UNIVERSITÉ DE LILLE

FACULTÉ DE MÉDECINE HENRI WAREMBOURG

Année : 2020

THÈSE POUR LE DIPLÔME D'ÉTAT

DE DOCTEUR EN MÉDECINE

La sécurité des systèmes d'information en médecine générale

Présentée et soutenue publiquement le jeudi 02 juillet 2020 à 16h
au Pôle Formation

par Lotfallah ZERHOUI

JURY

Président :
Monsieur le Professeur Antoine DRIZENKO
Assesseurs :
Monsieur le Professeur Denis DELEPLANQUE
Monsieur le Docteur Nordine BENKELTOUM
Directeur de thèse :
Monsieur le Docteur Nassir MESSAADI

Table des matières

Introduction

Contexte

Les technologies de l'information et de la communication prennent une place de plus en plus importante dans nos vies quotidiennes, mais aussi dans nos pratiques professionnelles. L'informatisation du secteur de la santé n'est pas un phénomène nouveau comme peuvent en témoigner les évènements suivants :

- La télétransmission des feuilles de soins par Carte vitale, lancée en 1998.
- L'apparition des services en ligne de de l'Assurance Maladie, AMELI Pro, en 2006.
- L'apparition de sites permettant la prise de rendez-vous en ligne, en 2013 (doctolib, pages jaunes...)
- La mise en place de la Rémunération sur objectifs de Santé publique (ROSP), en 2011, contenant un volet incitant à l'informatisation du cabinet.
- L'apparition de logiciels de gestion de cabinet intégralement en ligne, en 2017 (monlogiciel-medical.com, Weda...)
- Le remboursement des actes de téléconsultation par l'Assurance Maladie depuis le 15 septembre 2018.
- Le Dossier médical partagé (DMP) rendu disponible au public depuis le 6 novembre 2018.

De fait, l'outil informatique permet non seulement de gérer les dossiers médicaux, mais aussi de prendre des rendez-vous en ligne, échanger avec d'autres professionnels de santé, communiquer avec

l'Assurance Maladie...

Cependant, toutes les données résultant de l'informatisation des pratiques, auparavant sous format papier confinées au cabinet du praticien, sont devenues vulnérables. Elles peuvent être la cible de cyberattaques, consultées par du personnel non autorisé, ou encore perdues suite à une panne matérielle...

Ainsi, en parallèle de ces évolutions technologiques, le cadre législatif a dû lui aussi évoluer : En France, le droit concernant traitement des données personnelles, est régi par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi informatique et libertés). Cette loi créé la Commission nationale informatique et liberté (CNIL), une autorité administrative française indépendante, ayant pour buts d'informer les citoyens, de protéger leurs droits, accompagner les professionnels pour qu'ils se mettent en conformité mais aussi de contrôler et de sanctionner en cas de manquements [1].

Le 28 mai 2018, le Règlement général sur la protection des données (RGPD), est entré en vigueur. C'est un règlement européen, c'est-à-dire qu'il est "obligatoire dans tous ses éléments et directement applicable à tout État membre" [2]. Le RGPD introduit de nouvelles obligations en faveur des utilisateurs et aggrave les sanctions en cas de manquement pour les personnes traitant des données à caractère personnel. De fait, la loi informatique et liberté s'est vue modifiée en juin 2018 pour que le droit français ne s'oppose pas au droit européen. Les données des dossier médicaux récoltées par les médecins durant leur exercice des soins étant considérées comme des données à caractère personnel, les médecins ont l'obligation de s'y conformer.

C'est à l'occasion de l'entrée en vigueur du RGPD que nous avons décidé de nous intéresser aux pratiques de sécurité des médecins généralistes vis-à-vis des données de santé qu'ils détiennent.

1. https ://www.cnil.fr/fr/les-missions-de-la-cnil
2. article 288 du traité sur le fonctionnement de l'Union européenne du 09 mai 2008

Recherche bibliographiques

Les travaux de recherche menés auprès de médecins libéraux vis-à-vis de la sécurité des systèmes d'information (SSI) ont surtout été menés dans le cadre du développement du DMP [1] [2]. On constate que les médecins ont exprimé des réserves sur la sécurité des données à propos du DMP et sont sensibles aux problématiques de sécurité des données.

D'autres études menées au Royaume-Uni [3] [4] et à Singapour [5], là encore à propos de projets semblables au DMP, ont montré des résultats similaires.

Nous avons donc élargi nos recherches du côté des systèmes d'information hospitaliers. Des études menées en France [6] [7] montraient que les politiques de sécurité informatique en milieu hospitalier étaient inadaptées pour concilier exigences de sécurité, accès par de multiples acteurs et système décentralisé.

D'autres études ont été réalisées aux États-Unis, ces études concluent à une recrudescence des attaques des systèmes d'information du milieu de la santé [8] [9] [10] pour plusieurs raisons :

— l'évolution rapide des technologies et des menaces informatiques
— le management des systèmes d'information insuffisants, avec des comportements délétères des personnels
— le manque d'investissements financiers et humains dans la SSI, avec pour corollaire la facilité d'intrusion par rapport à d'autres structures possédant de données personnelles
— l'augmentation croissante de la valeur des informations médicales sur le marché noir.

Nous avons exclu les travaux menés par des entrprises commercialisant des solutions de sécurité en raison du conflit d'intérêt évident qui se pose.

Hypothèse

L'informatique n'est pas notre métier, le seul cours d'informatique dispensé par l'Université étant le C2i, notre formation initiale ne contient aucune notion de SSI. Les connaissances des médecins généralistes sont donc issus de l'autoformation.

Ainsi au vu des insuffisances constatées en milieu hospitalier et de l'absence de formation initiale, nous sommes partis de l'hypothèse que les médecins généralistes ne maîtrisaient pas suffisamment la SSI pour être en conformité avec le RGPD.

Objectif

Notre objectif est de connaître les moyens mis en œuvre par les médecins généralistes pour assurer la sécurité des données de santé, mais aussi ceux qu'ils ne mettent pas en œuvre et de savoir pour quelles raisons.

Notre but étant de réaliser un état des lieux des différentes pratiques en lien avec la sécurité des données en médecine générale, dans le cadre du RGPD.

Nous discuterons ensuite des différentes failles de sécurité constatées et des solutions qu'il est possible de mettre en place dans le contexte actuel, afin de satisfaire aux obligations du légales du RGPD.

Question de recherche

Qu'est-ce que la sécurité des systèmes d'information pour un médecin généraliste ?

Matériel et Méthode

Mode de recueil et population

Dans cette étude, nous ne cherchons pas à quantifier les pratiques de sécurité, mais à voir lesquelles sont en place et quelles failles peuvent exister, ainsi cette étude est qualitative. Aussi l'entretien individuel semblait être le moyen le plus approprié, car il permet de constater de visu les différentes pratiques de sécurité et de s'assurer de la bonne compréhension des questions. Nous avons pris le parti de réaliser un entretien directif, afin d'avoir un temps d'entretien maîtrisé, mais aussi de pouvoir en faire suffisamment pour explorer un maximum de comportements.

