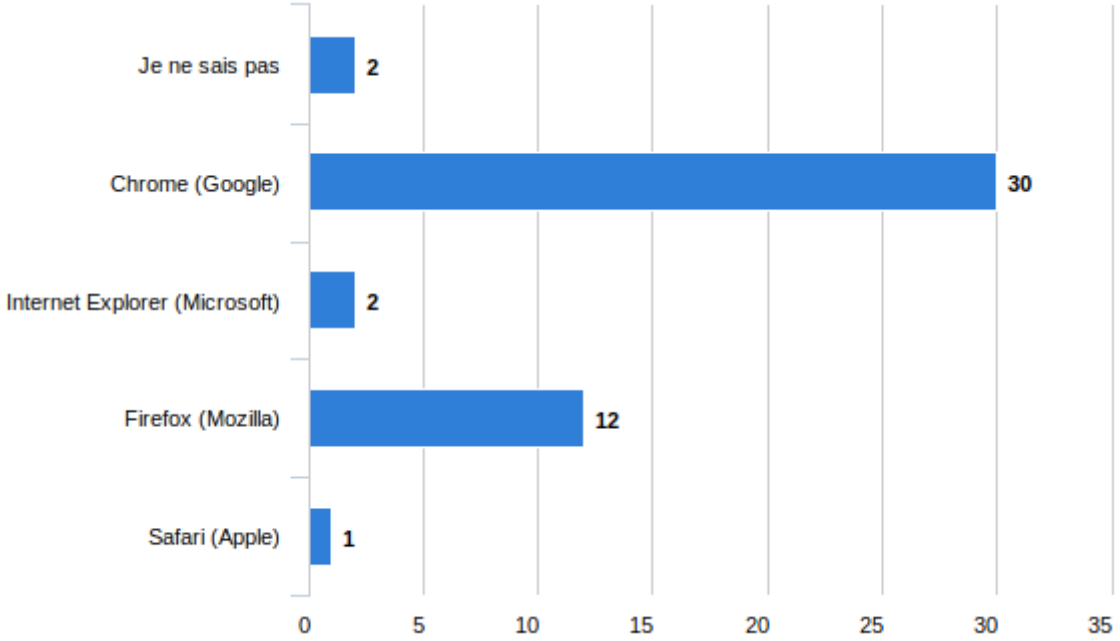
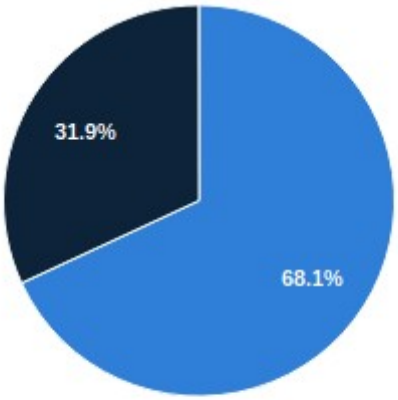



*Figure 15 : Quel navigateur internet utilisez-vous le plus souvent ? (n=47)*

Tableau VII : Navigateur et DMP (n=47)

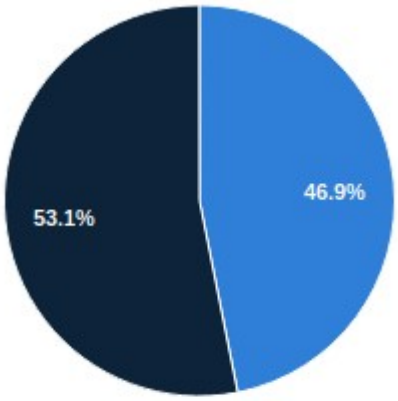
| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Votre navigateur est-il mis à jour automatiquement ?* | 34 (72,3 %) | 1 (2,1 %) | 12 (25,5 %) |
| *Utilisez-vous l'option « retenir le mot de passe » de votre navigateur ?* | 16 (34 %) | 29 (61,7 %) | 2 (4,3 %) |
| *Alimentez-vous le Dossier Médical Partagé (DMP) ?* | 3 (6,4 %) | 44 (93,6 %) | 0 (0 %) |

**NSP pour « Ne sait pas »*




| | |
|---|---|
| Oui | 32 |
| Non | 15 |

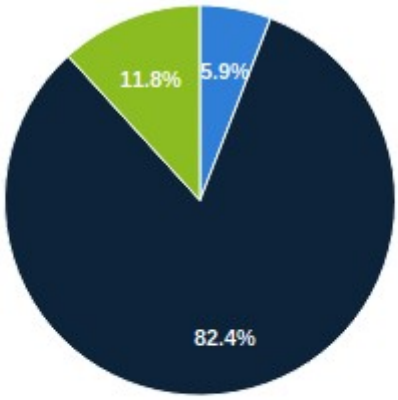
*Figure 16 : Utilisez-vous le courriel pour communiquer des données médicales ? (n=47)*




| | |
|---|---|
| Oui | 15 |
| Non | 17 |

*Figure 17 : Utilisez-vous systématiquement une messagerie de santé sécurisée pour communiquer des données médicales ?*

*Question posée aux participants ayant répondu « Oui » à la question « Utilisez-vous le courriel pour communiquer les données médicales ? » (n=32)*




| | |
|---|---|
| Oui | 1 |
| Non | 14 |
| Je ne sais pas | 2 |

*Figure 18 : Lorsque vous utilisez cette messagerie non-sécurisée, anonymisez-vous systématiquement le contenu de ces courriels ?*

*Question posée aux participants ayant répondu « Non » à la question « Utilisez-vous systématiquement une messagerie de santé sécurisée pour communiquer des données médicales ? » (n=17)*

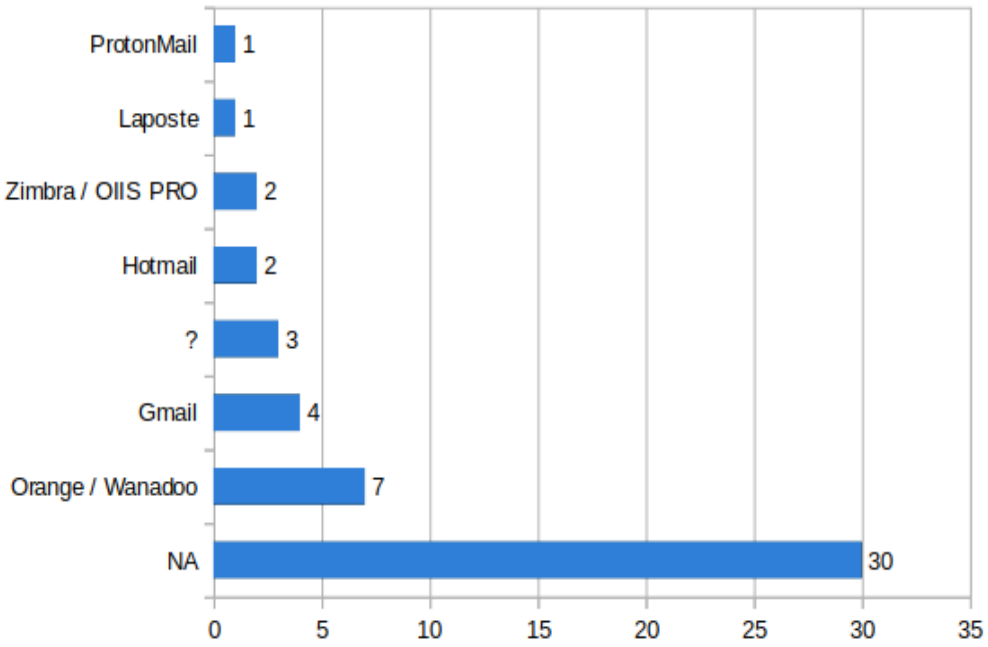



*Figure 19 : Fournisseurs d'adresse électronique non-Messagerie Sécurisée de Santé*

*Question à choix multiples, posée aux participants ayant répondu « Non » à la question « Utilisez-vous systématiquement une messagerie de santé sécurisée pour communiquer des données médicales ? » (n=17)*

Cent pour cent des utilisateurs d'un logiciel médical en ligne (n=6) ont déclaré ne pas réaliser de sauvegarde du fait de la gestion des sauvegardes par une entreprise tierce.

Un participant a déclaré ne pas savoir combien de sauvegardes étaient réalisées par semaine.

Un participant a déclaré ne faire aucune sauvegarde.

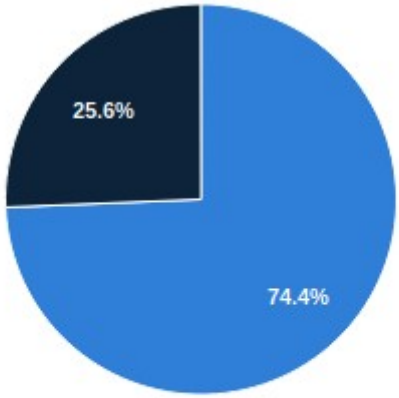
Les autres participants (n=39) ont déclaré réaliser 5 sauvegardes par semaine en moyenne (min. 1, max. 15).

Les supports de sauvegardes les plus utilisés étaient les disques dur externes pour 34 participants (87,1 %, n=39) avec en moyenne 1,4 disques durs par participant (min. 1, max. 4).

Les clés USB étaient utilisées par 10 participants (25,6 %, n=39) avec en moyenne 1,6 clés USB par participant (min. 1, max. 3).

Sept participants (17,9 %, n=39) utilisaient à la fois une clé USB et un disque dur externe.

Aucun participant n'a déclaré utiliser de sauvegardes sur CD/DVD.




| | |
|---|---|
| Oui | 29 |
| Non | 10 |

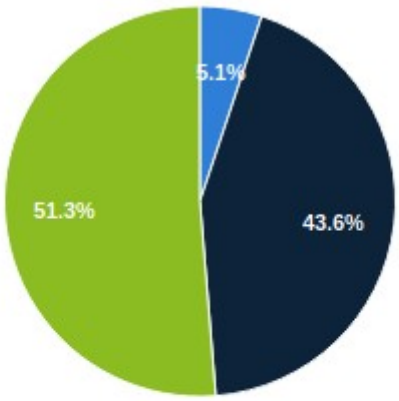
*Figure 20 : Stockez-vous une sauvegarde dans un lieu hors du cabinet ?*

*Question posée aux participants ayant répondu réaliser au moins une sauvegarde par semaine (n=39)*

Tableau VIII : Stockage des sauvegardes, question posée aux participants ayant répondu réaliser au moins une sauvegarde par semaine (n=39)

| Question | Oui | Non | NSP* |
|---|---|---|---|
| *Stockez-vous une sauvegarde sur internet ou dans le cloud ? (n=39)* | 3 (7,7 %) | 33 (84,6 %) | 3 (7,7 %) |
| *Si oui, utilisez-vous un hébergeur agréé de données de santé ? (n=3)* | 2 (66,7 %) | 0 (0 %) | 1 (33,3 %) |
| *Pour effectuer votre sauvegarde, utilisez-vous votre logiciel médical ? (n=39)* | 28 (71,8 %) | 4 (10,3 %) | 7 (17,9 %) |

**NSP pour « Ne sait pas »*




| | |
|---|---|
| Oui | 2 |
| Non | 17 |
| Je ne sais pas | 20 |

*Figure 21 : Lorsque vous n'utilisez plus un de ces supports de stockage, utilisez-vous un logiciel de suppression sécurisée des données ?*

*Question posée aux participants ayant répondu réaliser au moins une sauvegarde par semaine (n=39)*

Parmi les participants ayant répondu réaliser au moins une sauvegarde par semaine (n=39), 4 participants (10,3 %, n=39) ont déclaré ne pas utiliser leur logiciel médical pour effectuer leurs sauvegardes. Un seul d'entre eux a pu préciser le nom du logiciel utilisé qui était *EaseUS Todo Backup Free*.

Parmi les participants ayant répondu réaliser au moins une sauvegarde par semaine (n=39), 36 participants (92,3 %, n=39) ont déclaré conserver les données de leurs patients pour une durée illimitée. Un participant a déclaré les conserver pour une durée de 20 ans, un autre participant pour une durée de 10 ans, un autre pour une durée de 1 an.

