# UNIVERSITÉ DE LILLE

UFR3S-MÉDECINE

Année :2025

## THÈSE POUR LE DIPLÔME D'ÉTAT DE DOCTEUR EN MÉDECINE

**Cybersécurité : connaissances et pratiques des médecins généralistes de la Côte d'Opale**

Présentée et soutenue publiquement le 28 novembre 2025 à 16h
au *Pôle Formation*

**par Romain COURTOIS**

_____

**JURY**

**Président :**
**Monsieur le Professeur Emmanuel CHAZARD**
**Assesseur :**
**Monsieur le Docteur Maurice PONCHANT**
**Directeur de thèse :**
**Monsieur le Docteur Adrien DAUZAT**

# AVERTISSEMENT

**L’université n’entend donner aucune approbation aux opinions émises dans les thèses : celles-ci sont propres à leurs auteurs.**

**TABLE DES MATIERES**

**LISTE DES ABBREVIATIONS ..... 7**
**GLOSSAIRE ET DEFINITIONS ..... 8**
**INTRODUCTION ..... 9**
**METHODOLOGIE ..... 11**
1)Population étudiée, recrutement et déroulement de l'étude ..... 11
2) Le questionnaire ..... 12
a) Élaboration et contenu du questionnaire ..... 12
b) Diffusion du questionnaire ..... 14
c) Aspect éthique et réglementaire ..... 15
d) Analyse des données ..... 15
**RESULTATS ..... 16**
1) Autoévaluation et degré de confiance du système informatique ..... 16
1a) Sources des connaissances ..... 17
1b) Formation personnelle récente en cybersécurité ..... 17
1c) Auto-évaluation du degré de confiance au poste de travail et smartphone ..... 18
2) Sécurité du système informatique ..... 19
2a) Personne en charge de la sécurité des systèmes informatiques du cabinet: ..... 19
2b) Antivirus et/ou pare-feu : ..... 20
2c) Changement régulier des mots de passe (mails, logiciels médicaux) et session d'ordinateur ..... 20
2d) Chiffrement des données et Authentification à deux facteurs ..... 22
3) Connaissance des principales cybermenaces ..... 23
4) Habitudes pratiques en cybersécurité ..... 24
4a) Gestion des sauvegardes ..... 24
4b) Mise à jour des logiciels et système d'exploitation ..... 25
4c) Fermeture de session d'ordinateur en quittant le cabinet ..... 25
4d) Moyens de communication avec patients/professionnels de santé et précautions lors du téléchargement de pièces jointes ..... 26
4e) Type de connexion au cabinet et en visite à domicile ..... 28
4f) Partage d'identifiants et moyen(s) de transmissions ..... 29
4g) Téléconsultation et matériel utilisé ..... 30
4h) Moyens de partage de documents aux patients ..... 31
5) Profil des répondants ..... 32
5a) Age, mode et lieu d'exercice ..... 32
6) Ethique et cadre légal autour de la cybersécurité ..... 33

6a) Cyberattaque subie et réaction en cas d'attaque ..... 33
6b) Connaissance/conscience du RGPD des obligations légales et juridiques ..... 33
6c) Conséquences d'une fuite de données ..... 34
7) Impact du questionnaire ..... 35
**DISCUSSION ..... 36**
Pratiques en cybersécurité : des habitudes à risque et des vulnérabilités critiques ..... 39
Perception des risques et besoins : un potentiel de sensibilisation ..... 41
Limites de l'étude et perspectives ..... 42
Charge de Travail Accablante et Contraintes de Temps ..... 43
Cyberattaque, cadre légal et conséquences ..... 43
Amélioration/optimisation de la gestion de la cybersécurité au cabinet ..... 45
Perspectives de Recherche et Actions à Long Terme ..... 46
**CONCLUSION ..... 48**
**BIBLIOGRAPHIE ..... 50**