La période de recueil était de six mois, de août 2019 à février 2020, et la zone géographique était limitée aux médecins du Nord et du Pas-de-Calais. Nous nous sommes fixés comme objectif pour cette étude qualitative de réaliser une cinquantaine d'entretiens.

Pour recruter des praticiens, je suis passé principalement par des internes en SASPAS de ma promotion.

Élaboration du questionnaire

Afin d'élaborer le questionnaire, nous avons pris comme sources 2 documents : le RGPD [11] et le guide pratique de la sécurité édité par la CNIL et le conseil national de l'ordre des médecins (CNOM) [12] en juin 2018 à l'occasion de l'entrée en vigueur du RGPD. Ce qui a permis d'extraire

les éléments suivants :

- Les obligations ”administatives” :
  - L’information et le consentement des patients sur le traitement des données.
  - Le recueil des données doit être strictement limité à l’exercice des soins et de l’administration.
  - Le droit d’accès et de rectification des données
  - La tenue d’un registre d’activité de traitement des données
- Les obligations en lien avec la sécurité des données :
  - La restriction de l’accès au lieu de stockage des informations sur support papier
  - La restriction de l’accès au lieu où se trouve le poste de travail
  - L’utilisation de mots de passe forts
  - La communication sécurisée des données de santé avec les médecins et les non-médecins
- Les restrictions à propos des informations récoltées lors des prises de rendez-vous autrement que par le praticien lui-même (secrétaire ou site web) :
  - Seules les informations administratives nécessaires doivent être récoltées
  - Le motif de la consultation ne peut être demandé que s’il implique du matériel spécifique ou une consultation plus longue
  - Il n’y a pas d’obligation de conservation de ces données
- Les recommandations :
  - Nommer un délégué à la protection des données
  - Utiliser une authentification à deux facteurs
  - Se connecter au logiciel de gestion de cabinet via la CPS
  - Verrouiller la session automatiquement en cas d’inactivité de plus de 30 minutes
  - Chiffrer les données de santé
  - Avoir un système d’exploitation, un antivirus et un pare-feu à jour

— Les données de santé doivent être conservées pendant 20 ans

Le questionnaire que nous avons élaboré à partir de cette liste a été découpé en trois parties :

— La première partie porte sur la connaissance du RGPD

— La deuxième partie porte sur la sécurité matérielle et l'accès physique au cabinet.

— Enfin, la troisième partie porte sur la sécurité des données, la gestion des mots de passe et la communicaton des données-patients avec des tiers.

Les points non abordés

Nous n'avons pas exploré certaines problématiques pour les raisons suivantes :

La durée de conservation des données de santé : la CNIL recommande dans son guide [12] p.27, de conserver les données pendant 20 ans à partir de la dernière consultation, en application de l'article R.1112-7 du code de la Santé publique, or cela concerne les établissements de santé, et il n'y a pas d'autre texte de loi applicable aux médecins libéraux.

Les informations prises pour les rendez-vous : cette problématique s'adresse avant tout aux éditeurs de logiciel de prise de rendez-vous en ligne, sur lesquels le praticien n'a pas d'influence.

Le DMP : les problématiques liées à sa sécurité sont gérées par l'Agence du numérique en santé, et non les praticiens.

La télémédecine : c'est un mode de soins très peu diffusé, il représente moins de 1% des consultations, selon l'Assurance Maladie [3]. À noter qu'il y a eu un pic à 11% des consultations en mars 2020 (après la fin du recueil de données), lié à la crise du COVID-19 [4].

3. Dossier de presse de la CNAM : https ://www.ameli.fr/fileadmin/user_upload/documents/DP_1er_anniversaire_du_remboursement_de_la_teleconsultation_sept_2019.pdf

4. Communiqué de presse de la CNAM : https ://www.ameli.fr/fileadmin/user_upload/documents/20200331_-CP_Teleconsultations_Covid_19.pdf

Résultats

Modifications du questionnaire

Il était prévu de poser 59 questions, 30 questions fermées, 29 questions à choix multiples, avec une option de réponse ouverte courte.

6 questions n'ont jamais été posées, car la situation ne s'y prêtait pas.

13 questions reposaient sur l'observation.

Il a fallu reformuler ou préciser 5 questions.

La durée de l'entretien était de l'ordre de 20 minutes.

En annexe se trouve le questionnaire avec les modifications suivantes :

- Pour les questions :
  - en italique : les questions reposant sur l'observation
  - en gras : les précisions ou les reformulations apportées lors de l'entretien
- Pour les réponses :
  - en police normale : les réponses possibles attendues
  - en gras : les réponses données non attendues

Démographie de l'échantillon

Nous avons pu réaliser 50 entretiens. Le tableau suivant montre les caractéristiques de notre échantillon.

Sexe		Âge		Mode d'exercice		Milieu d'exercice	
Femme	16	< 35 ans	8	Seul	5	Rural	13
Homme	34	35-45 ans	13	Groupe	33	Urbain	37
		45-55 ans	15	MSP*	12		
		> 55 ans	14				

Tableau 1 – Démographie de l'échantillon

* : Maison de santé pluridisciplinaire

Connaissance du RGPD

Seuls 3 médecins avaient entendu parler du RGPD. Parmi ceux-ci, les connaissances des obligations étaient vagues. Les notions évoquées étaient : l'obligation de sécurisation des échanges, la sécurisation des données.

L’accès physique

	Accès au cabinet	Accès au bureau de consultation
Pas de clé	0/50	3/50
Clé simple	20/50	31/50 (dont 12 identiques à la clé du cabinet)
Clé sécurisée	26/50	16/50 (dont 4 identiques à la clé du cabinet)
Digicode	4/50	0/50
Personnel ayant accès du bureau de consultation		
Agent d’entretien		37/50
Secrétaire		25/50
Autre professionnel de santé du cabinet		11/50
Interne stagiaire		22/50
Alarme		15/50
Caméra		7/50
Fermeture systématique du bureau de consultation		18/50

Tableau 2 – Aspects de sécurité physique

Globalement l’accès physique au cabinet est bien encadré, la plupart des bureaux de consultation sont fermés à clé, sauf pour 3 praticiens qui ne disposaient pas de serrure pour le bureau de consultation où se trouve l’ordinateur. À noter que pour les 7 médecins disposant d’une caméra, celle-ci est utilisée pour savoir s’il y a des patients en salle d’attente, sans enregistrer les images.

Les documents papier sont numérisés puis détruits pour 35 médecins interrogés. Parmis ceux conservant des archives papier :

— 6 le faisaient dans une pièce dédiée du cabinet fermée à clé.