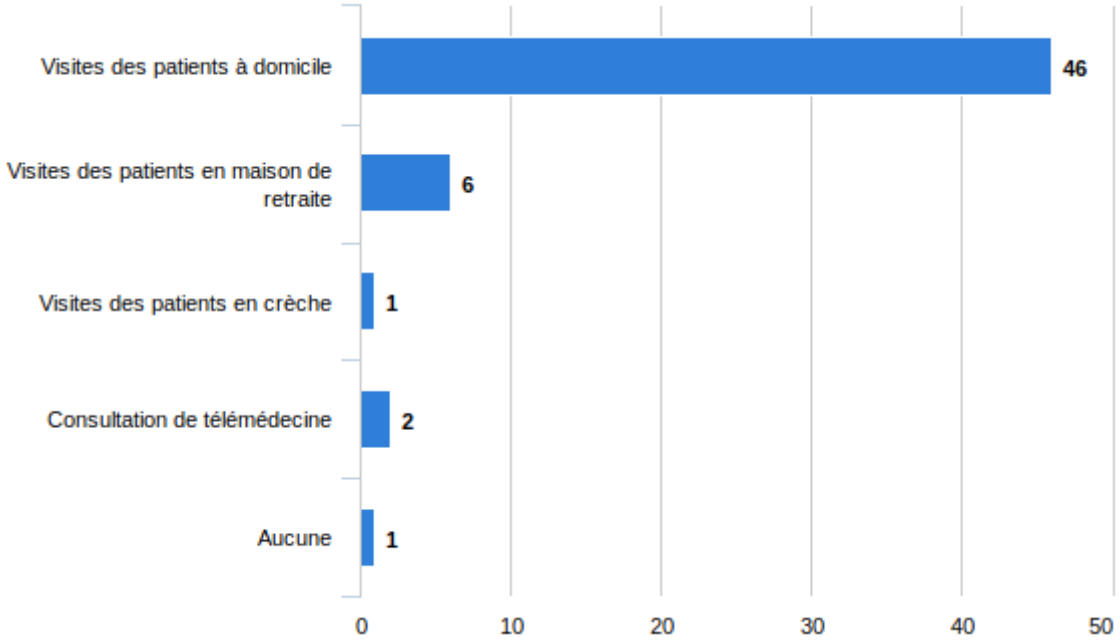
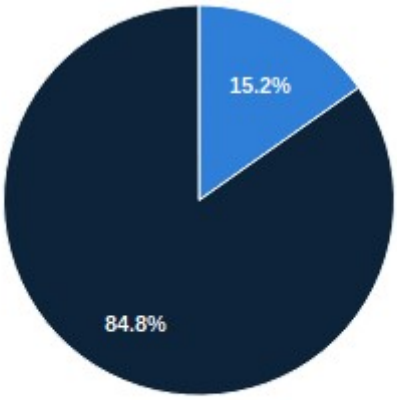



*Figure 22 : Quelles consultations hors de votre cabinet réalisez-vous ? (n=47)*

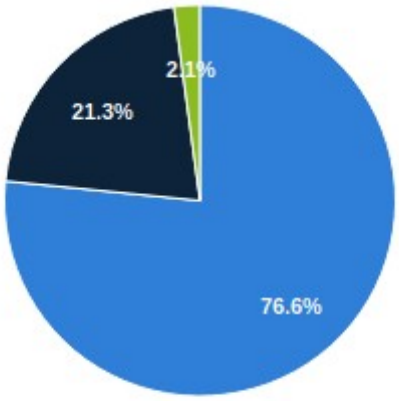
*Question à choix multiples*




| | |
|---|---|
| Oui | 7 |
| Non | 39 |

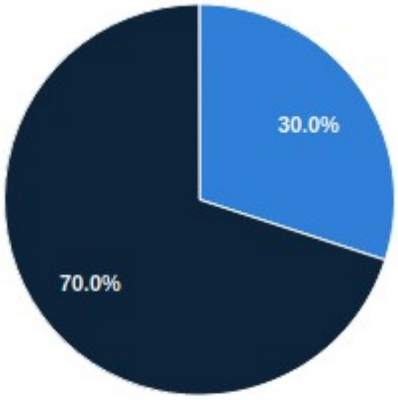
*Figure 23 : Utilisez-vous un logiciel pour compléter à distance votre dossier médical ?*

*Question posée aux participants ayant répondu réaliser des consultations hors du cabinet (n=46)*




| | |
|---|---|
| Oui | 36 |
| Non | 10 |
| Je ne sais pas | 1 |

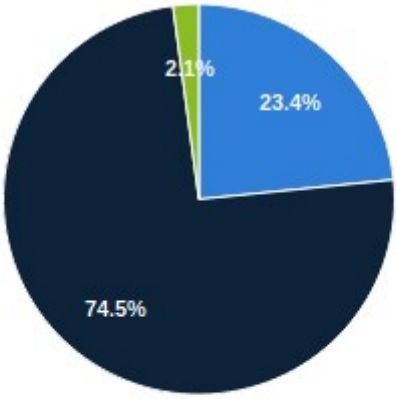
*Figure 24 : Lorsque vous vous absentez, éteignez-vous votre poste ? (n=47)*




| | |
|---|---|
| Oui | 3 |
| Non | 7 |

*Figure 25 : Si non, lorsque vous vous absentez, déconnectez-vous votre session de votre logiciel médical ?*

*Question posée aux participants ayant répondu « Non » à la question « Lorsque vous vous absentez, éteignez-vous votre poste ? (n=10)*




| | |
|---|---|
| Oui | 11 |
| Non | 35 |
| Je ne sais pas | 1 |

*Figure 26 : Utilisez-vous un écran de veille verrouillé ? (n=47)*

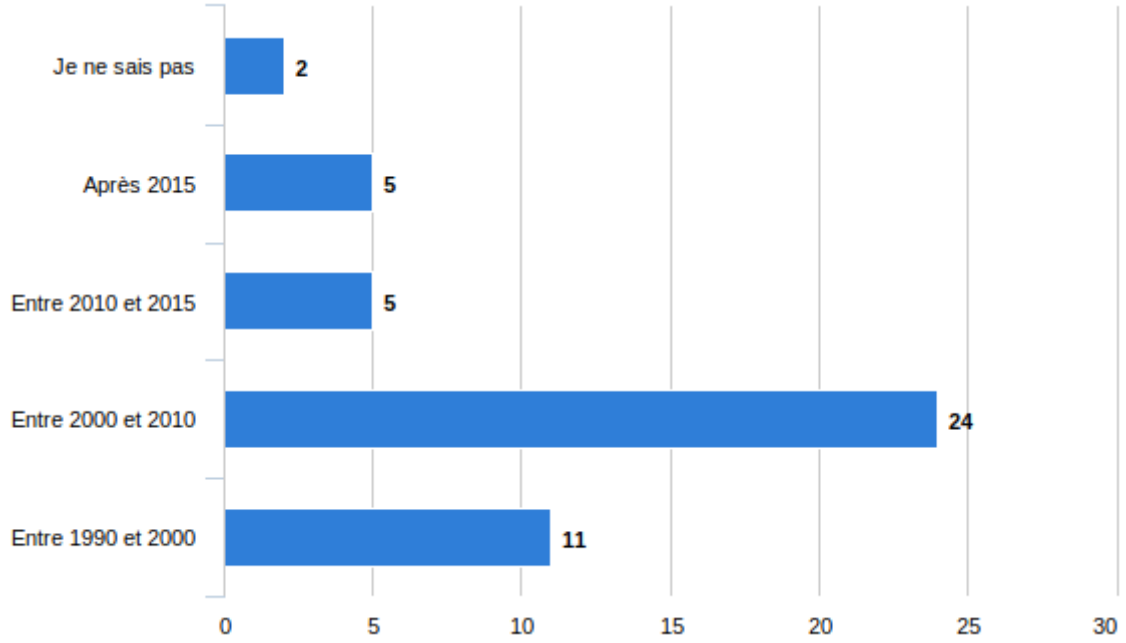



*Figure 27 : A quelle période êtes vous passé aux dossiers informatisés ? (n=47)*

Vingt-six participants (55,3 %, n=47) ont renseigné leur budget informatique annuel global, main d'œuvre comprise. Ce budget était estimé en moyenne à 2974 euros par an (min. 500, max. 20,000).

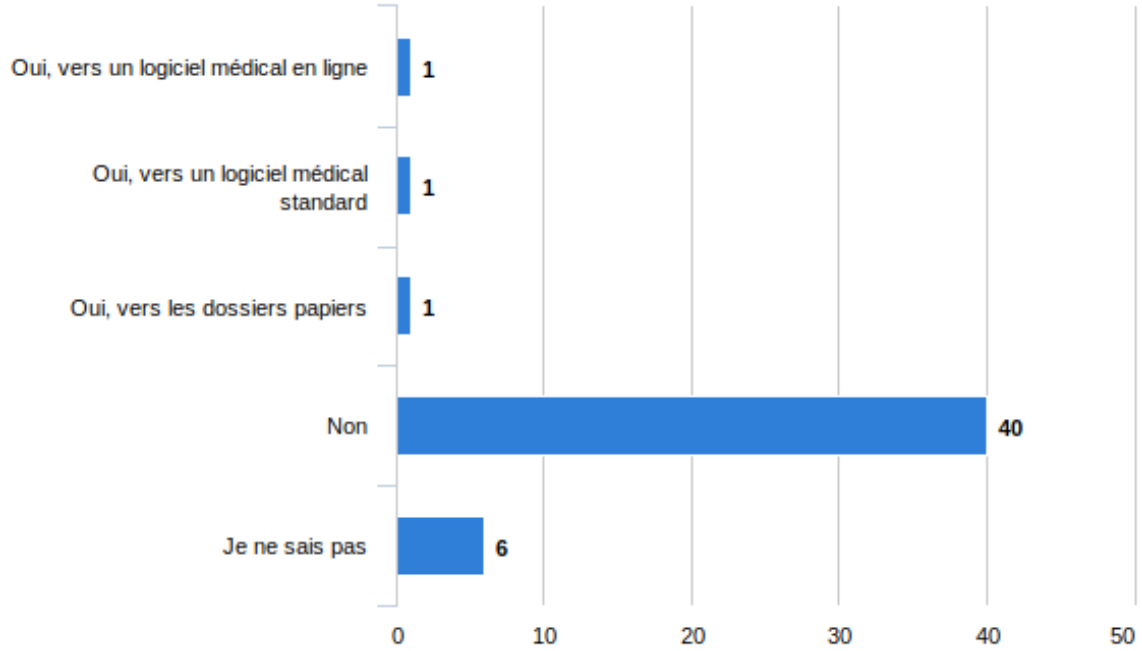



*Figure 28 : Envisagez-vous de migrer vers un autre système de dossier médical ? (n=49)*

*Question à choix multiples*

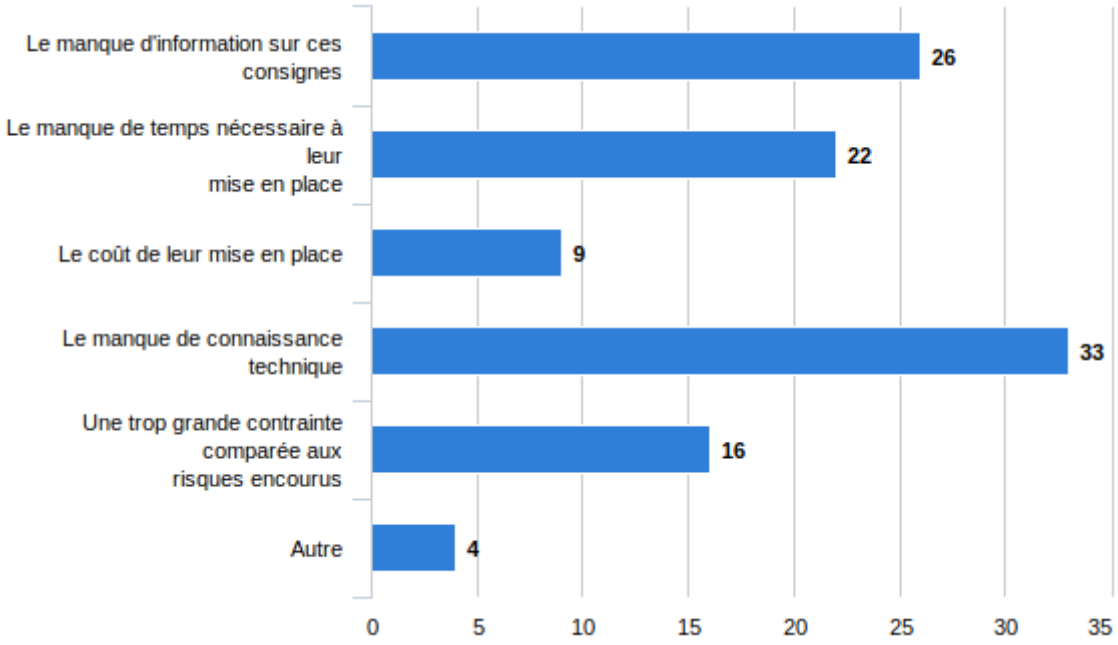



*Figure 29 : Dans votre cas, quels freins identifiez-vous à la mise en place de toutes les règles de sécurité informatique citées dans ce questionnaire ? (n=47)*

*Question à choix multiples*

## 3.4 Réponses des participants non-informatisés

Deux participants (4 %, n=49) ont déclaré ne pas posséder de dossiers informatisés.