**Liste des figures**

Figure 1 : Cartographie des Hauts-de-France (en violet, délimitation de la Côte d'Opale) ..... 12
Figure 2 : Autoévaluation des connaissances en cybersécurité ..... 16
Figure 3 : Indice de confiance ordinateur et smartphone ..... 18
Figure 4 : Degré de confiance ordinateur vs smartphone ..... 19
Figure 5 : gouvernance de la sécurité informatique ..... 20
Figure 6 : Utilisation d'un antivirus et pare-feu ..... 20
Figure 7 : Gestion des mots de passes (session/boîte mail) ..... 21
Figure 8 : Utilisation de la 2FA ..... 22
Figure 9 : principales attaques informatiques ..... 23
Figures 10 : Fréquence des sauvegardes et supports de sauvegarde utilisés ..... 24
Figure 11 : Stockage sur support physique et chiffrement des sauvegardes ..... 25
Figure 12 : Moyens de communication utilisés ..... 27
Figure 13 : précautions lors du téléchargement de pièces jointes ..... 27
Figure 14 : Type de Connexion en visite ..... 29
Figure 15 : transmission des identifiants ..... 30
Figure 16 : Transmission des documents aux patients ..... 31
Figure 17 : Age des répondants et mode d'exercice ..... 32
Figure 18 : connaissance du RGPD ..... 34

Figure 19 : Conscience des conséquences d’une fuite de données ..... 34
Figure 20 : Impact du questionnaire..... 35
**Annexes ..... 55**
Annexe 1 : Questionnaire, version complète..... 55
Annexe 2 : Courrier de demande d'enquête..... 58
Annexe 3 : Attestation de conformité avec la CNIL ..... 59
Annexe 4 : Fiche réflexe sur les rançongiciels..... 60
Annexe 5 : Mémo/conseils gestion des mots de passe ..... 61
Annexe 6 : Conseils/sauvegardes ..... 63
Annexe 7 : Comment réagir en cas de cyberattaque ?..... 64
**RESUME..... 66**

**LISTE DES ABBREVIATIONS**

**ANS** : Agence du Numérique en Santé

**ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information

**CNIL** : Commission Nationale de l'Informatique et des Libertés

**CNOM** : Conseil National de l'Ordre des Médecins

**CPAM** : Caisse Primaire d'Assurance Maladie

**CPTS** : Communauté Professionnelle Territoriale de Santé

**CPS** : Carte de Professionnel de Santé

**DPC** : Développement Professionnel Continu

**DPO** : Délégué à la Protection des Données

**MMS** : *Multimedia Messaging Service*

**QCM** : Question à Choix Multiples

**QR code** : *Quick Response code*

**RGPD** : Règlement Général sur la Protection des Données

**SMS** : *Short Message Service*

**SSID** : *Service Set IDentifier*

**URL** : *Uniform Resource Locator*

**USB** : *Universal Serial Bus*

**WEP** : *Wired Equivalent Privacy*

**WiFi** : *Wireless Fidelity*

**WPA** : *Wi-Fi Protected Access*

**2FA** : *Two-factor authentication*

## GLOSSAIRE ET DEFINITIONS

**Antivirus** : « Logiciel utilitaire qui détecte et détruit les virus informatiques s'attaquant à la mémoire d'un ordinateur » [1].

**Chiffrement** : « Opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission » [2].

**Cloud** : « Le *cloud computing* (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés » [3].

**Cybercriminalité/Cybermalveillance : «** Ensemble des activités illégales effectuées par l'intermédiaire d'Internet. » [4]

**Hacker** : « Personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique. » [5]

**Logiciel espion** : « Logiciel destiné à collecter et à transmettre à des tiers, à l'insu de l'utilisateur, des données le concernant ou des informations relatives au système qu'il utilise » [6].

**Mise à jour** : « En informatique, une mise à niveau, ou mise à jour — parfois abrégée en MAJ ou MàJ, parfois appelée révision, ou *upgrade* en anglais, est l'action qui consiste à déployer vers des équipements électroniques des utilisateurs les changements effectués (ou à effectuer) à un outil informatique, un service ou une prestation en téléchargeant, ou en chargeant, un nouveau logiciel, micrologiciel ou encore le contenu de quelconques données » [7].

**Pare-feu** (*firewall*) : « Un pare-feu est un système de sécurité de réseau informatique qui limite le trafic Internet entrant, sortant ou à l'intérieur d'un réseau privé.

Il est généralement destiné à aider à prévenir les activités malveillantes et à empêcher quiconque, à l'intérieur comme à l'extérieur d'un réseau privé, de se livrer à des activités Web non autorisées » [8].