— 7 le faisaient dans une armoire fermée à clé dans le bureau de consultation.

— 3 le faisaient dans une armoire non fermé à clé dans le bureau de consultation.

L'environnement logiciel

Système d'exploitation		Logiciels de protection	
Windows 10 à jour	23/50	Antivirus	33/50
Windows 10 non à jour	0/50	Parefeu	33/50
Windows obsolète	10/50		
MacOS à jour	10/50		
MacOS non à jour	5/50		
MacOS obsolète	2/50		

Tableau 3 – Enivronnement logiciel

Par ailleurs, tous les médecins interrogés disposaient d'un ordinateur dans le bureau de consultation.

Le système d'exploitation

Certains médecins avaient un système d'exploitation non à jour voire obsolète. Les raisons évoquées pour la non mise à jour du système d'exploitation sont :

— l'ancienneté du matériel

— la crainte d'une panne ou d'une perte de données durant la mise à niveau

— la méconnaissance de l'intérêt de réaliser la mise à niveau

Seuls 7 médecins avaient activé le verrouillage automatique de session. Les raisons évoquées par

les médecins ne l'ayant pas activé sont : la méconnaissance de l'existence de cette fonctionnalité, l'absence d'intérêt pour cette fonctionnalité et la gêne dans l'activité de soins.

Les logiciels de protection

Les utilisateurs de Windows avaient tous un antivirus, toujours à jour. Seuls les utilisateurs de Windows disposaient d'un pare-feu actif, qui était à chaque fois le pare-feu intégré par défaut.

Les utilisateurs de MacOS n'utilisent pas d'antivirus, ils évoquent tous l'idée que les virus sous MacOS n'existent pas. De plus, MacOS dispose d'une pare-feu intégré, cependant celui-ci est désactivé par défaut et aucun praticien ne l'a activé.

La connexion WiFi

Pendant l'entretien, nous avons cherché s'il y avait un accès sans fil au réseau et quel en était la protection. Si tous les réseaux retrouvés étaient protégés par une clé, une clé WEP (une technologie obsolète et facilement cassable) était utilisé chez 3 médecins interrogés.

Les sauvegardes

Tous les médecins interrogés réalisent des sauvegardes régulières. À noter que 17 d'entre eux le faisaient sur le disque dur interne du poste de travail, ce qui peut compromettre les données en cas de panne matérielle.

Les mots de passe

	Mot de passe session	Mot de passe logiciel de gestion de cabinet
Aucun	15/50	7/50
Mot de passe faible	30/50	20/50
Mot de passe fort	5/50	3/50
CPS	0/50	15/50
Double authentification	0/50	5/50
Présence d'un support papier	14/50	
Renouvellement régulier	0/50	

Tableau 4 – La gestion des mots de passe

En ce qui concerne les mot de passe, les pratiques sont variées : de l'absence de mot de passe à la double authentification par SMS en passant par la carte professionnel de santé (CPS). Nous avons pu constater la présence de mots de passe sur papier au bureau de consultation, parfois même le code PIN de la CPS directement sur le lecteur de carte Vitale.

L'absence de mot de passe, les mots de passe simples et la présence d'un support papier sont justifiées par un aspect pratique : celui de faciliter la tâche des remplaçants.

Les quelques médecins qui utilisent des mots de passes complexes ne font pas appel aux remplaçants. Enfin, aucun médecin interrogé ne renouvelle ses mots de passe.

La communication d'informations au sujet des patients

	Professionnel de santé hospitalier	Professionnel de santé en ville	Non professionnel de santé
Courrier	50/50	50/50	50/50
Fax	35/50	0/50	0/50
Conversation téléphonique	40/50	45/50	0/50
SMS/MMS	10/50	24/50	0/50
Messagerie non sécurisé	16/50	26/50	0/50
Messagerie sécurisée	30/50	50/50	0/50

Tableau 5 – Moyens de communications utilisés

Avec les professionnels de santé hospitaliers, les moyens de communication sont variés, mais pas forcément sécurisés. Le fax est encore largement utilisé, le recours à la messagerie personnelle aussi, le téléphone reste le moyen préféré. Cependant, les courriers de sortie d'hospitalisation sont transmis par Apicrypt, lorsque l'hôpital en dispose.

En ville, la communication sécurisée est systématique avec les laboratoire pour les bilan biologiques via Apicrypt. Cependant, lors de la communication avec d'autres professionnels de santé en ville, l'utilisation de messagerie sécurisée n'est pas systématique et passe encore par des canaux non sécurisés comme les SMS ou les mails personnels.

Enfin, les médecins interrogés ne communiquent pas avec des non-professionnels de santé sans l'accord du patient. La pratique courante est l'utilisation d'un courrier remis au patient.

Les pratiques de sécurités en place

Les pratiques de sécurité en place chez les praticiens résultent des paramètres des applications par défaut, ou mises en place par le fournisseur du logiciel de gestion de cabinet. Les différentes failles de sécurité observées imputables au praticien sont faites dans le but de faciliter l'accès aux remplaçants, pour éviter le blocage de la CPS ou permettre à celui-ci de travailler en cas d'oubli.

Discussion

Forces et limites de l'étude

Les contraintes posées par l'organisation d'un entretien individuel nous ont limités dans le nombre de personnes interrogées. Ainsi, un receuil de données par questionnaire envoyés par mail ou par courrier nous aurait permis d'avoir beaucoup plus de répondants.

Cependant, cela nous a permis d'observer le comportement des médecins interrogés, cette observation directe a permis d'avoir un recueil fiable. Nous avons pu récolter des données sans poser la question au médecin, comme la présence de caméra, le type de protection du WiFi, la presence de post-it avec les identifiants sur l'ordinateur...

De plus, nous avions la possibilité d'expliquer les termes qui auraient pu paraître compliqués. Enfin, l'entretien directif a permis d'explorer tous les critères de conformité au RGPD sur une durée raisonnable de 20 minutes environ.

Les risques légaux

La CNIL a laissé jusqu'au 1er janvier 2020 aux différents organismes pour se conformer au RGPD avant de commencer les contrôles. Les règles de contrôle ont depuis été explicitées et sont accessibles sur le site de la CNIL [5]. Les peines prévue par le RGPD sont lourdes : jusqu'à 20 millions d'euros

5. https ://www.cnil.fr/fr/la-chaine-repressive-de-la-cnil

ou jusqu'à 4% du chiffre d'affaires annuel [6]. Il y a 4 types de signalement à la CNIL permettant de déclencher un contrôle :

— Les plaintes des usagers

— L'autosaisine sur des thèmes identifiés comme prioritaires

— Les faits remontés par voie de presse ou sur le web

— La coopération avec d'autres organismes européens homologues à la CNIL

Les 3 dernières formes de signalement ne concerneront vraisemblablement pas le médecin généraliste. En effet, il est peu probable que la CNIL, la presse ou un autre organisme européen s'intéresse à un praticien libéral isolé.