Ces deux participants ont déclaré s'être installé entre 1980 et 1990, et être en cabinet de groupe.

Ils ont déclaré ne pas envisager de migrer vers un autre système de dossier médical.

Parmi les raisons de ce choix, les deux participants ont exprimé le fait qu'ils « n'aim[aient] pas » « l'informatisation des dossiers médicaux » ou simplement « l'ordinateur ».

Un des participants a précisé qu'il « rest[ait] fidèle aux fiches cartonnées ».

# IV. Discussion

## 4.1 Réponse à l'objectif principal

D'un côté, plusieurs résultats suggèrent une maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de santé de leurs patients :

– système d'exploitation non-obsolète dans 100 % des cas,

– Wi-Fi privé dans 100 % des cas,

– logiciel métier conforme à la réglementation en vigueur dans 91,5 % des cas (IC[78,8-96,9]) et à jour dans 89,4 % des cas (IC[32,7-61,4]),

– pas de mot de passe en vue du bureau dans 97 % des cas,

– utilisation d'un anti-virus dans 74,5 % des cas (IC[59,6-85,2]),

– utilisation d'un navigateur non obsolète dans 100 % des cas, dont les mises à jour sont automatiquement appliquées dans 72,3 % des cas, utilisation de l'option « retenir le mot de passe » dans 34 % des cas (IC[21,6-49,1]),

– utilisation sécurisée d'un logiciel de dépannage à distance dans 69,7 % des cas,

– sauvegardes au moins une fois par semaine dans 82,9 % des cas, stockées hors du cabinet dans 74,4 % des cas (IC[57,9-85,9]),

– extinction du poste de travail lors des absences dans 76,6 % des cas (IC[61,9-86,8]).

D'un autre côté, plusieurs résultats suggèrent des améliorations possibles de cette sécurité :

– réseau Wi-Fi suffisamment sécurisé dans 54,5 % des cas,

– utilisation d'un mot de passe pour accéder au logiciel métier dans 72,3 % des cas (IC[57,4-83,5]),

– mot de passe suffisamment robuste dans 23,5 % des cas,

– renouvellement du mot de passe annuel dans 14,7 % des cas (IC[6,1-31,6]),

– utilisation d'une MSS dans 46,9 % des cas (IC[30,1-64,4]),

– anonymisation des données de santé avant leur envoi par courriel non sécurisé dans 5,9 % des cas (IC[0,8-33,7%]),

– utilisation d'un fournisseur de courriel dont la juridiction se trouve hors UE dans 55,5 % des cas,

– utilisation d'un logiciel de suppression sécurisée des données dans 5,1 % des cas,

– déconnexion de la session du logiciel médical lors des absences dans 30 % des cas lorsque le poste de travail n'est pas éteint,

– utilisation d'un écran de veille verrouillé dans 23,4 % des cas (IC[13,2-38,1]).

Par ailleurs, les résultats suggèrent des progrès possibles concernant certaines connaissances techniques, ce qui pourrait améliorer leur maîtrise des DPS des patients :

– type de chiffrement du réseau Wi-Fi (70 % ne savaient pas répondre),
– limitation du nombre de tentative d'accès au dossier médical (38,2 % ne savaient pas répondre),
– utilisation d'un logiciel pare-feu (36,2 % ne savaient pas répondre),
– mises à jour automatiques du navigateur (25,5 % ne savaient pas répondre),
– utilisation d'un hébergeur agréé de données de santé pour le stockage des sauvegardes (33,3 % ne savaient pas répondre),
– utilisation d'un logiciel de suppression sécurisée des données (51,3 % ne savaient pas répondre).

De plus, les résultats suggèrent un manque de connaissance et/ou d'information concernant les recommandations sur la durée de conservation des DPS, ce qui pourrait diminuer la maîtrise des DPS des patients :

– conservation des DPS des patients pour une durée indéfinie dans (92,3 % ne savaient pas et ont indiqué une durée illimitée).

## 4.2 Analyse des résultats

### Informatisation des dossiers patients

Les résultats suggèrent que l'utilisation de dossiers informatisés dans la population étudiée (95,9 %, IC[84,4-99]) est comparable à celle des médecins de métropole (96 %) (1).

### Système d'exploitation

La CNIL recommande l'utilisation de logiciels qui ne sont pas obsolètes. Aucun participant n'a déclaré utiliser un système d'exploitation obsolète (3).

Un seul participant (2,1 %) a répondu ne pas savoir si son système d'exploitation était Windows, MacOS ou autre.

Ce résultat pourrait être expliqué par le fait que les logiciels médicaux ne sont plus compatibles avec les systèmes d'exploitation obsolètes.

Par ailleurs, les résultats suggèrent une utilisation de Microsoft Windows de 93,6 % versus 73.47 % dans la population métropolitaine tout venant. De même, l'utilisation de Apple MacOS représenterait 4,3 % des cas versus 19.89 % dans la population métropolitaine tout venant (24)

### Réseau Wi-Fi

La CNIL recommande la sécurisation du réseau Wi-Fi.

Vingt-deux participants informatisés (46,8 %, IC[32,7-61,4]) ont déclaré avoir leur poste de travail connecté à internet par Wi-Fi.

La question sur le chiffrement du réseau Wi-Fi était probablement trop technique car 14 des 20 participants ayant répondu avoir un mot de passe Wi-Fi (70 %) n'ont pas su y répondre.

Si l'on considère que le mode de sécurité WEP-128 n'est plus proposé par défaut par les constructeurs de routeurs depuis 2003, il est probable que la plupart des participants ont un réseau Wi-Fi chiffré par WPA/WPA2-PSK. Néanmoins, un participant a déclaré avoir un chiffrement autre que WPA/WPA2-PSK, ce qui semble indiquer que ce chiffrement n'est pas appliqué à 100 % des réseaux Wi-Fi.

Si l'on écarte la question du chiffrement, 12 participants (54,5 %) ont déclaré avoir une sécurité Wi-Fi suffisante (réseau Wi-Fi privé, protégé par un mot de passe comprenant au moins 12 caractères, non visible à proximité du poste de travail).

Si l'on prend en compte la question du chiffrement, seulement 5 participants (22,7 %) ont déclaré avoir une sécurité Wi-Fi suffisante selon les recommandations de la CNIL (réseau

Wi-Fi privé, protégé par un mot de passe comprenant au moins 12 caractères, non visible à proximité du poste de travail et chiffré en WPA/WPA2-PSK) (3).

## Logiciel métier

La CNIL recommande un logiciel métier à jour et conforme à la réglementation en vigueur.

Quarante-six participants (97,8 %) ont déclaré utiliser un logiciel métier conforme à la réglementation. Quarante-deux participants (89,4 %, IC[76,3-95,6]) ont déclaré utiliser la dernière version de leur logiciel. Quarante-trois participants (91,5 %, IC[78,8-96,9]) ont déclaré utiliser un logiciel métier possédant le label e-santé de l'ASIP Santé (25). Ce label e-santé atteste de la conformité d'un corpus d'exigences, qui sont l'adéquation fonctionnelle aux besoins des professionnels, la conformité avec la réglementation en vigueur et la compatibilité avec le DMP.

Tableau IX : logiciels métiers utilisés et certification HAS / label e-santé (n=47)

| Label e-santé | Certification HAS | Logiciel métier | Utilisation par les participants |
|---|---|---|---|
| Avancée (niveau 2) | Oui | ALMA PRO (ASSOCIATION ALMA) | 4 (8,5 %) |
| Standard (niveau 1) | Oui | AXISANTE MSP (COMPUGROUP MEDICAL SOLUTIONS)<br>CROSSWAY (CEGEDIM LOGICIELS MEDICAUX)<br>Hellodoc (IMAGINE EDITIONS)<br>Weda (WEDA) | 39 (83 %) |
| Non | Oui | MEDI+4000 (RM INGENIERIE)<br>MédiClick® (CEGEDIM LOGICIELS MEDICAUX FRANCE)<br>Médistory® 3.5 macOS (PROKOV EDITIONS) | 3 (6,4 %) |
| ? | ? | Ne sait pas | 1 (2,1 %) |

## Mot de passe

La CNIL recommande l'utilisation d'un mot de passe suffisamment robuste pour accéder aux DPS.

Les résultats suggèrent que 72,3 % IC[57,4-83,5] des médecins de la population étudiée utilisent un mot de passe pour accéder au logiciel métier. Ce mot de passe nécessite une robustesse qui varie en fonction du moyen d'identification employé (3).

Tableau X : Validité de la robustesse du mot de passe en fonction du moyen d'identification et de la limitation du nombre de tentative d'accès en cas d'erreurs, parmi les participants ayant répondu utiliser un mot de passe (n = 34)

| | Limitation du nombre de tentative d'accès en cas d'erreurs ? | |
|---|---|---|
| | Oui | Non ou NSP* |
| *CPS requise*<br>*et mot de passe (≥ 4 caractères)* | **Valide**<br>**5** | Non-valide<br>3 |
| *CPS requise*<br>*mais mot de passe < 4 caractères*<br>*ou NSP** | Non-valide<br>2 | |
| *Identifiant*<br>*et mot de passe ≥ 5 caractères* | **Valide**<br>**1** | Non-valide<br>3 |
| *Identifiant*<br>*mais mot de passe < 5 caractères* | Non-valide<br>4 | |
| *Mot de passe seul*<br>*≥ 12 caractères de 4 types* | **Valide**<br>**2** | |
| *Mot de passe seul*<br>*≥ 12 caractères de moins de 4 types* | Non-valide<br>0 | |
| *Mot de passe seul*<br>*< 12 caractères*<br>*≥ 8 caractères d'au moins 3 types* | Non-valide, sécurité minimum<br>0 | |
| *Mot de passe seul*<br>*< 12 caractères*<br>*≥ 8 caractères de moins de 3 types* | Non-valide<br>1 | |
| *Mot de passe seul*<br>*< 8 caractères ou NSP** | Non-valide<br>13 | |

**NSP pour « Ne sait pas »*

Les résultats suggèrent que le mot de passe employé était suffisamment robuste chez 8 participants ayant un mot de passe (23,5 %).

L’accès aux DPS n’était pas compromis par l’affichage du mot de passe en vue du bureau chez 33 participants (97 %).

Parmi les 10 participants qui utilisaient leur CPS associé à un mot de passe pour accéder aux données, 2 participants (20 %) ne laissaient pas leur CPS dans le lecteur lorsqu’ils s’absentaient du cabinet.

La comparaison avec les résultats d’une enquête de 2007 ne suggérait pas une augmentation de l’utilisation du mot de passe (72,3 % vs 79 %) (11).

## Logiciels anti-virus, pare-feu et navigateur internet

La CNIL recommande l’utilisation de logiciels antivirus, pare-feux et navigateurs non-obsolètes et à jour.

Les résultats suggèrent que 74,5 % IC[59,6-85,2] des médecins de la population étudiée utilisent un logiciel anti-virus, contre 78,8 % en 2007. Cet anti-virus serait mis à jour automatiquement dans 82,9 % des cas, contre 80 % en 2007. Les résultats suggèrent que 57,4 % des médecins de la population étudiée utilisent un logiciel pare-feu, contre 50 % en 2007 (11).

Les résultats suggèrent que 100 % des médecins de la population étudiée utilisent un navigateur non-obsolète (26). Ce résultat concorde avec le fait que 100 % des participants déclaraient utiliser un système d’exploitation non-obsolète. En effet, les mises à jour du navigateur peuvent être limitées par la version du système d’exploitation.

Les résultats suggèrent que 72,3 % des médecins de la population étudiée maintiennent leur navigateur à jour. Ce chiffre pourrait s’expliquer par le fait que les navigateurs les plus utilisés activent les mises à jour automatiques par défaut.

Les résultats suggèrent que 34 % IC[21,6-49,1] des médecins de la population étudiée utilisent l’option « retenir le mot de passe » de leur navigateur. Cela pourrait s’expliquer par un manque de sensibilisation quant à la faille de sécurité que cette pratique représente. En effet, les mots de passe stockés au sein du navigateur sont aisément lisibles par les autres utilisateurs, car ils ne sont pas cryptés.