**WEP** : « Le *Wired Equivalent Privacy* (abrégé WEP) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi » [9]

**Wi-Fi** : connexion Internet sans fil.

**WPA 2** : Norme Wi-Fi : évolution du protocole WEP, plus difficile à pirater.

# INTRODUCTION

A l'ère du numérique et de l'intelligence artificielle, l'utilisation de l'informatique fait partie intégrante de la vie quotidienne et connaît dans le domaine médical un formidable essor. La transformation de l'ordinateur vers de nouveaux objets (console de jeux, téléphones, montres connectées, robots autonomes...) a fait de l'informatique un outil essentiel et indispensable. Aujourd'hui, les ordinateurs sont dans notre poche, autour du poignet et partout autour de nous. Avec ces outils, Internet est donc autant présent que l'air que nous respirons. La croissance de la puissance informatique au fil des décennies en fait à la fois un brillant outil mais également parfois un redoutable adversaire. En effet, la cybercriminalité suit naturellement cette dynamique et progresse continuellement, et les établissements de santé en sont d'ailleurs fréquemment la cible.

Dans le tourbillon de l'évolution informatique, le système de santé n'est donc pas épargné. Tout au long du parcours de soins, les données numériques de santé sont partout : au cabinet, à l'hôpital ou à la maison. Une omniprésence qui s'est accrue avec la crise sanitaire de 2020. La cybersécurité, en général, et dans le domaine de la santé est alors aujourd'hui une priorité pour les grandes instances de notre pays [10]. Pivot du système de santé, le médecin généraliste n'échappe pas non plus aux actes de cybermalveillance qui sont de plus en plus fréquents. En effet, les cabinets médicaux constituent un réservoir d'informations personnelles, médicales et confidentielles sur leurs patients. Ces données telles que leurs noms, adresses, numéro de sécurité sociale et numéro de retraite constituent des données très sensibles. Elles peuvent être lucratives pour les cybercriminels qui misent sur cet impact potentiellement élevé pour exercer une pression sur les victimes et obtenir des rançons. Très récemment, le 22 novembre 2024, un cybercriminel a publié en ligne une base de données contenant les informations personnelles et médicales de 758 912 personnes. Les données exposées incluent les coordonnées personnelles (nom, adresse, téléphone, etc.), des détails médicaux (ordonnances, médecins traitants, déclarations de décès) et des identifiants externes) [11].

Une cyberattaque peut en effet non seulement perturber le quotidien des professionnels de santé, mais aussi mettre en péril la prise en charge et la qualité des soins pour les patients.

Les médecins généralistes utilisent de plus en plus d'outils numériques pour la gestion des dossiers patients. Par exemple, la télétransmission des feuilles de soins, l'envoi de mail et d'ordonnance au patient (par exemple avec Doctolib® et dans un second temps le transfert de celle-ci à la pharmacie) ou encore la messagerie classique ou instantanée.

La prise de rendez-vous en ligne est également omniprésente. Ces plates-formes centralisent des données personnelles et médicales, ce qui soulève des questions de sécurité et de confidentialité.

Depuis 2018, les actes de téléconsultation sont ouverts à tous les patients (par l'intermédiaire d'une plateforme sécurisée). Le nombre de téléconsultations a augmenté considérablement durant la pandémie avec un total de 14 millions d'actes réalisés en 2024 en France [12]. Celle-ci offre une plus grande souplesse pour les patients et les médecins, mais nécessite l'utilisation de plateformes et d'outils de communication numériques. L'utilisation croissante de technologies numériques augmente automatiquement leur exposition aux cybermenaces. Certains cabinets de médecine générale disposent de systèmes informatiques peu sophistiqués (anti-virus obsolète, pare-feu inefficace...). Ils sont par conséquent moins bien protégés que ceux des grandes structures hospitalières et donc potentiellement plus vulnérables [13] [14].

Face à ces risques, il est crucial que les médecins généralistes prennent des mesures pour renforcer la sécurité de leurs systèmes informatiques et se forment régulièrement aux bonnes pratiques en matière de cybersécurité.