En revanche, un médecin peut se voir contrôlé et sanctionné s'il y a une fuite de données ET que le ou les patients concernés portent plainte. Ce risque est réel et ne doit pas être sous-estimé, comme le montre une affaire jugée en 2017 [7], où une patiente a pu accéder à une base de données médicale en entrant son nom sur Google, et a donc porté plainte. Un médecin avait établi cette base données à des fins de recherche avec les manquements suivants : sans autorisation de la CNIL, sans prévenir la direction des systèmes d'information de l'hôpital où il travaillait, sans sécuriser l'accès aux données, sans en informer les patients, chez un hébergeur non agréé pour héberger des données de santé. Le médecin a alors été condamné à 5000€ d'amende pour "traitement de données à caractère personnel sans autorisation" uniquement. Dans le cadre du RGPD, les autres manquements auraient été pris en compte et auraient mené à une sanction plus sévère.

Enfin, une fuite de données peut s'apparenter à une rupture du secret médical, un médecin encourant alors aussi des poursuites ordinales, cependant, nous n'avons pas pu retrouver de condamnation ordinale en lien avec une fuite de données de santé.

6. RGPD - article 83, paragraphe 6

7. TGI de Marseille, 6ème ch. corr., jugement du 7 juin 2017

Les obligations administratives du RGPD

Les médecins que nous avons interrogés n'avaient pas connaissance des obligations administratives du RGPD, cependant, nous allons voir qu'il est facile d'y remédier

L'information et le consentement des patients

Le RGPD rend l'information des patients obligatoire sur le traitement des données et de leurs droits, mais pas forcément par le praticien oralement pour chaque patient, un affiche ou un dépliant à disposition des patients suffit [8]. Le guide de la CNIL p.27 contient un modèle de fiche d'information qu'il est tout à fait possible de reprendre sur une affiche pour se mettre en conformité.

En revanche, un consentement explicite et positif (comme le RGPD peut l'exiger en cas d'utilisation des données à des fins commerciales, par exemple) n'est pas nécessaire dans les situations de soins "dans la mesure où leur collecte et leur conservation sont nécessaires aux diagnostics médicaux et à la prise en charge sanitaire ou sociale des patients concernés" [9]. Le consentement est toujours nécessaire mais il est tacite, comme le consentement aux soins. C'est un aspect plutôt positif, puisque le RGPD ne vient donc pas altérer la relation médecin-patient.

Le registre des activités de traitement

Ce document introduit par le RGPD est une trace écrite des différentes pratiques de sécurité du praticien et doit être disponible en cas de contrôle par la CNIL.

Ici aussi, il est assez simple de se mettre en conformité puisque la CNIL a mis à disposition un modèle [10], qu'il ne reste qu'à imprimer et remplir. Il est important de ne pas négliger ce document et de bien y consigner tous les actes entrepris pour améliorer la sécurité des données. En effet, de la

8. https ://www.cnil.fr/fr/traitement-de-donnees-de-sante-comment-informer-les-personnes-concernees
9. https ://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir
10. https ://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

même manière qu'un dossier médical bien rempli permet de prouver la bonne conduite du médecin en cas de conflit avec un patient, un registre d'activité bien documenté permet de prouver la bonne foi du médecin en cas de fuite de données.

Délégué à la protection des données et analyse d'impact

La nomination d'un délégué à la protection des données et une analyse d'impact sont obligatoire dès que l'on "traite des données à grande échelle". Le RGPD déclare clairement que "le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients [...] par un médecin [...] exerçant à titre individuel" [11].

Si les hôpitaux et les cliniques sont clairement considérés comme traitant des données à grande échelle [12], pour les praticiens exerçant en cabinet de groupe ou en MSP, la limite de ce qui relève d'un traitement de données à grande échelle n'est pas clairement explicitée par le RGPD. La CNIL ne le définit pas non plus, et indique par ailleurs : "il appartient donc au responsable du traitement de décider de la qualification de son traitement de 'traitement à grande échelle'" [13]. De fait, un cabinet de groupe ou une MSP se rapprochant plus du fonctionnement d'un médecin isolé que d'un hôpital, on peut considérer qu'ils n'entrent pas dans ce cadre, tant que la CNIL ne s'est prononcée clairement.

La sécurité des données

Le système d'exploitation et les logiciels de protection

Avoir un système d'exploitation (OS) à jour est absolument nécessaire, les mises à jour permettant d'améliorer la sécurité en refermant des brèches potentiellement exploitables. Par défaut, les mises à

11. RGPD - "considérant" 91
12. https ://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-un-traitement-grande-echelle-cest-quoi
13. https ://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-un-traitement-grande-echelle-cest-quoi

jour sont proposées, ou installées automatiquement, refuser les mises à jour requiert un effort délibéré. En théorie, en cas de fuite de données, un OS non à jour pourrait donc être un motif de sanction.

La mise à niveau (changer la version de l'OS pour une plus récente) est plus délicate, en effet, Les nouvelles versions des OS demandent souvent plus de ressources et le matériel peut être alors trop ancien pour la supporter. Or, les mises à niveau sont encore plus importantes que les mises à jour car Microsoft et Apple ne distribuent plus de mises à jour de sécurité pour leurs OS les plus anciens, les vulnérabilités nouvellement découvertes ne pouvant alors plus être corrigées. Il n'y a donc pas d'autre choix que renouveler le matériel si celui-ci n'est plus adapté. Il faut cependant être vigilant et réaliser une sauvegarde des données en premier lieu, car une mise à niveau est une opération pouvant induire une perte de données. De plus, le logiciel de gestion de cabinet peut nécessiter d'être reconfiguré. Dans cette situation, le fournisseur du logiciel est l'interlocuteur à contacter afin de se faire accompagner.

Pour ce qui est des logiciels de protection, Windows 10 dispose d'un antivirus et d'un pare-feu intégré qu'il suffit de mettre à jour (ce qui est fait automatiquement par défaut).

En ce qui concerne les ordinateurs Apple, MacOS ne dispose pas d'un antivirus par défaut, il est nécessaire d'en avoir un. L'idée reçue qu'un ordinateur Apple ne nécéssite pas d'antivirus remonte aux années 2000 à l'époque où ils représentaient une faible part de marché, disposaient d'une architecture matérielle et logicielle différente des ordinateurs sous Windows et supposément n'intéressaient pas les personnes mal intentionnées.

Dans le rapport sur les vulnérabilités de 2019 de l'Agence européenne chargée de la sécurité des réseaux et de l'information [13], on peut constater que la plateforme MacOS est aussi sujette à des vulnérabilités majeures de sécurité.