## DMP

En ce qui concerne le DMP, les résultats suggèrent une utilisation marginale (6,4 %, IC[2,0-18,6]), qui peut s'expliquer par son lancement encore récent, comme le montrent les précisions apportées par les participants :

– 3 participants ont exprimé « [ne pas avoir] encore compris comment cela fonctionn[ait][…] » ou « commenc[er] à peine à [se] familiariser avec [le] DMP. »,
– Un participant a exprimé des craintes concernant l'utilisation du DMP et a écrit « ne [pas savoir] comment, par où ou par qui transitent les données [du DMP], [ni] qui ou quel organisme peut y avoir accès […] [Il n'y a] aucune façon de savoir si la réception est faite par un médecin de mon choix et du choix du patient […] »,
– Un participant a écrit que le DMP était (sic) « mal foutu et personne n'ira le lire ! »,
– Un participant a précisé qu'il laissait au patient le soin « de mettre à jour son DMP »,
– Un participant a précisé avoir refusé d'utiliser le DMP car « [son] numéro de téléphone personnel était systématiquement affiché dans le dossier du patient. »

## Logiciel de contrôle de l'environnement de bureau à distance

La CNIL recommande une utilisation sécurisée des logiciels d'aide à distance. Cela implique deux paramètres :

– lorsqu'un utilisateur distant souhaite prendre le contrôle de la machine, un message de connexion est affiché à l'utilisateur du poste afin qu'il puisse accepter ou décliner cette connexion, en lui laissant si besoin le temps de cacher les données sensibles affichées à l'écran,

– lorsqu'un utilisateur distant est connecté au poste, le logiciel affiche un message à l'intention de l'utilisateur du poste afin que celui-ci sache qu'un autre utilisateur a actuellement accès à ce qui est affiché à l'écran.

Les résultats suggèrent une utilisation d'un logiciel d'aide à distance dans 91,5 % des cas, IC[78,8-96,9], soit plus que l'utilisation d'un anti-virus (74,5 %, IC[59,6-85,2]). Ils suggèrent que 69,7 % des utilisateurs de ce logiciel en avait une utilisation sécurisée (message d'autorisation de connexion et message pendant l'utilisation du logiciel).

## Sauvegardes

La CNIL recommande des sauvegardes régulières, sans toutefois recommander un rythme de sauvegarde précis. La CNIL recommande également d'effectuer un test de restauration de ces sauvegardes, qui devraient être cryptées et dont un exemplaire devrait être stocké hors du cabinet médical.

Les résultats suggèrent que 82,9 % des médecins de la population étudiée effectuaient au moins une sauvegarde par semaine, versus 85 % dans une étude de 2007 (11). Une autre étude effectuée en 2018, portant spécifiquement sur les sauvegardes, montrait que 71 % des médecins interrogés effectuaient au moins une sauvegarde par semaine. À noter que les résultats de cette dernière étude suggéraient qu'aucun test de restauration des sauvegardes n'avait été réalisé dans 51 % des cas (27).

Les types de supports de sauvegarde les plus courants, semblent être, comme en 2007, les disques durs externes suivis des clés USB.

Les résultats suggèrent qu'une sauvegarde est stockée hors du cabinet dans 74,4 % des cas, IC[57,9-85,9] contre 65 % des cas en 2007. Les résultats suggèrent une non-augmentation de l'utilisation d'un logiciel de destruction des données (5,1 % des cas, versus 9 % en 2007) (11).

La particularité des sauvegardes via le logiciel médical est qu'elles sont réalisées de façon cryptée, avec le mot de passe du logiciel médical. Ainsi, une personne ayant accès au support de sauvegarde devra décrypter les données sauvegardées pour pouvoir les lire. Le logiciel *EaseUs Todo Backup Free*, utilisé par un des participants, propose bien une option afin de crypter les sauvegardes qu'il effectue (28).

Les résultats suggèrent que 92,3 % des médecins de la population étudiée conservent les données de leur patient pour une durée indéfinie. Le Conseil National de l'Ordre des Médecins (CNOM) et la CNIL recommandent de s'aligner sur les délais de conservation prévus pour les dossiers médicaux des établissements de santé, soit : 20 ans après la dernière consultation ou 10 ans à compter de la date de décès du patient, avec exception pour le patient mineur (28$^{e}$ anniversaire s'il était mineur lors de cette dernière consultation). En cas d'action tendant à mettre en cause la responsabilité du médecin, il est recommandé de conserver le dossier pour une durée illimitée (29).

## Courriels

Le RGPD oblige l'hébergement des DPS par des hébergeurs agréés de données de santé.

Lorsque les données sont stockées sur internet (que ce soit dans un cloud, dans une boite de réception de courriel en ligne ou sur les serveurs d'un réseau social), on dit que ces données sont hébergées par un service distant (l'hébergeur). Chaque hébergeur possède des conditions d'utilisation des données qu'il héberge, que l'on accepte et signe avant envoi des données. Ainsi, les DPS ne devraient pas être hébergées par un service dont les conditions d'utilisation autorisent le traitement des données hébergées à des fins commerciales, de collecte, de publicité ou d'apprentissage automatisé, à moins que ces DPS ne soient préalablement dé-identifiées, c'est-à-dire anonymisées et exempte de toute information pouvant permettre l'identification du patient (numéro de sécurité sociale, adresse, numéro de téléphone, photographie identifiable, etc.).

Une charte pour la sécurité des services électroniques a été élaborée par l'ANSSI, avec les fournisseurs de messagerie électronique français, afin de garantir que les données des courriels soient chiffrées et hébergées sur le territoire national (30). En effet, les lois qui encadrent l'utilisation des données personnelles peuvent varier d'un pays à l'autre : le transfert de données hors Union Européenne (UE) peut exposer ces données à des lois qui ne sont pas en adéquation avec le RGPD (31).

Les résultats suggèrent que les DPS sont partagées par courriel dans 68,1 % des cas (IC[53,0-80,1]). Les résultats suggèrent l'utilisation dans 46,9 % des cas (IC[30,1-64,4]), d'une messagerie sécurisée de santé (MSS). Si l'on ajoute à ce chiffre les deux participants ayant répondu ne pas utiliser de MSS mais ayant indiqué utiliser la messagerie Zimbra fournie par OIIS PRO (qui est une MSS) ce pourcentage grimpe à 53,1 %.

Lorsqu'une autre messagerie est utilisée, les résultats suggèrent une anonymisation des données dans 5,9 % des cas (IC[0,8-33,7]).

Tableau XI : Messageries électroniques utilisées et signature de la charte pour la sécurité des services de courriers électroniques de l'ANSSI, adéquation avec le RGPD

| Signature de la charte | Fournisseur de messagerie électronique | Pays et adéquation en matière de loi sur la protection des données | Utilisations |
|---|---|---|---|
| Oui | Orange.fr / Wanadoo.fr (France Télécom) | France (adéquat, RGPD) | 8 (44,4 %) |
| | Laposte.fr (La Poste) | France (adéquat, RPGD) | |
| Non | Gmail.com (Google / Alphabet Inc) | EUA* (adéquation partielle) | 10 (55,5 %) |
| | Hotmail.fr / Hotmail.com (Microsoft) | EUA* (adéquation partielle) | |
| | ProtonMail.ch (Proton Technologies AG) | Suisse (adéquat) | |
| | Ne sait pas | ? | |

**EUA pour « États-Unis d'Amérique »*

Les résultats suggèrent une utilisation des services de courriel gratuits sous juridiction des États-Unis d'Amérique (adéquation partielle au RGPD) dans 33,3 % des cas. L'une de ces entreprises a d'ailleurs été condamnée à 50 millions d'euros d'amende par la CNIL, en janvier 2019, pour non respect du RGPD (32).

Pour ce qui est de ProtonMail, il s'agit d'un service privé, de messagerie cryptée, sous juridiction suisse (législation adéquate). Mais il ne s'agit pas d'une MSS.

Trois participants ont déclaré être obligés de recevoir des comptes-rendus par courriels non sécurisés et non anonymisés, « [faute] de messagerie sécurisée pour les hospitaliers » ou car « quelques confrères envoient le compte-rendu par mail sur messagerie [non-sécurisée] et n'ont pas de messagerie sécurisée » ou car « ne [pouvant] pas utiliser [la MSS] pour tous les destinataires ». Cela suggère qu'il faudrait généraliser les MSS à tous les soignants pour une meilleure maîtrise des DPS.

Il est tout à fait légal d'utiliser une messagerie non sécurisée, voire un réseau social, pour communiquer des données de santé. Néanmoins, ces dernières doivent être dé-identifiées au préalable, car le service qui héberge ces données n'est pas un service agréé, et pourrait utiliser ces données à des fins commerciales, ce qui est puni par la loi (33).

Il en va de même pour les ordonnances, qui comportent des DPS du patient (les médicaments renseignent sur les pathologies dont le patient souffre) et qui renseignent également sur les habitudes de prescription du médecin (habitudes qui ne peuvent pas être collectées à des fins commerciales si le médecin est identifiable). Ainsi, la transmission d'ordonnance via des applications non agréées ne semble pas conforme à la loi (33).

Parmi les précisions apportées dans les champs libres, un participant a dit anonymiser les DPS qu'il envoie par courriel « de plus en plus, suite à l'intervention du Pr. [Bruno] PY ». Le Pr. Bruno PY est un professeur français de droit privé et sciences criminelles, spécialisé en droit pénal et en droit médical (34). Il donne régulièrement des conférences sur le droit médical à La Réunion. Cela suggère que les interventions de sensibilisation des soignants sont importantes pour parvenir à une meilleure maîtrise des DPS de leurs patients.

## Secrétariat

Les résultats suggèrent que 82,9 % des médecins interrogés emploient au moins une personne au secrétariat. Les secrétaires auraient accès au dossier médical dans 94,9 % des cas, IC[80,9-98,8]. Cela pourrait être expliqué par l'évolution du métier de secrétaire médical, avec une augmentation de la délégation des tâches (35)

La loi rappelle que le secret professionnel s'impose à tous les professionnels intervenant dans le système de santé. Cela vaut également pour les secrétaires du cabinet médical, mais également pour toute personne qui intervient au cabinet médical pour une raison professionnelle (agent d'entretien, informaticien, électricien, etc) (36).

Ce secret professionnel, inscrit dans la loi, est à différencier du devoir de discrétion inscrit dans le contrat des secrétaires médicales. Ce dernier concerne plutôt la gestion du cabinet (son fonctionnement, l'état et la gestion de ses finances, etc.) et non pas les informations de santé des patients.

Idéalement, la CNIL recommande que le secrétariat médical ne devrait pouvoir accéder qu'aux informations nécessaires à l'accomplissement de son métier (ce qui dépend des tâches qui lui sont confiées) sans accès au dossier médical dans sa globalité (3,37).

## Consultations hors cabinet

Les résultats suggèrent que les médecins de la population étudiée réalisaient des consultations hors de leur cabinet dans 97,8 % des cas. Quinze virgule deux pourcents (IC[7,2-29,2]) d'entre eux semblaient accéder à leur logiciel métier à distance. Notons que seulement 2 participants proposaient des consultations de télémédecine, ce qui peut être expliqué par la nouveauté du remboursement de cette consultation à distance.

Sept participants (100 % n=7) qui accédaient à leur logiciel métier à distance ont répondu avoir un logiciel d'accès au bureau à distance.

## 4.3 Les limites de cette étude

### Représentativité

À la Réunion au 1er Janvier 2018, 757 des 1 165 médecins généralistes en activité (65 %) exerçaient en libéral (23). Parmi ces 757 médecins généralistes, 700 étaient inscrits à la lettre d'information de l'URML-OI et 49 ont répondu au questionnaire, soit 6,4 %. Avec cette taille d'échantillon, la marge d'erreur se situe entre 14 % et 15 % pour un niveau de confiance de 95 %. Ainsi, les résultats ne peuvent que suggérer une tendance à certaines pratiques sans que nous soyons certains qu'ils reflètent bien les pratiques actuelles des médecins généralistes.

### Biais

Outre la marge d'erreur due à la taille de l'échantillon, les résultats de cette étude sont à interpréter avec prudence, du fait de la présence de plusieurs biais, dont au moins deux biais de sélection :

– biais de recrutement, avec le choix d'envoyer uniquement par courriel un questionnaire qui porte sur l'informatisation. Cependant, les résultats suggèrent que l'utilisation de dossiers patients informatisés dans la population étudiée (95,9 %, IC[84,4-99]) était comparable à celle des médecins métropolitains (96 %) (1).

– biais de volontariat, avec un risque de participation plus élevée parmi les médecins ayant un attrait pour l'informatique en général, ou pour la sécurité informatique et la protection des données. Remplir ce questionnaire demandait une certaine compétence en informatique. Néanmoins, les tests préalables ont permis de le simplifier au maximum afin d'améliorer sa faisabilité.

Nous pouvons également évoquer un biais de classement, avec des réponses volontairement erronées par crainte de compromettre des informations sensibles en cas de ré-identification. C'est la crainte qu'a exprimé un participant en précisant avoir volontairement répondu « Ne sait pas » aux questions concernant la présence ou non de différents types de caractères employés dans le mot de passe.