La cybersécurité est l'ensemble des pratiques et des technologies visant à protéger les systèmes, les réseaux et les données numériques des attaques malveillantes. En d'autres termes, c'est le bouclier qui protège notre monde numérique [15]. C'est un domaine en constante évolution, qui s'adapte aux nouvelles menaces et aux avancées technologiques.

Dans ce contexte d'effervescence du système de santé français et de cette utilisation accrue de l'informatique en médecine, nous avons voulu réaliser un état des lieux quant aux pratiques et connaissances des médecins généralistes en matière de cybersécurité.

# METHODOLOGIE

## 1) Population étudiée, recrutement et déroulement de l'étude

En complément des travaux menés en Picardie (O.Castellano 2023) [16] et dans le Nord (L.Zerhoui 2020) [17], notre étude centrée sur la Côte d'Opale actualise et approfondit l'analyse des pratiques de cybersécurité des médecins généralistes. Pour cela, elle a traité les aspects techniques (sécurisation des systèmes informatiques, gestion des mots de passe, sauvegardes, authentification), organisationnels (recours à un prestataire, formation des équipes, protocoles internes) et réglementaires (conformité au RGPD, responsabilités légales, obligations déontologiques). Pour y parvenir, cette étude, quantitative, descriptive et transversale a été conduite à l'aide d'un questionnaire envoyé aux médecins généralistes de la Côte d'Opale.

L'ensemble des médecins généralistes libéraux de la Côte d'Opale (Dunkerque, Calais, Boulogne et alentours) a été contacté pour la réalisation de cette thèse. Cet échantillon représente un total de 316 médecins généralistes en exercice, responsables de leur propre système informatique. La liste nominative des médecins a été obtenue par l'intermédiaire de l'agence du numérique en santé (référence CAS-1479641-N9P2T1) avec leur accord sur l'utilisation des données après les avoir informé et contacté par mail[1].

La recherche a été complétée par l'utilisation de l'annuaire en ligne mis à disposition par l'agence du numérique en santé[2] en effectuant une recherche détaillée et l'application de filtres (par lieu d'exercice, spécialité de médecine générale, en activité). Nous avons également utilisé l'annuaire AMELI des professionnels de santé[3] ainsi que l'annuaire incorporé dans la messagerie sécurisée MSSANTE (mailiz).

[1] monserviceclient.annuaire@esante.gouv.fr
[2] https://annuaire.sante.fr/web/site-pro
[3] https://annuairesante.ameli.fr/




**Figure 1 : Cartographie des Hauts-de-France (en violet, délimitation de la Côte d'Opale)**

## 2) Le questionnaire

### a) Élaboration et contenu du questionnaire

Le questionnaire (anonyme) se compose de 41 questions réparties de la manière suivante *:*

*- 6 questions portant sur l'autoévaluation et le degré de confiance du système informatique,*

*- 8 questions sur la sécurité du système informatique,*

*- 17 questions sur les habitudes pratiques en cybersécurité,*

*- 3 questions portent sur le profil et les données démographiques des répondants : tranche d'âge, lieu et mode d'exercice,*

*- 7 questions sur l'éthique et le cadre légal autour de la cybersécurité.*

Certaines sont des questions binaires (réponse oui/non) et constituent un branchement conditionnel qui a permis de choisir la prochaine question à afficher en fonction de la réponse donnée à la question en cours.

Le questionnaire **(Encart 1 en version simplifiée, Annexe 1 version complète)** a été relu par un ingénieur en cybersécurité ainsi qu'un spécialiste de métier en informatique. Il a également été présenté à des internes et remplaçants en médecine générale pour le rendre le plus pertinent possible.

*Encart 1 : Questionnaire simplifié*

Vos connaissances en cybersécurité

**1. Comment estimez-vous vos connaissances en cybersécurité?** Médiocres / Moyennes / Bonnes / Excellentes

**2. D'où tenez-vous vos connaissances?** Expérience pro antérieure ; Formation DPC ; Intérêt personnel ; Conseils ; Autre