Les sauvegardes

L'objectif des sauvegardes est d'éviter la perte de données, celle-ci peut arriver en raison de 3 causes : la panne logicielle, la panne matérielle et vol. La sauvegarde des données sur le disque dur

dur poste de travail ne protège que des pannes logicielles. il est donc indispensable de réaliser des sauvegardes régulières sur un support externe au poste de travail, en ligne pour les logiciels de gestion de cabinet en ligne, sur un disque dur externe pour les logiciels installé sur l'ordinateur.

La plupart des logiciels de gestion de cabinet disposent d'un outil de sauvegarde des données, une solution simple étant alors de contacter le fournisseur du logiciel pour paramétrer les sauvegardes afin qu'elles se réalisent automatiquement à intervalle régulier. La CNIL recommande une sauvegarde par semaine dans son guide pratique.

La connexion au réseau sans fil

La clé de protection WiFi dépend du matériel, la protection par une clé WPA2 est suffisante et disponible sur tous les materiels récents. La protection par clé WEP est obsolète et très facilement cassable. La solution est de contacter le fournisseur d'accès internet pour mettre à jour l'équipement en cause. Dans tous les cas, si le WiFi n'est pas nécessaire au fonctionnement du cabinet, le désactiver permet de supprimer un point de vulnérabilité facilement.

L'authentification

La restriction de l'accès au données se fait par l'authentification. Le moyen le plus répandu est l'accès par mot de passe, mais il en existe d'autres, comme la double authentification par SMS, où encore par carte professionnel de santé (CPS).

La carte professionnel de santé

La CPS est une carte permettant la signature électronique des feuilles de soins électroniques (FSE) et la télétransmission de celles-ci aux caisses primaires d'assurance maladie (CPAM), elle est délivrée par l'Agence numérique en santé à chaque médecin (interne remplaçant ou non, remplaçant exclusif thésé ou non, et médecin installé). Elle permet aussi l'identification du praticien sur le site AméliPro

et donc l'accès aux téléservices de l'Assurance Maladie.

Selon l'article R161-58 du Code de la sécurité sociale, la signature électronique par CPS est équivalente à une signature manuscrite et interdit le prêt de la CPS. Le prêt de cette carte est donc équivalent à prêter sa signature et donc assimilable à une fraude et passible de poursuites. Le remplaçant est sensé utiliser sa propre carte. Or, tous les médecins interrogés qui se font remplacer donnent leur CPS et le code PIN au remplaçant. Il y a plusieurs raisons évoquées :

— le flou sur la gestion des FSE par la CPAM et le paiement des praticiens
— la difficulté ou l'impossiblité de paramétrer le logiciel de gestion de cabinet pour fonctionner avec la carte du remplaçant
— les CPS des remplaçant n'ont pas accès AmeliPro

Le principal risque est que le médecin titulaire voit sa responsabilité engagée pour des actes réalisés avec sa CPS par le remplaçant, comme des arrêts de travail non justifiés. Dans la pratique, nous n'avons pas trouvé dans la jurisprudence de médecin condamné pour cette pratique.

Par ailleurs, nous avons contacté un ingénieur informatique de la CPAM de Lille. Il nous a informé que cette situation avait déjà été notifié, que le problème était ”d'ordre technique” et ”dû à la gestion de ceux qui remplacent plusieurs praticiens”, et qu'il ”y a une perspective de changement mais pour le moment cette évolution est toujours au stade embryonnaire”.

En dehors du problème légal que pose le prêt de la CPS, la transmission du code PIN est une problématique récurrente pour les médecins faisant régulièrement appel à des remplaçants. La CPS fonctionne comme une carte bleue, 3 erreurs sur le code bloquent la carte, le médecin doit alors commander une nouvelle carte et transmettres des feuilles de soins papier.

Certains font le choix d'inscrire sur papier ce code, parfois même sur le lecteur pour être sûr que le remplaçant ne bloque pas la CPS.

En terme de sécurité, la CPS est la méthode d'authentification la plus fiable à disposition. Elle a l'avantage d'être en possession de tous les médecins en exercice. Les éditeurs de logiciels médicaux

devraient utiliser systématiquement la CPS comme moyen d'authentification et faciliter le paramétrage des logiciels pour intégrer les remplaçants. Débloquer l'accès à AmeliPro pour les remplaçants est indispensable. Ces trois mesures uniquement logicielles (passant donc "simplement" par des mises à jour) amélioreraient grandement la sécurité des données, puisque chaque médecin n'aurait à retenir que son code PIN et n'aurait pas à le transmette à qui que ce soit.

Créer un bon mot de passe

Les mots de passe permettent de restreindre l'accès aux données des patients, il est donc important d'avoir des mots de passe robustes. La force d'un mot de passe dépend de deux critères : sa complexité et son caractère aléatoire et unique.

La complexité d'un mot de passe aléatoire est évaluée par l'entropie de Shannon. L'entropie reflète le nombre de combinaisons possibles de réaliser pour un mot de passe de longueur L constitué de symboles d'un alphabet A selon la formule suivante : $entropie = log_2(A^L)$
Ainsi une entropie inférieure à 80 est considérée comme faible et une entropie supérieure à 100 est considérée comme forte [14].

Pour augmenter l'entropie d'un mot de passe on peut donc soit augmenter sa longueur, soit augmenter le nombre de symboles différents. La recommendation d'utiliser des majuscules, des minsucules, des chiffres et des caractères spéciaux pour obtenir un mot de passe fort est issue d'un document [14] de 2003 du National institute of standard and technology (NIST, une agence sous le contrôle du gouvernement américaine). Cependant, depuis 2017, le NIST a changé cette recommendation [15] et insiste maintenant sur la longueur du mot de passe. En effet, il a été observé une mauvaise mémorisabilite des mots de passe complexes, poussant alors à des comportements délétères, comme la réutilisation de mots de passe, l'utilisation de mots de passe complexes mais courants.

— "M0t2pA$$e" a une entropie théorique de 67

— "ceciestunmotdepasselongmaissimple" a une entropie théorique de 141

14. https ://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Dans la pratique l'entropie de ces mots de passe est bien plus faible car il ne s'agit pas d'une chaîne de caractères purement aléatoires.

Un autre facteur important de qualité d'un mot de passe est son caractère aléatoire et unique Un mot de passe ne doit pas être lié à la vie personnelle, ne pas être couramment utilisé (comme 123456) ou issu de dictionnaire et être lié à un seul compte. [15]. Un moyen de créer un mot de passe facile à retenir est d'utiliser une phrase de passe : à partir d'une phrase, on prend les initiales de chaque mots et la ponctuation pour en faire un mot de passe. La CNIL propose un outil pour générer ce type de mot de passe. [16]. Ainsi à partir de la phrase : "Le carré de l'hypoténuse est égal à la somme des carrés des 2 autres côtés.", on obtient le mot de passe très robste "Lcdl'heéàlsdcd2ac.".