### Les questions qui manquent

Dans une volonté d'améliorer sa faisabilité, le questionnaire a été raccourci au détriment de certaines questions, dont certaines concernaient les moyens physiques pour sécuriser le matériel du cabinet, dont les machines contenant les DPS des patients. Ainsi, nous n'avons pas d'information sur l'utilisation d'alarmes incendies, de détecteur de mouvements, de

coffres étanches et/ou ignifugés. Pourtant, leur utilisation est recommandée par la CNIL dans le cadre du RGPD.

Le questionnaire ne comportait pas de questions sur la restriction des droits d'accès des secrétaires. Trois participants ont précisé dans les champs « Précision » que les informations du dossier médical étaient « filtrables » et que les droits d'accès étaient « uniques pour chaque utilisateur, différents pour la secrétaire […] » ou « limité[s] ». Le questionnaire aurait pu demander quelles tâches étaient confiées aux secrétaires et les comparer avec la restriction des droits d'accès qui leur était imposée.

Le questionnaire ne comportait pas de questions sur les moyens employés lors des consultations de télémédecine (2 participants déclaraient en proposer). Utilisaient-ils une application agréée ? Comment communiquaient-ils leurs ordonnances ? De même, il n'y avait pas de question sur les moyens employés par les participants pour accéder à leur logiciel médical à distance.

Le questionnaire aurait pu s'intéresser à la part d'utilisation de logiciels libres, et/ou comparer les logiciels utilisés par les médecins avec ceux recommandés par le gouvernement français via le Socle interministériel des logiciels libres (38)

Le questionnaire s'est intéressé au système d'exploitation employé, mais sans questionner sur le paramétrage de ce dernier. En effet, certains paramétrages sont recommandés par l'ANSSI afin de préserver le respect de la vie privée et de la confidentialité des données, par exemple sous Windows 10 (39). Ainsi, il est recommandé de désactiver l'assistant vocal Cortana en milieu professionnel. De même, le questionnaire aurait pu comporter des questions sur les plugins des navigateurs internet utilisés, dans la mesure où ceux-ci présentent un risque de sécurité supplémentaire, quel que soit le navigateur.

Concernant le système d'exploitation, le questionnaire aurait pu faire préciser la version de Windows utilisée, car les versions de Windows antérieures à Windows 10 ne sont plus maintenues à partir du 14 janvier 2020 (26).

## 4.4 Comment améliorer la maîtrise des médecins généralistes libéraux concernant la sécurité des données personnelles de leurs patients ?

### Améliorer les freins à la mise en place des consignes de sécurité

Parmi les freins identifiés par les participants, le plus représenté semble être le manque de connaissance technique (70,2 % étaient d'accord). Venait ensuite le manque d'information sur les consignes de sécurité (55,3 %), puis le manque de temps nécessaire à leur mise en place (46,8 %). Seulement 34 % des participants considéraient que la contrainte était trop grande par rapport au risque encouru. Le coût de leur mise en place concernait 19,1 % des participants (le budget informatique annuel global était estimé à 2974 euros en moyenne). Parmi les autres freins cités, le « manque d'adaptation [des correspondants] à la messagerie sécurisée » est cité deux fois.

### Ce qui dépend d'un informaticien

Les résultats suggèrent un manque de connaissance concernant plusieurs aspects techniques de la sécurité informatique. Comme l'a souligné un participant dans un champ « Précision », cette sécurité ne « devrait jamais dépendre du praticien, qui n'est ni informaticien […] ni hacker. » Ainsi, la sécurité du cabinet pourrait être renforcée par sa sous-traitance à un informaticien, avec pour consignes de tendre vers le respect des recommandations du RGPD.

### Ce qui dépend des médecins

L'anonymisation des courriels hors utilisation d'une MSS semble être réalisée dans 5,9 % des cas (IC[0,8-33,7]). Comme le suggère la précision d'un participant, cela pourrait être amélioré par une meilleure campagne de sensibilisation et d'intervention d'experts tels que le Pr. Bruno PY auprès des professionnels de santé.

Anonymiser ou plutôt dé-identifier des DPS demande une certaine maîtrise de l'outil informatique, comme le précise un participant qui écrit : « Je ne sais pas comment anonymiser les mails. » Nous pourrions imaginer un tutoriel de dé-identification à destination des professionnels de santé, ou encore intégrer les techniques de dé-identification des DPS dans le cursus des études de santé.

Accepter d'utiliser des mots de passe complexes, de ne pas retenir les mots de passe de son navigateur, est difficilement acceptable aussi bien par la population générale que par les médecins. Est-ce la peur d'oublier son mot de passe ? Considérons-nous comme une perte de temps de renseigner un champ « mot de passe » ? Pourtant, n'est-ce pas à force de ne pas

employer nos mots de passe régulièrement, parce qu'il est retenu dans notre navigateur, que nous finissons par l'oublier ?

Pour sensibiliser les médecins sur les principales problématiques soulevées par cette étude, une fiche d'aide à la sécurisation des DPS va être rédigée et leur sera transmise.

## Ce qui dépend des développeurs

Certaines applications, par exemple le DMP, doivent fournir une haute garantie de sécurité concernant leurs DPS. Ainsi, il n'est pas possible de choisir un mot de passe faible pour s'y connecter, car l'application ne le permet pas. De même, l'identifiant qui permet de se connecter au DMP n'est pas une simple adresse courriel, ni un simple nom d'utilisateur. Ces précautions, qui obligent les utilisateurs à renforcer la sécurité de leurs données, pourraient être généralisées au niveau des logiciels médicaux.

L'avenir est-il aux logiciels métiers « en ligne » ? Les résultats suggèrent qu'ils étaient utilisés dans 12,7 % des cas. Avec ces logiciels, les sauvegardes et la protection physique des DPS est garantie par l'entreprise gestionnaire du logiciel (hébergeurs agréés de données santé). Reste à la charge du médecin de sécuriser son accès (via internet) à ces données, notamment grâce à un mot de passe suffisamment robuste. L'inconvénient de ce type de logiciel métier pourrait être de dépendre de la qualité du réseau internet et de ses éventuelles coupures (accidentelles ou criminelles, par attaque par déni de service). Un autre inconvénient est lié au fait de centraliser une quantité importante de DPS : ces hébergeurs pourraient devenir une cible de choix pour les cybercriminels, tout comme le sont les hébergeurs des DPS des établissements de soins.

## Ce qui dépend d'une stratégie plus globale

Les résultats suggèrent une utilisation de courriel dans 68 % des cas, mais une utilisation d'une MSS dans 53,1 % des cas. Comme le suggèrent les précisions des participants, l'utilisation des MSS pourrait augmenter si l'on généralisait son attribution à tous les professionnels de santé, par exemple en attribuant automatiquement une MSS à chaque professionnel de santé, par exemple dès son entrée dans les études de santé.

## Poursuivre le combat contre la marchandisation des données personnelles et pour un « Internet libre, décentralisé et émancipateur »

Parmi les précisions apportées par les participants en fin de questionnaire, 3 participants semblent exprimer leur scepticisme sur la capacité des médecins à sécuriser les DPS de leurs patients : « Je pense qu'il est illusoire de penser protéger nos données. Quoi que l'on fasse cela nous dépasse largement », « Si quelqu'un veut nous pirater, je pense que cela doit être

facile puisque des sites officiels [mieux] protégés […] que nous sont piratés. Il n'y a plus de secret médical » et « C'est impossible, je le sais, et agis en mon âme et conscience dans le respect du secret médical absolu ».

Une autre précision de fin de questionnaire semble questionner sur la déshumanisation que pourrait engendrer l'informatisation de la pratique médical : « 'Non !' au glissement du temps de contact humain vers la surcharge d'exigences informatiques déshumanisant la pratique médicale. Installé depuis 20 ans c'est cela qui me fera quitter prématurément la profession. » Un avis qui rejoint celui de l'auteur de l'article « Why doctors hate their computers », paru dans The New Yorker (40). Une étude américaine de 2016, cité dans cet article, montrait que pour chaque heure allouée à la clinique, deux heures étaient allouées à la maintenance du dossier informatisé (41).

Même si plusieurs évènements récents vont dans le sens de ces affirmations, il semble légitime de poursuivre nos efforts. En France, La Quadrature du Net est une association qui promeut et défend les libertés fondamentales dans l'environnement numérique. C'est cette association qui est à l'origine, par exemple, de la plainte qui a mené la CNIL à sanctionner Google à hauteur de 50 millions d'euros (42). À l'heure où le gouvernement français considère comme prioritaire la mise en place du Health Data Hub (43), il semble fondamental de se questionner, avec cette association, sur « la façon dont le numérique et la société s'influencent mutuellement », et d'œuvrer pour « un Internet libre, décentralisé et émancipateur ».

## « Take home message »

La maîtrise des médecins généralistes libéraux quant aux données personnelles de santé de leurs patients pourrait être améliorée par la sous-traitance de la sécurité des logiciels à un informaticien, par la sensibilisation des médecins généralistes concernant les mots de passe et la dé-identification de ces données lors des correspondances non sécurisées, par un design sécurisé des applications de santé, par une généralisation des MSS à tous les personnels de santé et par la poursuite de la réflexion concernant le numérique en général.

# V. Conclusion

L'objectif de cette étude était de décrire la maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de leurs patients, à l'Île de la Réunion en 2019.

Les résultats suggèrent d'une part une certaine maîtrise quant au système d'exploitation, à l'utilisation du Wi-Fi, à l'emploi d'un logiciel métier conforme et à jour, à l'utilisation d'un anti-virus et d'un navigateur non-obsolète et à jour, à l'utilisation sécurisée d'un logiciel d'aide à distance, à la pratique de sauvegardes régulières et à l'extinction du poste de travail lors des absences.

D'autre part, cette maîtrise était améliorable concernant la sécurité du réseau Wi-Fi, la robustesse et le renouvellement du mot de passe, l'utilisation d'une messagerie sécurisée de santé, la dé-identification des données personnelles de santé lors des transmissions non sécurisées, l'utilisation d'un fournisseur de courriel soumis au RGPD, l'utilisation d'un logiciel de suppression sécurisée des données, la déconnexion du logiciel médical lors des absences et lorsque le poste de travail n'est pas éteint et l'utilisation d'un écran de veille verrouillé.

Par ailleurs, le principal frein retrouvé était le manque de connaissance technique concernant la sécurité des DPS. Il semblait y avoir un manque d'information sur la durée recommandée de conservation des données de santé.

Les résultats de cette étude sont à interpréter avec prudence du fait de la petite taille de l'échantillon, mais aussi du fait de la présence de plusieurs biais de sélection et de classement.

Les résultats de cette étude et les freins retrouvés interrogent sur les actions à mener pour améliorer la maîtrise des médecins généralistes libéraux quant aux données personnelles de santé de leurs patients. Elle pourrait être améliorée par la sous-traitance de la sécurité des logiciels à un informaticien, par la sensibilisation des médecins généralistes concernant les mots de passe et la dé-identification de ces données lors des correspondances non sécurisées, par un design sécurisé des applications de santé, par une généralisation des MSS à tous les personnels de santé et par la poursuite de la réflexion concernant le numérique en général.

C'est sur cette base de réflexion qu'une fiche d'aide à la sécurisation a été conçue (annexe IV). Elle a été communiquée aux médecins généralistes ayant demandé à la recevoir, ainsi qu'à l'URML-OI, afin d'être plus largement diffusée aux médecins libéraux.