**3. Formé par vos propres moyens ces 2 dernières années?** Oui / Non

**4. Besoin de suivre/poursuivre une formation?** Oui / Non

**5. Note de confiance poste de travail (0-10):** 0-10

**6. Note de confiance smartphone (0-10):** 0-10 / Je n'en ai pas

La sécurité de votre/vos systèmes informatiques

**7. Personne en charge de la sécurité SI?** Interne ; Externe ; Interne+Externe ; Moi

**8. Antivirus/pare-feu?** Oui / Non / Je ne sais pas

**9. Changement régulier des mots de passe mails/logiciels?** ≥1/an ; <1/an ; Non ; NSP

**10. Changement mot de passe session?** Oui ; Non ; NSP

**11. Savez-vous ce qu'est le chiffrement?** Oui / Non / NSP

**12. Utilisez-vous la 2FA?** Oui souvent / Non / Je ne sais pas

**13. 2FA configurée via:** SMS ; App ; Mail ; NSP

**14. Connaissez-vous ces attaques?** Phishing ; Ransomware ; Cheval de Troie ; MitM ; DDoS ; Fraude au président

Vos habitudes pratiques de cybersécurité

**15. Fréquence sauvegardes:** Hebdo ; Mensuelle ; 6 mois ; Jamais

**16. Supports sauvegarde:** PC ; Disque/clé ; Cloud

**17. Lieu stockage sauvegarde:** Cabinet ; Domicile ; Autre

**18. Données sauvegardées chiffrées?** Oui / Non / NSP

**19. Mise à jour régulière logiciels/systèmes?** Oui / Non

**20. Fermeture session cabinet?** Oui ; Non ; Fermeture auto ; NSP

**21. Moyens de communication utilisés:** Téléphone pro ; Fixe ; Smartphone ; Mail perso/pro ; WhatsApp ; SMS ; Messageries sécurisées

**22. Envoi e-mails depuis mobile?** Oui / Non / Parfois

**23. Précautions pièces jointes?** Toujours ; Souvent ; Rarement ; Jamais

**24. Connexion Internet cabinet:** Ethernet ; WiFi ; Bluetooth ; Clé 3G/4G/5G ; Partage mobile

**25. Caractéristiques WiFi:** Public ; Sécurisé ; SSID visible/caché ; NSP

**26. Connexion en visite domicile:** WiFi dispo ; Réseau mobile ; Clé 3G/4G/5G ; Partage ; WiFi patient

**27. Partagez-vous identifiants?** Oui / Non

**28. Mode transmission identifiants:** Post-it ; SMS/WhatsApp ; Oral ; Autre

**29. Travail à domicile avec PC?** Oui perso ; Oui pro ; Non

**30. Utilisation PC pro à domicile à titre perso?** Oui / Non

**31. Transmission documents aux patients:** Mail perso ; SMS ; Clé USB ; Plateforme sécurisée ; Autre

Critères démographiques

**32. Tranche d'âge:** 25–35 ; 36–45 ; 46–55 ; 56–65 ; 66+

**33. Exercez-vous dans le secteur B/C/D (<20km)?** Oui / Non

**34. Mode d'exercice:** Seul ; Groupe ; MSP ; Salarié

Éthique et cadre légal

**35. Avez-vous subi une cyberattaque?** Oui / Non

**36. Sauriez-vous réagir immédiatement?** Oui / Non

**37. Connaissez-vous le RGPD?** Oui / Non / Un peu

**38. Obligations légales connues?** Oui / Partiellement / Non

**39. Connaissez-vous conséquences juridiques fuite données?** Oui / Non

**40. Responsabilité engagée en cas d'attaque?** Oui / Non

**41. Ce questionnaire vous incite-t-il à changer vos habitudes?** Oui / Non

**b) Diffusion du questionnaire**

Le support de diffusion utilisé est la plateforme *LimeSurvey*, outil d'enquête, de création de questionnaire anonyme en ligne nécessitant d'effectuer au préalable une demande à la faculté de Lille.

En raison de l'anonymisation, il est impossible d'estimer le taux de réponse : le nombre de médecins ayant reçu le questionnaire ou ouvert le courriel d'invitation n'est pas connu. Par ailleurs, afin de s'assurer que les répondants appartenaient bien à la population cible, une question de sélection portant sur le lieu d'exercice a été posée dans le questionnaire. Cela a permis d'exclure les réponses hors zone géographique étudiée.