La gestion des mots de passe

Une autre recommandation fréquente est renouvellement des mots de passe à intervalle régulier, et de ne jamais les écrire nulle part. [17]. Mais le National Cyber Security Center (NCSC, une agence sous le contôle du gouvernement britannique), et le NIST déconseillent de forcer le renouvellement régulier. [16] [15]. En effet, le changement fréquent de mot de passe est une situation où l'utilisateur risque d'oublier le nouveau mot de passe et entraine des comportement à comme :

— le choix de mot de passe plus faible

— l'inscription sur un support papier

— l'utilisation d'un mot de passe déjà utilisé ailleurs

L'attitude recommandée étant alors de renouveler les mots de passe qu'en cas de fuite de données suspectée.

Le problème qui se pose est que si l'on respecte les recommendations précédentes, on se retrouve avec des mots de passes complexes, longs, aléatoires, différents pour chaque compte sans les avoir

15. https ://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
16. https ://www.cnil.fr/fr/generer-un-mot-de-passe-solide
17. https ://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

écrits nulle part. Le risque d'oubli, par exemple après un arrêt de travail prolongé, est donc important.

La première solution est donc de limiter leur nombre en utilisant un gestionnaire de mots de passe par exemple. Un gestionnaire de mots de passe est un logiciel renseignant les mots de passe automatiquement sur les sites web. L'accès au gestionnaire de mot de passe se fait aussi par un mot de passe, mais comme il en remplace potentiellement plusieurs dizaines, l'avantage est indéniable. Cependant, un gestionnaire de mots de passe est inopérant pour se connecter au poste de travail et aussi pour l'accès au logiciel de gestion de cabinet.

On se retrouve au final avec un maximum de 4 mots de passes : le mot de passe de session, le mot de passe du logiciel de gestion de cabinet, le code PIN de la CPS et le mot de passe du gestionnaire du mot de passe (à noter que l'on peut encore en éliminer un si on utililse la CPS comme moyen de connexion au logiciel de gestion de cabinet).

Si l'on craint d'oublier ses mots de passe, on peut envisager de les noter sur un support papier mais de ne pas les conserver au cabinet, mais au domicile dans un endroit où l'on dépose des documents importants régulièrement, comme un classeur de factures, et ne pas noter explicitement ce qu'est ce support (par exemple juste noter la phrase de passe, sans écrire que c'est pour se connecter au logiciel de gestion de cabinet). L'intérêt de conserver ce support dans un lieu que l'on consulte régulièrement permet de remarquer sa disparition, le cas échéant, il faut alors changer les mots de passe et le notifier sur le registre de traitement des données. La perte de ce document pourrait résulter d'un cambriolage ou d'un déménagement et on peut raisonnablement considérer que le risque de cambriolage pour récupérer spécifiquement des mots de passe d'un cabinet médical est bien plus faible que le risque d'oubli d'un mot de passe complexe.

Enfin, lorsqu'un médecin fait appel à un remplaçant il doit lui transmettre les mots de passe. Et si l'on utilise des mots de passe complexe que l'on transmet uniquement oralement, il y a fort à parier que le remplaçant le notera sur un papier ou sur son smartphone. La solution que nous proposons est de noter ces mots de passe sur un support papier mais avec les contraintes suivantes :

— on le donne en mains propre au remplaçant

— on donne la consigne de conserver ce support dans son portefeuille avec sa carte bleue

— on récupère ce support en fin de remplacement

— on détruit ce support à la fin du remplacement

L'idée est que le remplaçant fera attention à son portefeuille et donc indirectement au support des mots de passe. Enfin, la nécessité de récupérer le support pour le détruire est de s'assurer qu'il ne soit pas perdu, dans le cas contraire, on peut alors supecter une fuite de donnée. Il faudra alors changer tous les mots de passe et le notifier sur le registre de traitement des données.

La communication sécurisée

Le RGPD et l'article L1110-4 du Code de la santé publique exigent que la communication de données de santé soit fait au travers d'une messagerie sécurisée, mais l'article L1111-8 du Code de la Santé publique impose en plus que les données soient stockées réalisée par un prestataire certifié. De ce fait, une messagerie sécurisée grand public, même sécurisée par un chiffrement de bout en bout, comme Whatsapp, n'est pas légalement utilisable pour communiquer à propos des patients.

Cependant, il existe plusieurs solutions de messagerie sécurisée instantanée accessibles et gratuites. Il y a par exemple MiSS et Apicrypt Mobile, deux applications de messagerie instantanée utilisant le réseau Apicrypt. Elles ont l'avantage d'être utilisable directement utilisables par les médecins disposant d'une adresse Apicrypt, mais excluent de fait ceux qui n'en ont pas comme les praticiens hospitaliers. Une autre solution simple est d'utiliser PandaLab, une application disposant d'une version gratuite accessible cette fois à tous les professionnels de santé (hospitaliers, infirmières, libéraux). Ainsi, l'utilisation de messageries non sécurisée comme les mails personnels, les SMS, ne sont pas admissibles au regard du RGPD.

En ce qui concerne la communication avec l'hôpital, l'accès aux messageries sécurisées est inégal. Certains centres hospitaliers mettent à disposition une adresse sécurisée pour chacun de ses praticiens,

d'autres n'ont qu'une adresse par service et enfin certains n'en ont pas du tout. À noter que cette situation devra finir par évoluer puisqu'il est fort probable que la CNIL s'intéresse en premier lieu (dans le domaine de la santé) aux hôpitaux pour qu'ils se mettent conformité.

La CNIL émet beaucoup de réserves sur l'utilisation du fax [18] et préconise d'éviter de l'utiliser. Ces informations datent de 2015 et il n'y a pas eu de recommandations nouvelle sur ce sujet. Si la situation l'oblige, le fax peut tout de même être utilisé, ce qui risque vraisemblablement de se produire pour communiquer avec un hôpital ne disposant pas d'une messagerie sécurisée. Dans les cas où une structure de santé oblige à communiquer des données de santé par des canaux non sécurisés, il faut notifier sur le registre d'activités de traitement quels établissements sont en cause pour pouvoir se justifier en cas de contrôle.

Enfin, la communication par téléphone orale est permise, et doit repsecter les impératifs liées au secret médical. La communication par SMS, quant à elle, est interdite au même titre que les messageries personnelles.

18. https ://www.cnil.fr/fr/donnees-de-sante-messagerie-electronique-et-fax

Conclusion

Le RGPD est un texte de loi imposant de obligations nouvelles obligations aux médecins en matière de sécurité des données, sans affecter la relation médecin-patient. La mise en confromité au RGPD n'est pas impossible et des solutions existent pour tous les aspects.

L'obligation d'information et la création d'un registre de traitement des données est simple à mettre en place, grâce aux modèles que fournit la CNIL.