# Glossaire

**ADRESSE IP** : avec IP pour *Internet Protocol,* numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique. [wikipédia.org]

**ATTAQUE PAR DÉNI DE SERVICE** : Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. [wikipedia.org]

**CLOUD** : Le *cloud computing*, en français l'informatique en nuage, consiste à utiliser des serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet, pour stocker des données ou les exploiter. [wikipedia.org]

**CRYPTÉ** : La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. La cryptographie rend un message inintelligible à autre que qui-de-droit. [wikipedia.org]

**DONNÉE PERSONNELLE DE SANTÉ** : données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne. [cnil.fr]

**HACKER** : en sécurité informatique, un hacker, francisé hackeur ou hackeuse, est un spécialiste d'informatique, qui recherche les moyens de contourner les protections logicielles et matérielles. Il agit par curiosité, en recherche de gloire, par conscience politique ou bien contre rémunération. [wikipedia.org]

**LOGICIEL LIBRE** : Un logiciel libre est un logiciel dont l'utilisation, l'étude, la modification et la duplication par autrui en vue de sa diffusion sont permises, techniquement et légalement, ceci afin de garantir certaines libertés induites, dont le contrôle du programme par l'utilisateur et la possibilité de partage entre individus. [wikipedia.org]

**OS** : Un système d'exploitation (souvent appelé OS — de l'anglais *Operating System*) est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs. [wikipedia.org]

**PARE-FEU** : Un pare-feu (de l'anglais *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets). [wikipedia.org]

**RANÇONGICIEL** : logiciel malveillant qui chiffre des données personnelles puis exige au propriétaire d'envoyer de l'argent en échange de la clé de déchiffrement. [wiktionary.org]

**RE-IDENTIFICATION** : (en anglais : *Data re-identification*) est la pratique qui consiste à associer des données anonymes (aussi appelées « données dé-identifiées ») avec des informations publiques, ou des données auxiliaires, dans le but de découvrir l'identité de la personne à qui les données appartiennent. [wikipedia.org]

**ROBUSTESSE :** (d'un mot de passe) est la mesure de la capacité d'un mot de passe à résister au cassage de mot de passe. On mesure la robustesse d'un mot de passe en estimant le nombre de tentatives nécessaires à un attaquant pour casser le mot de passe. [wikipedia.org]

**Wi-Fi** : (contraction de « *Wireless Fidelity* ») ensemble de protocoles de communication sans fil. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem internet, etc). au sein d'un réseau informatique afin de permettre la transmission de données entre eux. [wikipedia.org]

**WEP** : (Wired Equivalent Privacy) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. [wikipedia.org]

**WPA/WPA2-PSK** : (Wi-Fi Protected Access) mécanismes pour sécuriser les réseaux sans-fil de type Wi-Fi. Il a été créé au début des années 2000 en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP. [wikipedia.org]

# Références bibliographiques


1. IPSOS. Les médecins à l'ère du numérique. ASIP Santé. 31 janv 2017;

2. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3. CNIL. Guide de la CNIL sur la sécurité des données personnelles. 2018.

4. Orcutt M. Hackers May Target the Health-Care Industry in 2015 [Internet]. MIT Technology Review. [cité 21 juin 2018]. Disponible sur: https://www.technologyreview.com/s/533631/2015-could-be-the-year-of-the-hospital-hack/

5. Orcutt M. Hospitals Are Getting Hacked More Frequently [Internet]. MIT Technology Review. [cité 21 juin 2018]. Disponible sur: https://www.technologyreview.com/s/530411/hackers-are-homing-in-on-hospitals/

6. Vos données médicales sont revendues, vous le saviez? [Internet]. RTBF Info. 2017 [cité 4 juin 2018]. Disponible sur: https://www.rtbf.be/info/belgique/detail_vos-donnees-medicales-sont-revendues-vous-le-saviez?id=9728058

7. Dumons O. Des hôpitaux français eux aussi victimes de chantage informatique. Le Monde.fr [Internet]. 24 févr 2016 [cité 4 juin 2018]; Disponible sur: https://www.lemonde.fr/pixels/article/2016/02/24/des-hopitaux-francais-eux-aussi-victimes-de-chantage-informatique_4870885_4408996.html

8. Reynaud F. Dans les hôpitaux français, « le vrai, gros piratage n'a pas encore eu lieu ». Le Monde.fr [Internet]. 9 juill 2017 [cité 4 juin 2018]; Disponible sur: https://www.lemonde.fr/pixels/article/2017/07/09/dans-les-hopitaux-francais-le-vrai-piratage-le-gros-il-n-a-pas-encore-eu-lieu_5158152_4408996.html

9. A Singapour, un piratage d'ampleur touche le système de santé. 20 juill 2018 [cité 26 nov 2018]; Disponible sur: https://www.lemonde.fr/pixels/article/2018/07/20/a-singapour-un-piratage-d-ampleur-touche-le-systeme-de-sante_5334108_4408996.html

10. RGPD : un hôpital portugais écope de € 400'000 d'amende | NTIC [Internet]. Droit & Nouvelles Technologies. 2018 [cité 18 avr 2019]. Disponible sur: https://ntic.ch/rgpd-un-hopital-portugais-ecope-de-e400000-damende/

11. Karp P. Police can access My Health Record without court order, parliamentary library warns. The Guardian [Internet]. 24 juill 2018 [cité 16 janv 2019]; Disponible sur: https://www.theguardian.com/australia-news/2018/jul/25/police-can-access-my-health-record-without-court-order-parliamentary-library-warns

12. Karp P, Knaus C. GPs and social service providers demand My Health Record protections. The Guardian [Internet]. 26 juill 2018 [cité 16 janv 2019]; Disponible sur: https://www.theguardian.com/australia-news/2018/jul/27/gps-and-social-service-providers-demand-my-health-record-protections

13. Knaus C. My Health Record: former privacy head warned of dangers six years ago. The Guardian [Internet]. 30 juill 2018 [cité 16 janv 2019]; Disponible sur: https://www.theguardian.com/australia-news/2018/jul/30/my-health-record-former-privacy-head-warned-of-dangers-six-years-ago

14. Brami G. Protection des données patients informatisées en médecine générale. 2007.

15. CSA - Protection des données personnelles [Internet]. csa.eu. [cité 19 avr 2019]. Disponible sur: https://www.csa.eu/fr/survey/les-français-et-la-protection-de-leurs-donnees-personnelles

16. Droit à l'oubli: la France en tête des demandes. 15 juill 2015 [cité 4 avr 2019]; Disponible sur: https://www.lemonde.fr/pixels/article/2015/07/15/droit-a-l-oubli-la-france-en-tete-des-demandes_4684029_4408996.html

17. Ameli.fr. La téléconsultation [Internet]. 2019 [cité 16 janv 2019]. Disponible sur: https://www.ameli.fr/assure/remboursements/rembourse/teleconsultations/teleconsultation

18. ASIP Santé. Fiche pratique : le Dossier Médical Personnel et la sécurité [Internet]. 2011 [cité 17 janv 2019]. Disponible sur: https://leo-lp.pagesperso-orange.fr/these/ASIPsante_DMP_et_securit%C3%A9_juin2011.pdf

19. Davey M. Private health sector most vulnerable to data breaches – report. The Guardian [Internet]. 31 juill 2018 [cité 16 janv 2019]; Disponible sur: https://www.theguardian.com/technology/2018/jul/31/private-health-sector-most-vulnerable-to-data-breaches-report

20. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) [Internet]. OJ L, 32016R0679 mai 4, 2016. Disponible sur: http://data.europa.eu/eli/reg/2016/679/oj/fra

21. Calculatrice de taille de l'échantillon : Comprendre les tailles d'échantillon | SurveyMonkey [Internet]. [French] SurveyMonkey. [cité 18 janv 2020]. Disponible sur: https://fr.surveymonkey.com/mp/sample-size-calculator/

22. data.meta.name. Framasoft - Changer le monde, un octet à la fois. [Internet]. [cité 17 janv 2019]. Disponible sur: https://framasoft.org/fr/charte/

23. Bouet P, Mourgues J-M. Approche territoriale des spécialités médicales et chirurgicales. Conseil national de l 'Ordre des médecins; 2018.

24. Desktop Operating System Market Share France [Internet]. StatCounter Global Stats. [cité 18 avr 2019]. Disponible sur: http://gs.statcounter.com/os-market-share/desktop/france

25. ASIP Santé. Les solutions labellisées [Internet]. 2018 [cité 21 janv 2019]. Disponible sur: http://esante.gouv.fr/services/labellisation/les-solutions-labellisees

26. Agence nationale de la sécurité des systèmes d'information. Les systèmes et logiciels obsolètes. 2017.

27. Idrissi Kandri Y. Sauvegarde des informations médicales informatisées chez les médecins généralistes ambulatoires [Internet]. 2019 [cité 18 avr 2019]. Disponible sur: http://pepite.univ-lille2.fr/notice/view/UDSL2-workflow-11867

28. EaseUS Todo Backup - Backup Options [Internet]. [cité 27 août 2019]. Disponible sur: https://www.easeus.com/support/todo-backup/backup-options.html

29. CNIL, CNOM. Guide pratique sur la protection des données personnelles. 2018.

30. Charte pour la sécurité des courriers électroniques [Internet]. ANSSI. [cité 4 avr 2019]. Disponible sur: https://www.ssi.gouv.fr/particulier/precautions-elementaires/charte-pour-la-securite-des-courriers-electroniques/

31. Transférer des données hors de l'UE | CNIL [Internet]. [cité 3 sept 2019]. Disponible sur: https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

32. Données personnelles : la CNIL condamne Google à une amende record de 50 millions d'euros. 21 janv 2019 [cité 18 avr 2019]; Disponible sur: https://www.lemonde.fr/pixels/article/2019/01/21/donnees-personnelles-la-cnil-condamne-google-a-une-amende-record-de-50-millions-d-euros_5412337_4408996.html

33. Code de la santé publique - Article L4113-7. Code de la santé publique.

34. Bruno Py. In: Wikipédia [Internet]. 2019 [cité 28 août 2019]. Disponible sur: https://fr.wikipedia.org/w/index.php?title=Bruno_Py&oldid=157061235

35. Chanu A, Caron A, Ficheur G, Berkhout C, Duhamel A, Rochoy M. Préférences des médecins généralistes libéraux en France métropolitaine quant à la délégation des tâches médico-administratives aux secrétaires assistant(e)s médico-social(e)s : étude en analyse conjointe. Rev DÉpidémiologie Santé Publique. mai 2018;66(3):171-80.

36. Code de la santé publique - Article L1110-4. Code de la santé publique.

37. RGPD et professionnels de santé libéraux : ce que vous devez savoir | CNIL [Internet]. [cité 20 sept 2019]. Disponible sur: https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir

38. Socle Logiciels Libres | Les documents de référence du S.I. de l'État [Internet]. [cité 3 juin 2019]. Disponible sur: http://references.modernisation.gouv.fr/socle-logiciels-libres

39. ANSSI. Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10. 2017.

40. Gawande A. Why Doctors Hate Their Computers. 5 nov 2018 [cité 28 août 2019]; Disponible sur: https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers

41. Sinsky C, Colligan L, Li L, Prgomet M, Reynolds S, Goeders L, et al. Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties. Ann Intern Med. 6 déc 2016;165(11):753.

42. Première sanction contre Google suite à nos plaintes collectives [Internet]. La Quadrature du Net. 2019 [cité 4 sept 2019]. Disponible sur: https://www.laquadrature.net/2019/01/21/premiere-sanction-contre-google-suite-a-nos-plaintes-collectives/

43. Hourdeaux J. «Health Data Hub»: le méga fichier qui veut rentabiliser nos données de santé [Internet]. Mediapart. [cité 20 janv 2020]. Disponible sur: https://www.mediapart.fr/journal/france/221119/health-data-hub-le-mega-fichier-qui-veut-rentabiliser-nos-donnees-de-sante

# Annexe I – Questionnaire

Le questionnaire en ligne est disponible à l'adresse suivante :

https://framaforms.org/securite-des-donnees-personnelles-de-sante-des-patients-1528374835/

*QRCODE 1: QR code du questionnaire*

| n° | Intitulé | Réponses possibles |
|---|---|---|
| **1** | Vos dossiers médicaux sont-ils informatisés ? | Oui / Non |
| | Si oui, passer à la question n°3 | |
| **2** | Si non, pourriez-vous en préciser les principales raisons ?<br>Puis passer à la question n°80 | Champ libre |
| **3** | Qui se charge habituellement de votre matériel et de la maintenance des logiciels informatiques ? (Question à choix multiples) | - Vous-même<br>- Un informaticien<br>- Votre associé<br>- Votre secrétariat<br>- Personne en particulier<br>- Je ne sais pas |
| **4** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **5** | Quel système d'exploitation (OS) utilisez-vous pour vos dossiers médicaux ? | - Microsoft Windows<br>- Apple MacOS<br>- Autre<br>- Je ne sais pas |
| **6** | Si vous avez répondu « Autre », précisez le nom du système d'exploitation : | Champ libre |
| **7** | Si vous avez répondu « Microsoft Windows », quelle version de Microsoft Windows utilisez-vous ? | - Windows 7, 8 ou 10<br>- Autre<br>- Je ne sais pas |
| **8** | Si vous avez répondu « Apple MacOS », quelle version de Apple MacOS utilisez-vous ? | - OS X Yosemite, El Capitan, Sierra ou High Sierra<br>- Autre<br>- Je ne sais pas |
| **9** | Quelle(s) machine(s) utilisez-vous pour accéder au dossier médical ? | - Ordinateur portable<br>- Ordinateur fixe<br>- Tablette<br>- Téléphone intelligent (smartphone)<br>- Je ne sais pas |
| **10** | Emportez-vous parfois une de ces machines hors du cabinet médical ? | Oui / Non / Je ne sais pas |
| **11** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **12** | Votre poste de travail est-il connecté à Internet en WIFI ? | Oui / Non / Je ne sais pas |
| **13** | Si oui à la question n°12, proposez-vous à vos patients de se connecter au même réseau WIFI que le vôtre ? | Oui / Non / Je ne sais pas |
| **14** | Si oui à la question n°12, l'accès à votre réseau WIFI est-il protégé par un mot de passe ? | Oui / Non / Je ne sais pas |