Le questionnaire a été diffusé par différentes voies :

- Par mail au secrétariat des CPTS avec envoi à l'ensemble des médecins généralistes faisant partis des CPTS correspondantes (Littoral en nord, Grand Calaisis et Opale Sud) suivi d'une relance dans les groupes *Whatsapp*® de celles-ci (un lien URL et QR code) ;
- Transmission du lien URL (et QR code) du questionnaire à une liste de diffusion mise à disposition par une ressource du Boulonnais (liste groupe Google® qui inclut un grand nombre de participants)
- Transmission grâce à des listes de diffusions privées à l'aide de personnes-ressources avec effet "boule de neige" escompté,
- Par mail avec lien URL (et QR code) par l'intermédiaire de la plateforme de messagerie sécurisée MSSanté et des adresses mails personnelles de médecins volontaires après présentation du projet de thèse.

La durée de diffusion était de 2 mois, s'étalant de mai à juin 2025. Deux relances étaient planifiées, respectivement à 15 et à 45 jours.

Le mail reçu pour la présentation du sujet et l'invitation à répondre au questionnaire est présenté **(Annexe 2).**

### c) Aspect éthique et réglementaire

Afin d'être en conformité avec la CNIL, une déclaration simplifiée à la Faculté de Médecine de Lille a été faite auprès du délégué à la protection des données (DPO). Une attestation de déclaration en accord avec le RGPD a été délivrée **(Annexe 3).** Le questionnaire étant anonyme et non identifiant, cette étude a été exonérée de déclaration relative au règlement général sur la protection des données par le délégué à la protection des données (DPO) de l'Université de Lille.

### d) Analyse des données

Des réponses aux questionnaires ont été extraites de *LimeSurvey* et consignées dans un tableau Microsoft® Excel© afin de réaliser les analyses statistiques. Les réponses incomplètes aux questionnaires ont été exclues de l'analyse.

# RESULTATS

Les résultats sont présentés selon les 4 axes principaux qui subdivisent le questionnaire. Au total 316 médecins généralistes ont été inclus grâce à l'annuaire santé en ligne de la CPAM. 42 médecins généralistes ont répondu au questionnaire jusqu'à la fin. 7 médecins ont répondu de façon incomplète, leur participation n'a pas été prise en compte.
Le taux de réponse, estimé, est donc de 13,2%.

## 1) Autoévaluation et degré de confiance du système informatique

*Q1- Comment estimez-vous vos connaissances en Cybersécurité ?*
- *Médiocres / Moyennes / Bonnes / Excellentes*

Les deux-tiers des médecins répondants estiment que leurs connaissances en cybersécurité sont médiocres (66.67%, soit 28 répondants), un tiers estime avoir un niveau moyen des connaissance (28.57%, soit 12 répondants) et, enfin, seuls 2 médecins jugent leur connaissances "Bonnes" (4.76%, 2 répondants). Aucun médecin ne prétend avoir un niveau excellent en cybersécurité.

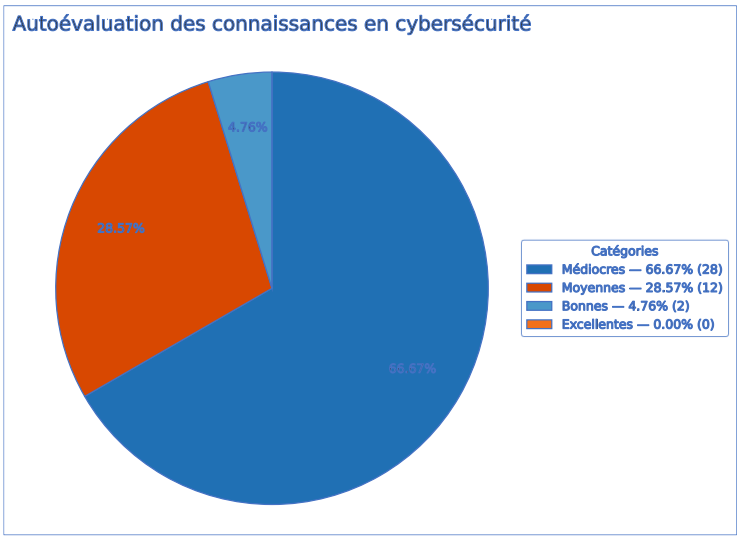



**Figure 2 : Autoévaluation des connaissances en cybersécurité**

### 1a) Sources des connaissances

**Q2- D'où tenez-vous vos connaissances en Cybersécurité ?*

- *Expérience professionnelle antérieure*
- *D'une formation dans le cadre du développement professionnel continu*
- *D'un intérêt personnel pour la cybersécurité*
- *De conseils émanant d'un professionnel en cybersécurité*
- *Autre*