La restriction d'accès au poste de travail et aux documents papiers est nécessaire pour se mettre en conformité, de même que de disposer d'un ordinateur à jour avec des logiciels de protection à jour. Les utilisateurs de MacOS doivent prendre conscience que cette plateforme est vulnérable et nécessite aussi des logiciels de protection.

La gestion des mots de passe est problématique (mots de passe faibles, ou notés sur papier). La nécessité de transmettre les mots de passe aux remplaçants est la principale cause évoquée. L'utilisation de phrases de passe permet la création de mots de passe forts et mémorisables facilement. L'utilisation d'un support papier temporaire pour transmettre les mots de passe est envisageable si l'on applique des règles strictes.

La CPS est le moyen d'authentification le plus sécurisé actuellement à disposition. Cependant, des difficultés logicielles empêchent l'utilisation des CPS des remplaçants et des internes et obligent les médecins à prêter leur carte et divulguer leur code PIN. La résolution de cette problématique est entre les mains de la CNAM et des éditeurs de logiciels médicaux.

En ce qui concerne la communication sécurisée, tous les médecins interrogés disposent d'une mes-

sagerie sécurisée, et s'en servent notamment pour les bilan biologiques et les courriers d'hospitalisation. Cependant l'utilisation de celle-ci entre médecins ou avec d'autres professionnels de santé n'est pas systématique. Des applications de messagerie instantanée existent et rendent l'utilisation de communication non sécurisée (mail personnel, fax, SMS, MMS, messagerie instantanée grand public...) non acceptables.

Bibliographie

[1] Hurtaud A, Dépinoy D. Dossier médical personnel : qu'en pensent les médecins ? Une enquête auprès des médecins de l'agglomération de Reims. Médecine. 2007 Jun ;3(6) :278–282.

[2] Marcelli A, Solaret D. La sécurisation du dossier médical partagé (DMP). Bulletin de l'Académie Nationale de Médecine. 2010 Apr ;194(4) :767–778.

[3] Bouamrane MM, Mair FS. A study of general practitioners' perspectives on electronic medical records systems in NHSScotland. BMC Medical Informatics and Decision Making. 2013 May ;13 :58.

[4] Stahl BC, Doherty NF, Shaw M. Information security policies in the UK healthcare sector : a critical evaluation. Information Systems Journal. 2012 ;22(1) :77–94. _eprint : https ://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2575.2011.00378.x.

[5] Qin Yong S. Attitudes and Perceptions of General Practitioners towards the National Electronic Health Record (NEHR) in Singapore ; 2020. Library Catalog : www.emjreviews.com Section : Uncategorised.

[6] Kalam AAE. Politiques de sécurité pour les systèmes d'informations médicales. 2002 ;.

[7] Béranger J, Mancini J, Dufour JC, Le Coz P. Évaluation éthique des systèmes d'information auprès des acteurs de santé. European Research in Telemedicine / La Recherche Européenne en Télémédecine. 2013 Nov ;2(3) :83–92.

[8] Coventry L, Branley D. Cybersecurity in healthcare : A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul ;113 :48–52.

[9] Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare : how safe are we ? BMJ. 2017 Jul ;358. Publisher : British Medical Journal Publishing Group Section : Analysis.

[10] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare : A systematic review of modern threats and trends. Technology and Health Care. 2017 Jan ;25(1) :1–10. Publisher : IOS Press.

[11] UE. Le règlement général sur la protection des données - RGPD ; 2018.

[12] CNIL, CNOM. Guide pratique sur la protection des données personnelles ; 2018.

[13] ENISA. State of vulnerabilities 2018/2019 ; 2019.

[14] NIST. Special publication 800-63 ; 2003.

[15] NIST. Special publication 800-63 ; 2017.

[16] NCSC. The problem with forcing regular password expiry ; 2016.

Questionnaire

Partie 1 : Le RGPD

1) Avez-vous déjà entendu parler du RGPD **(Règlement général sur la protection des données)** ?
   Oui / Non Si non -> passer à la question 7
2) Savez-vous ce qu'est le RGPD ?
   Oui / Non Si non -> passer à la question 7
3) Connaissez-vous globalement les obligations que le RGPD impose aux médecins ?
   Oui / Non Si non -> passer à la question 7
4) Pensez-vous remplir les obligations imposées par le RGPD ?
   Oui / Non Si oui -> passer à la question 7
5) Qu'est-ce qui vous empêche de remplir les obligations imposées par le RGPD ?
   Pas de solution adapté pour la messagerie sécurisée
   Oubli de mots de passe si trop complexes
6) En ce qui concerne les pratiques de sécurité actuelles **(mots de passe, sauvegardes, messagerie...**), comment les avez-vous mises en place ?
   Paramètres initiaux inchangés
   Autoformation
   Pratiques déjà en place du cabinet
   Autre : **Appel au prestataire du logiciel de gestion de cabinet**
7) Pensez-vous que vos pratiques de sécurité actuelles sont suffisantes, pour protéger les données ?
   Oui / Non Si oui -> passer à la question 9
8) Si non, qu'est ce qui vous empêche de le faire ?
   Pas pratique pour les remplaçants
   Pas les compétences
   Le risque d'attaque est peu probable
   Je n'ai jamais vraiement réfléchi à la question

9) Les patients sont-ils informés de leurs droit vis-à-vis des données **(leur droit de consulter leur dossier, de le faire supprimer)** ?
   Oui / Non
10) Si oui, par quel moyen ? (non posée)
11) Un patient vous a-t-il déjà demandé d'accéder ou de faire supprimer son dossier médical ?
   Oui / Non
12) Avez-vous accédé à sa demande ? (non posée)
13) Dans quel délai ? (non posée)

Partie 2 : Les locaux et l'accès au bureau de consultation

14) Y a-t-il une alarme ?
   Oui / Non

15) Y a-t-il une caméra ?
   Oui / Non Si non -> passer à la question 20
16) Les patients sont-ils informés de la présence de ces caméras ?
   Oui / Non
17) À quoi sert la caméra ?
   Voir s'il y a des patients
   Sécurité
18) Est-ce que la caméra enregistre ?
   Oui / Non Si non -> passer à la question 20
19) Combien de temps conservez-vous les vidéos ? (non posée)

20) Quel est le type de clé de la porte d'entrée du cabinet ?

Clé sécurisée
Clé non sécurisée
Autre : **Digicode**

21) La clé du bureau de consultation est-elle la même que celle de l'entrée ?

Pas de clé pour le bureau de consultation
Oui
Non

22) Si la clé est différente, quel est le type de clé du bureau de consultation ?

Clé non sécurisée
Clé sécurisée
Autre

23) Qui possède le double des clés du bureau de consultation ?

Agent d'entretien
Secrétaire
Autre :
Interne stagiaire
Remplaçant régulier

24) Fermez-vous systématiquement le bureau à clé à chaque fois que vous le quittez ?