| | | |
|---|---|---|
| **15** | Si oui à la question n°14, votre mot de passe WIFI est-il noté sur un papier de manière à être visible depuis votre poste de travail ? | Oui / Non / Je ne sais pas |
| **16** | Si oui à la question n°14, votre mot de passe WIFI fait-il au moins 12 caractères ? | Oui / Non / Je ne sais pas |
| **17** | Si oui à la question n°14, quel chiffrement utilise votre réseau WIFI ? | - WPA/WPA2-PSK<br>- Autre<br>- Je ne sais pas |
| **18** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **19** | Quel logiciel médical utilisez-vous ? | Champ libre |
| **20** | Utilisez-vous la dernière version de ce logiciel ? | Oui / Non / Je ne sais pas |
| **21** | Concernant votre identifiant pour vous connecter au logiciel médical : | - L'identifiant est pré-enregistré dans le logiciel<br>- Je dois taper mon identifiant à chaque connexion<br>- Je ne sais pas |
| **22** | Utilisez-vous un mot de passe pour y accéder ? | Oui / Non / Je ne sais pas |
| | Si non, passez à la question n°31 | |
| **23** | Si oui à la question n°22, quelle est la longueur de votre mot de passe ? | - Moins de 4 caractères<br>- 4 caractères<br>- 5 caractères<br>- Au moins 5 caractères, mais moins de 8 caractères<br>- Au moins 8 caractères, mais moins de 12 caractères<br>- Au moins 12 caractères<br>- Je ne sais pas |
| **24** | Si oui à la question n°22, possède-t-il une majuscule ? | Oui / Non / Je ne sais pas |
| **25** | Si oui à la question n°22, possède-t-il une minuscule ? | Oui / Non / je ne sais pas |
| **26** | Si oui à la question n°22, possède-t-il un chiffre ? | Oui / Non / Je ne sais pas |
| **27** | Si oui à la question n°22, possède-t-il un caractère spécial ? Par exemple : un point d'exclamation ou d'interrogation, une apostrophe, « @ », « # »… | Oui / None / Je ne sais pas |
| **28** | Si oui à la question n°22, votre mot de passe est-il noté sur un papier de manière à être visible depuis votre poste de travail ? | Oui / Non / Je ne sais pas |
| **29** | Si oui à la question n°22, renouvelez-vous votre mot de passe tous les ans ? | Oui / Non / Je ne sais pas |
| **30** | Si oui à la question n°22, est-ce que le nombre de tentative d'accès au dossier médical est limité en cas d'erreur de mot de passe ? | Oui / Non / Je ne sais pas |

| | | |
|---|---|---|
| **31** | Votre carte CPS est-elle nécessaire pour accéder aux données du logiciel médical ? | Oui / Non / Je ne sais pas |
| **32** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **33** | Combien de secrétaires travaillent à votre cabinet ? | Valeur numérique |
| **34** | Si ≥ 1 à la question n°33, les secrétaires ont-ils accès au dossier médical ? | Oui / Non / Je ne sais pas |
| **35** | Si ≥ 1 à la question n°33, les secrétaires ont-ils connaissance de vos identifiants et mots de passe ? | Oui / Non / Je ne sais pas |
| **36** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **37** | Vos remplaçants ont-ils des identifiants spécifiques ? | Oui / Non / Je ne sais pas |
| **38** | Si oui à la question n°37, renouvelez-vous cet identifiant à chaque nouveau remplaçant ? | Oui / Non / Je ne sais pas |
| **39** | Vos remplaçants ont-ils un mot de passe spécifique ? | Oui / Non / Je ne sais pas |
| **40** | Si oui à la question n°39, renouvelez-vous ce mot de passe à chaque nouveau remplacement ? | Oui / Non / Je ne sais pas |
| **41** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **42** | Utilisez-vous un logiciel anti-virus ? | Oui / Non / Je ne sais pas |
| **43** | Si oui à la question n°42, votre anti-virus est-il mis à jour automatiquement ? | Oui / Non / Je ne sais pas |
| **44** | Utilisez-vous un logiciel pare-feu ? | Oui / Non / Je ne sais pas |
| **45** | Utilisez-vous un logiciel de dépannage à distance ? Par exemple : TeamViewer, AnyDesk, UltraVNC… | Oui / Non / Je ne sais pas |
| **46** | Si oui à la question n°45, lorsque ce logiciel de dépannage à distance souhaite prendre le contrôle de votre poste, recueille-t-il votre autorisation avec un message de confirmation affiché à l'écran ? | Oui / Non / Je ne sais pas |
| **47** | Si oui à la question n°45, lorsque ce logiciel de dépannage à distance est utilisé, êtes-vous prévenu par un message affiché à l'écran ? | Oui / Non / Je ne sais pas |
| **48** | Quel navigateur internet utilisez-vous le plus souvent ? | - Je ne sais pas<br>- Chrome (Google)<br>- Internet Explorer (Microsoft)<br>- Firefox (Mozilla)<br>- Edge (Microsoft)<br>- Safari (Apple)<br>- Opera (Opera Software)<br>- Autre |
| **49** | Si « Autre », précisez lequel : | Champ libre |

| | | |
|---|---|---|
| **50** | Votre navigateur est-il mis à jour automatiquement ? | Oui / Non / Je ne sais pas |
| **51** | Utilisez-vous l'option « retenir le mot de passe » de votre navigateur ? | Oui / Non / Je ne sais pas |
| **52** | Alimentez-vous le Dossier Médical Partagé (DMP) ? | Oui / Non / Je ne sais pas |
| **53** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **54** | Utilisez-vous l'e-mail pour communiquer des données médicales ? | Oui / Non / Je ne sais pas |
| **55** | Si oui à la question n°54, utilisez-vous systématiquement une messagerie de santé sécurisée pour communiquer des données médicales ? | Oui / Non / Je ne sais pas |
| **56** | Si non à la question n°55, quel autre fournisseur de mail utilisez-vous ? Exemple : gmail.com | Champ libre |
| **57** | Si non à la question n°55, lorsque vous utilisez ce fournisseur, anonymisez-vous systématiquement le contenu de ces mails ? | Oui / Non / je ne sais pas |
| **58** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **59** | Combien de sauvegardes faites-vous par semaine ? | Valeur numérique |
| **60** | Si question n°59 ≥ 1, combien de clés USB utilisez-vous pour sauvegarder vos données ? | Valeur numérique |
| **61** | Si question n°59 ≥ 1, combien de clés disques durs externes utilisez-vous pour sauvegarder vos données ? | Valeur numérique |
| **62** | Si question n°59 ≥ 1, combien de CD-ROM ou DVD utilisez-vous pour sauvegarder vos données ? | Valeur numérique |
| **63** | Si question n°59 ≥ 1, stockez-vous une sauvegarde dans un lieu hors du cabinet ? | Oui / Non / Je ne sais pas |
| **64** | Si question n°59 ≥ 1, stockez-vous une sauvegarde sur internet ou dans le cloud ? | Oui / Non / Je ne sais pas |
| **65** | Si oui à la question n°64, utilisez-vous un hébergeur agréé de données de santé ? | Oui / Non / Je ne sais pas |
| **66** | Si question n°59 ≥ 1, pour effectuer votre sauvegarde, utilisez-vous votre logiciel médical ? | Oui / Non / Je ne sais pas |
| **67** | Si non à la question n°66, quel logiciel utilisez-vous ? | Champ libre |
| **68** | Si question n°59 ≥ 1, combien d'années conservez-vous vos données (0 pour illimité) ? | Valeur numérique |
| **69** | Si question n°59 ≥ 1, lorsque vous n'utilisez plus un de ces supports de stockage, utilisez-vous un logiciel de suppression sécurisée des données ? | Oui / Non / Je ne sais pas |

| | | |
|---|---|---|
| **70** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **71** | Quelles consultations hors de votre cabinet réalisez-vous ? (Question à choix multiples) | - Visites des patients à domicile<br>- Visites des patients en maison de retraite<br>- Visite des patients en crèche<br>- Consultations de télémédecine<br>- Aucune |
| **72** | Autre consultation hors du cabinet : | Champ libre |
| **73** | Si réponse différente de « Aucune » à la question n°71, utilisez-vous un logiciel pour compléter à distance votre dossier médical ? | Oui / Non / Je ne sais pas |
| **74** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **75** | Lorsque vous vous absentez, éteignez-vous votre poste ? | Oui / Non / Je ne sais pas |
| **76** | Si non, lorsque vous vous absentez, déconnectez-vous votre session de votre logiciel médical ? | Oui / Non / Je ne sais pas |
| **77** | Utilisez-vous un écran de veille verrouillé ? (C'est-à-dire un écran de veille qui nécessite un mot de passe pour se déverrouiller) | Oui / Non / Je ne sais pas |
| **78** | Lorsque vous vous absentez, laissez-vous votre carte CPS dans le lecteur ? | Oui / Non / Je ne sais pas |
| **79** | Si vous voulez apporter une précision sur votre manière de procéder, merci de préciser : | Champ libre |
| **80** | À quelle période vous êtes-vous installé dans votre cabinet actuel ? | - Je ne sais pas<br>- Après 2015<br>- Entre 2010 et 2015<br>- Entre 2000 et 2010<br>- Entre 1990 et 2000<br>- Entre 1980 et 1990<br>- Avant 1980 |
| **81** | À quelle période êtes-vous passé aux dossiers informatisés ? | - Je ne sais pas<br>- Après 2015<br>- Entre 2010 et 2015<br>- Entre 2000 et 2010<br>- Entre 1990 et 2000<br>- Avant 1990 |
| **82** | Travaillez-vous en cabinet de groupe ? | Oui / Non / Je ne sais pas |
| **83** | À combien d'euros s'élève le budget informatique annuel global de votre cabinet (main d'œuvre comprise ?) | Valeur numérique (en euros) |

| | | |
|---|---|---|
| **84** | Envisagez-vous de migrer vers un autre système de dossier médical ? (Question à choix multiples) | - Oui, vers un logiciel médical en ligne<br>- Oui, vers un logiciel médical standard<br>- Oui, vers les dossiers papiers<br>- Non<br>- Je ne sais pas |
| **85** | Dans votre cas, quels freins identifiez-vous à la mise en place de toutes les règles de sécurité informatique citées dans ce questionnaire ? (Question à choix multiples) | - Le manque d'information sur ces consignes<br>- Le manque de temps nécessaire à leur mise en place<br>- Le coût de leur mise en place<br>- Le manque de connaissance technique<br>- Une trop grande contrainte comparée aux risques encourus<br>- Autre |
| **86** | Quel(s) autre(s) frein(s) à la mise en place des consignes de sécurité identifiez-vous ? | Champ libre |
| **87** | Avez-vous une remarque ? | Champ libre |

# Annexe II – Lettre d'information de l'URML

## Thèse sur la sécurité des données personnelles de santé

Bonjour et merci de l'intérêt que vous portez à ce projet de thèse.

Dans le but de vous aider à mieux protéger les données personnelles de santé de vos patients, nous vous invitons à participer à cette enquête sur la maîtrise des médecins généralistes quant à la sécurité des données personnelles de santé de leurs patients. Répondre à ce questionnaire anonyme et confidentiel prend moins de 10 minutes en moyenne, et seulement 1 minute si vous n'avez pas de dossiers informatisés !

En vous remerciant d'avance pour votre participation,

Léo Lavaud (Interne en médecine générale) (leo.lavaud@orange.fr)
Dr Michel Bohrer (Directeur de thèse)
Dr Bernard-Alexandre Gauzere (Rapporteur de thèse)

Accèder au questionnaire

https://www.urml-oi.re/ZS/newsletter_54.html#5

# Annexe III – CNIL

L'auteur de cette thèse, Léo LAVAUD, atteste sur l'honneur que sa recherche ne comportera pas la collecte de données personnelles au sens de la Commission Nationale Informatique et Libertés (CNIL) et ainsi ne relève pas de la loi « Informatique et libertés » et ne nécessite pas de déclaration auprès de la CNIL.

# Annexe IV – Fiche d'aide à la sécurisation

Après la soutenance de cette thèse, la fiche suivante sera envoyée par courriel aux 14 médecins qui avaient demandé à la recevoir.

Ce document sera également transmis à l'URML-OI pour une éventuelle diffusion auprès des médecins libéraux de l'Île de la Réunion.

Elle se présente sous la forme d'un dépliant recto-verso intitulé « Petit guide pratique de sécurisation des données patients ».