Oui / Non

25) Y a-t-il un ordinateur au bureau de consultation ?

Oui / Non

Partie 3 : La sécurité des données

On demande au médecin de se connecter au poste de travail (ou de le redémarrer si déjà allumé)

26) Quel est le système d'exploitation ?

Windows 10
Windows obsolète
MacOSX
MacOSX obsolète
Autre

27) Est-ce que le système d'exploitation est à jour ?

Oui / Non

28) Si non, pourquoi, le système d'exploitation n'est pas à jour ?

Matériel trop ancien, ne supporte pas la mise à jour
Autre :
Crainte de perte de données
Ne voit pas l'intérêt, cela fonctionne bien

29) Quel est le mode de connexion à la session ?

Pas de mot de passe
Mot de passe faible
Mot de passe fort
Autre

30) Pour quelles raisons n'y a-t-il pas de mot de passe de session ?

Par peur de l'oubli
Plus pratique pour le médecin
Autre : Plus pratique pour les remplaçants

31) Y a-t-il un verrouillage automatique de session **(lors d'une période d'inactivité prolongée, l'ordinateur se verrouille-t-il automatiquement)** ?

Oui / Non

32) Si non, pourquoi le verrouillage automatique de session n'est pas activé ?
Gêne l'activité de soins
Ne voit pas l'intérêt
Autre : Ne sait pas ce que c'est

33) *Y a-t-il des logiciels de protection (antivirus, pare-feu...) ?*
Oui / Non
34) S'il n'y a pas d'antivirus, pour quelles raisons ?
Pas de risque sous MacOSX
35) S'il y a des logiciels de protection, sont-ils à jour ?
Oui / Non
36) Y a-t-il un accès WiFi ?
Oui / (Non
37) S'il y a un accès WiFi, quel est le type de sécurité ?
WEP
WPA
WPA-2
38) Le logiciel de gestion de cabinet est-il en ligne ?
Oui / Non
39) Quel est le mode de connexion au logiciel de gestion de cabinet ?
Aucun mot de passe
Mot de passe pré-enregistré
Mot de passe faible
Mot de passe fort
Carte CPS
Autre : **Double authentification par SMS**
40) Pour quelles raison n'y a-t-il pas de mot de passe ou est-il pré-enregistré ?
Plus pratique pour le médecin
Par peur de l'oubli
Autre : **Plus pratique pour les remplaçants**
41) Avez-vous écrit les mots de passe sur un support papier ?
Oui / Non Si non -> passer à la question 43
42) Pour quelles raisons avez-vous écrit les mots de passe sur un support ?
Pour m'aider à m'en rappeler
Autre : **Pour aider les remplaçant**

43) Renouvelez-vous vos mots de passe ?
Oui / Non Si non -> passer à la question 45
44) À quelle fréquence renouvelez-vous vos mots de passe ? (non posée)
45) Faites-vous des sauvegardes des données-patients ? Si non -> passer à la question
Oui / Non
46) Sur quel support faites-vous les sauvegardes des données-patients ?
Disque dur externe -> passer à la question 48
Disque dur de l'ordinateur -> passer à la question 50
En ligne, car logiciel de gestion en ligne -> passer à la question 50
En ligne, mais logiciel de gestion hors-ligne
Autre
47) Si la sauvegarde est en ligne, l'organisme est-il certifié hébergeur de données de santé ? (non posée)
48) Où stockez-vous le disque dur externe contenant les sauvegardes ?
Au cabinet
Au domicile
Autre :

49) Le disque dur est-il crypté ?
Oui / Non
50) À quelle fréquence réalisez-vous ces sauvegardes ?
Hebdomadaire
Mensuel
Autre
51) Comment stockez-vous les courriers et résultats de biologie des patients ?
Numérisation intégrale -> passer à la question 53
Archives papier uniquement
Mixte
Pas de stockage numérique ni papier -> passer à la question 53
52) Où sont stockés les documents papier ?
Armoire fermée à clé
Armoire non fermée à clé
Autre : **Pièce dédié du cabinet fermée à clé**

53) Avez-vous recours à des médecins remplaçants ?
Oui / Non Si non -> passer à la question 57
54) Utilisent-ils votre carte CPS ?
Oui / Non
55) S'ils utilisent votre carte CPS, pour quelles raisons ?
Problèmes avec le logiciel de gestion de cabinet
Autres :
Flou sur la compatbilité et le paiement par la CPAM
Fonctionnalités limitées pour les remplaçants sur AmeliPro
56) Comment communiquez-vous les mots de passe au remplaçant ?
En entretien
Par téléphone
Autre : **Sur un document papier déjà préparé**

57) Avec les professionnels de santé en ville **(autres médecins, IDE, pharmacies)**, par quels moyens échangez-vous à propos des patients ?
Fax
Messagerie non sécurisée
Messagerie sécurisé si possible
Courrier
Conversation téléphonique orale
58) Avec les professionnels de santé hospitalier, par quels moyens échangez-vous à propos des patients ?
Fax
Messagerie non sécurisée
Messagerie sécurisé
Courrier
Conversation téléphonique orale
59) Avec des non-professionnels de santé, par quels moyens échangez-vous à propos des patients ?
Messagerie personnelle
Messagerie sécurisé
Courrier remis au patient
Conversation téléphonique orale

AUTEUR : Nom : ZERHOUI **Prénom : Lotfallah**

Date de soutenance : 02/07/2020

Titre de la thèse : La sécurité des sytèmes d'information en médecine genérale

Thèse - Médecine - Lille 2020

Cadre de classement : ***Médecine générale***

DES + spécialité : ***Médecine générale***

Mots-clés : Sécurité informatique médecine générale

Résumé :
Contexte : Les outils informatiques prennent une place de plus en plus importante dans la pratique de la médecine générale, le thème de la sécurité a été peu étudié. Le RGPD entré en vigueur en 2018 impose des obligations d'information des patients, de sécurisation des données et de communication sécurisée avec les tiers.

Méthode :
Entretien directif auprès de 50 médecins généralistes du Nord-Pas-de-Calais.

Résultats :
L'accès au poste de travail et aux données papier est bien encadré.
La gestion des mots de passe est problématique, l'intervention des remplaçants est le principal obstacle.
Il y a des praticiens qui disposent d'un matériel non à jour voire obsolète.
L'utilisation de messagerie sécurisée n'est pas systématique, mais tous les médecins disposent d'un moyen de communication sécurisé

Conclusion :
La mise en conformité au RGPD est possible et demande surtout des efforts au niveau de la gestion des mots de passe et d'utiliser systématiquement des messageries sécurisées.

<u>Composition du Jury</u> :

Président : Pr Antoine DRIZENKO

Assesseurs : Pr Denis DELEPLANQUE, Dr Nordine BENKELTOUM

Directeur de thèse : Dr Nassir MESSAADI