## Sécuriser le partage des données des patients

La communication des données patient est indispensable entre soignants et internet est un outil de communication très efficace.

| Outil | Partage des données |
|---|---|
| Messagerie Sécurisée de Santé | Possible sans anonymisation |
| Messagerie non sécurisée (Gmail, Orange, etc.) | Possible après anonymisation et dé-identification |
| Textos et MMS | |
| Applications smartphone (Messenger, Whatsapp, Telegram, etc.) | |

Dé-identifier des données, c'est enlever le nom (anonymiser) ainsi que toute information pouvant conduire à l'identification de la personne (date de naissance, numéro de téléphone, numéro de sécurité sociale, adresse…)

**Si le canal n'est pas une messagerie sécurisée de santé, dé-identifiez !**

## Bibliographie


1. Agence nationale de la sécurité des systèmes d'information. Les systèmes et logiciels obsolètes. 2017.
2. ASIP Santé. Les solutions labellisées [Internet]. 2018 [cité 21 janv 2019]. Disponible sur: http://esante.gouv.fr/services/labellisation/les-solutions-labellisees
3. Socle Logiciels Libres | Les documents de référence du S.I. de l'État [Internet]. [cité 3 juin 2019]. Disponible sur : http://references.modernisation.gouv.fr/socle-logiciels-libres
4. Lagane C. L'utilitaire CCleaner compromis par une backdoor [Internet]. Silicon. 2017 [cité 16 janv 2020]. Disponible sur: https://www.silicon.fr/utilitaire-ccleaner-compromis-backdoor-184361.html
5. CNIL, CNOM. Guide pratique sur la protection des données personnelles. 2018.


Retrouvez la thèse complète à l'adresse suivante :
https://leo-lp.pagesperso-orange.fr/these/these.pdf



Feathericons.com @colebemis
https://twitter.com/colebemis

**Pour finir, voici un exemple de dé-identification d'une conversation par application pour smartphone :**


**Après dé-identification :**



**Contact** Léo Lavaud
Interne en Médecine Générale
leo.lavaud@orange.fr


# PETIT GUIDE PRATIQUE DE SÉCURISATION DES DONNÉES PATIENTS

Ce guide a été rédigé à l'issue d'un travail de thèse de médecine générale, dont l'objectif était de décrire la maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de santé de leurs patients, à l'Île de la Réunion en 2019.

## Quelles recommandations semblaient les plus pertinentes au terme de cette étude ?

### Ce qui pouvait être amélioré :

– la **robustesse du mot de passe**, ainsi que son **renouvellement annuel**,
– la communication de données de santé : via une **messagerie sécurisée de santé** ou en **dé-identifiant** les données transmises,
– la déconnexion des services lors des absences et l'utilisation d'un **écran de veille verrouillé**,
– la **suppression sécurisée** des données,
– le **chiffrement du réseau WIFI**.

### Ce que la plupart des participants maîtrisait :

– utilisation de logiciels non-obsolètes et **à jour**,
– réseau WIFI **privé** et protégé par un mot de passe,
– pratique de **sauvegardes régulières et testées**,
– **extinction du poste de travail** lors des absences.

### Pour aller plus loin :

Les pages suivantes détaillent certains aspects de la sécurisation des données des patients.

## Sécuriser les mots de passe

Un mot de passe sert à chiffrer les données : plus il sera complexe, plus une personne ne possédant pas votre mot de passe mettra de temps à accéder à vos données.

Quelle complexité de mot de passe choisir pour votre logiciel médical ?

| Cas de figure | | Complexité |
|---|---|---|
| Cas de figure n°1 : vous devez taper votre identifiant et votre mot de passe | → | 5 caractères minimum |
| Cas de figure n°2 : vous ne devez taper que votre mot de passe | → | 12 caractères minimum<br>1 majuscule<br>1 minuscule<br>1 chiffre<br>1 caractère spécial (par exemple « @ », « & », « # »...) |
| Cas de figure n°3 : vous devez insérer votre carte CPS et taper votre mot de passe | → | 4 caractères minimum |

### Exemple :

Lorsque j'ouvre mon logiciel médical, je n'ai qu'à rentrer mon mot de passe (cas de figure n°2). Un mot de passe suffisamment complexe pourrait être le suivant :

J'ai 3 canards.

En effet, ce mot de passe possède 15 caractères (en comptant les espaces), 1 majuscule, 9 minuscules, 1 chiffre et 2 caractères spéciaux (l'apostrophe et le point).

Navigateur internet : ne choisissez jamais de retenir votre mot de passe car celui-ci pourra alors être facilement récupérable.

Un mot de passe écrit à proximité de votre poste de travail ou dans un fichier sur votre ordinateur réduit sa complexité à néant.

Ne partagez pas le mot de passe WIFI de votre cabinet, changez votre mot de passe WIFI pour un mot de passe suffisamment complexe (cas de figure n°2). Gardez votre modem en sécurité, par exemple dans une armoire fermée à clé. Vérifiez que votre réseau WIFI est chiffré par un protocole autre que WEP-128, qui comporte des failles de sécurité.

Mots de passes à renouveler chaque année.

**Utilisez des « phrases » de passe !**

## Sécuriser le poste de travail

Les mises à jour corrigent les failles de sécurité de vos logiciels. Plus une faille est ancienne, plus le risque qu'elle soit exploitée est grand.

Les logiciels clés de votre poste de travail :

| | |
|---|---|
| Système d'exploitation | – Windows 10 (1)<br>– Mac OS X 10.10 ou supérieur<br>– Linux version LTS |
| Logiciel métier | – Certifié par la HAS<br>– Si possible, le logiciel médical possède une Labellisation standard (2) |
| Anti-virus et pare-feu | – Quel que soit votre système d'exploitation |
| Navigateur Internet | – Firefox (Mozilla) : logiciel libre recommandé par le gouvernement (3)<br>– Chrome (Google)<br>– Edge (Microsoft)<br>– Safari (Apple) |

### Concernant vos logiciels :

Si possible, demandez à ce que les mises à jour soient installées automatiquement.

N'installez qu'un nombre de logiciels limité au strict minimum.

Anti-spyware : non-recommandé depuis que certains anti-spywares gratuits aient été compromis (4).

Il est recommandé de désactiver les assistants personnels vocaux tels que Cortana, Siri, Alexa, etc. qui, pour s'activer, enregistrent en permanence les sons à leur portée.

Un écran de veille verrouillé par un mot de passe empêchera les curieux d'utiliser votre poste lorsque vous devez vous absenter.

**Mises à jour automatiques !**

## Sécuriser les données des patients

La menace numéro une est la destruction des données, par exemple suite à une panne informatique ou un dégât matériel ou logiciel (virus).

Quelle qu'en soit la menace, la seule véritable action de protection de vos données est la sauvegarde :

| | |
|---|---|
| Rythme | 1 fois par semaine minimum |
| Tester les sauvegardes | À chaque sauvegarde si possible, sinon une fois par mois |
| Supports | Disque dur externe |
| Nombre de supports | 2 au minimum |
| Conservation des supports | En dehors du cabinet ou dans un coffre-fort ignifugé |
| Logiciel de sauvegarde | Votre logiciel métier |

Attention au vol de données : n'autorisez pas une personne extérieure au cabinet à recharger ses appareils sur les ports USB de votre ordinateur.

### Concernant les sauvegardes :

La sauvegarde de données de santé sur internet (par exemple dans un Cloud) n'est autorisée que chez des hébergeurs agréés de données de santé.

Lorsque vous n'utilisez plus un disque dur de sauvegarde, les données, même effacées, même après formatage, sont encore récupérables.

Le Conseil National de l'Ordre des Médecins et la CNIL conseillent de conserver les données pour les durées suivantes : 20 ans après la dernière consultation ou 10 ans à compter de la date de décès du patient, avec exception pour le patient mineur (28e anniversaire s'il était mineur lors de cette dernière consultation). En cas d'action tendant à mettre en cause la responsabilité du médecin, il est recommandé de conserver le dossier pour une durée illimitée(5).

**Sauvegardes régulières et testées !**

# Serment d'Hippocrate

Au moment d'être admis à exercer la médecine, je promets et je jure d'être fidèle aux lois de l'honneur et de la probité.

Mon premier souci sera de rétablir, de préserver ou de promouvoir la santé dans tous ses éléments, physiques et mentaux, individuels et sociaux.

Je respecterai toutes les personnes, leur autonomie et leur volonté, sans aucune discrimination selon leur état ou leurs convictions. J'interviendrai pour les protéger si elles sont affaiblies, vulnérables ou menacées dans leur intégrité ou leur dignité. Même sous la contrainte, je ne ferai pas usage de mes connaissances contre les lois de l'humanité.

J'informerai les patients des décisions envisagées, de leurs raisons et de leurs conséquences.

Je ne tromperai jamais leur confiance et n'exploiterai pas le pouvoir hérité des circonstances pour forcer les consciences.

Je donnerai mes soins à l'indigent et à quiconque me les demandera. Je ne me laisserai pas influencer par la soif du gain ou la recherche de la gloire.

Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçue à l'intérieur des maisons, je respecterai les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs.

Je ferai tout pour soulager les souffrances. Je ne prolongerai pas abusivement les agonies. Je ne provoquerai jamais la mort délibérément.

Je préserverai l'indépendance nécessaire à l'accomplissement de ma mission. Je n'entreprendrai rien qui dépasse mes compétences. Je les entretiendrai et les perfectionnerai pour assurer au mieux les services qui me seront demandés.

J'apporterai mon aide à mes confrères ainsi qu'à leurs familles dans l'adversité.

Que les hommes et mes confrères m'accordent leur estime si je suis fidèle à mes promesses ; que je sois déshonoré et méprisé si j'y manque.

# Résumé / Abstract

**TITRE : Étude descriptive de la maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de santé de leurs patients, à la Réunion in 2019.**

**Objectif** : Décrire la maîtrise des médecins généralistes libéraux quant à la sécurité des données personnelles de santé (DPS) de leurs patients.
**Méthode** : Étude déclarative, réalisée de mai à septembre 2019 auprès des médecins généralistes libéraux installés à La Réunion. Questionnaire anonyme réalisé à l'aide des recommandations de la CNIL et diffusé via la lettre d'information de l'Union Régionale des Médecins Libéraux. Analyse statistique descriptive réalisée pour un niveau de confiance de 95 %.
**Résultats et discussion** : Sur 757 médecins inclus, 49 ont répondu au questionnaire. 95,9 % IC[84,4-99] étaient informatisés. D'une part, les résultats suggéraient principalement une maîtrise quant à l'utilisation de logiciels non-obsolètes et à jour, dont un anti-virus (74,5 % IC[59,6-85,2]). Les médecins réalisaient au moins une sauvegarde par semaine (82,9 %). D'autre part, cette maîtrise était améliorable principalement concernant la robustesse et le renouvellement du mot de passe, l'utilisation d'une messagerie sécurisée de santé (MSS) (46,9 % IC[30,1-64,4]) et la dé-identification des DPS (5,9 % IC[0,8-33,7]). Le principal frein retrouvé était le manque de connaissance technique (70,2 %). Le principal biais de l'étude est constitué par la petite taille de l'échantillon.
**Conclusion** : La maîtrise de la sécurité des DPS des patients est améliorable, probablement par la sous-traitance à un informaticien, la sensibilisation des médecins, un design sécurisé des applications de santé, une généralisation des MSS et par la poursuite de la réflexion concernant le numérique en général.

**Mots clés** : données personnelles de santé, sécurité informatique, médecine générale

**TITLE: Inventory of the control of liberal GPs with regards to the security of their patients' personnal health data, in Reunion Island in 2019.**

**Objective**: Describe the general practitioners' management regarding their patients' personal health data (PHD) security.
**Method**: Declarative stud conducted between May and September 2019. Study population included private general practitioners (GP) settled in Reunion Island. Survey was anonymous, made according to CNIL and sent by the Regional Private Practitioners Union's (URML) newsletter. Descriptive statistical analysis was performed with a confidence level of 95 %.
**Results and Discussion**: On 757 GPs included, 49 answered the survey. 95.9 % IC[84.4-99] were computerized. On the one hand, the results mainly suggested a good management regarding the use of non-obsolete and updated software, and the use of an antivirus (74.5 % IC[59.6-85.2]). At least one backup per week was made (82.9 %). On the other hand, PHD's management was improvable regarding password strength, the use of a Health Secure Messaging (HSM) (46.9 % IC[30.1-64.4]) and regarding PHD de-identification (5.9 % IC[0.8-33.7]). Main barrier was the lack of technical knowledge (70.2 %). Main bias is the small sample size.
**Conclusion**: GP's management regarding their patients' PHD could be improved, probably by subcontracting a computer specialist, raising GP's awareness regarding passwords and PHD de-identification, securely designing healthcare applications, generalizing the use of HSM and continue discussions about digital in general.

**Keywords**: health data, computing security, general practice.

**Discipline** : Médecine générale.