Cette question s'adresse aux participants qui jugent au minimum « moyennes » leurs connaissances en cybersécurité

Parmi ces 16 médecins, 4 personnes ont affirmé tenir leurs connaissances d'une expérience professionnelle antérieure, 4 d'un intérêt personnel pour la cybersécurité et 4 de conseils émanant d'un professionnel en cybersécurité. Une formation dans le cadre du DPC n'est citée que par un médecin.

### 1b) Formation personnelle récente en cybersécurité

**Q3- Vous êtes-vous formé par vos propres moyens en cybersécurité au cours des 2 dernières années ?*

- *Oui / Non*

**Q4- Eprouvez-vous le besoin de suivre ou poursuivre une formation en cybersécurité ?*

- *Oui / Non*

En ce qui concerne la formation en cybersécurité, l'immense majorité des médecins interrogés 83.33% (35 répondants) ne s'est pas formée par ses propres moyens en cybersécurité au cours des deux dernières années.

Pour 19 répondants (45,26 % des personnes interrogées) il existe un besoin de suivre une formation

## 1c) Auto-évaluation du degré de confiance au poste de travail et smartphone

**Q5- Attribuez une note de confiance de 0 à 10 à votre système informatique au cabinet (poste de travail)*

*- 0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10*

**Q6- Si vous possédez un smartphone (téléphone connecté à internet), attribuez-lui une note de confiance de 0 à 10*

*- 0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10 / Je n'en n'ai pas*

A propos de la note de confiance attribuée au poste de travail, les médecins ont plutôt confiance avec une grande majorité qui l'estime globalement moyenne ou haute.

Si l'on regroupe les notes :

- Faible confiance (0 à 4) : Seulement 6 répondants (14,4%) attribuent une note de 4 ou moins.
- Confiance moyenne (5-6) : 18 répondants (42,9%) donnent une note de 5 ou 6.
- Forte confiance (7-10) : 18 répondants (42,9%) affectent une note de 7 ou plus.

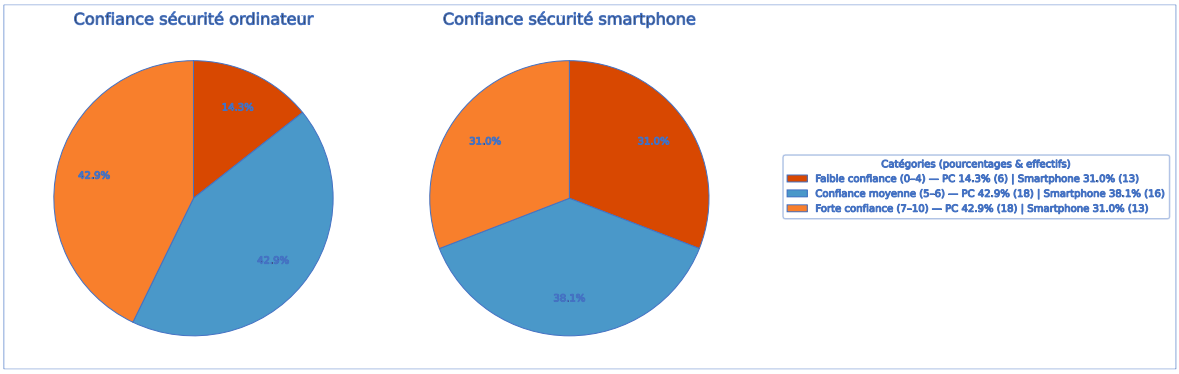



**Figure 3 : Indice de confiance ordinateur et smartphone**

La note de confiance en leur smartphone la plus donnée par les médecins est de 5 avec 13 réponses (31,0%). Cela indique que la plupart d'entre eux ont une confiance modérée en leurs téléphones mobiles.

Un nombre non négligeable de participants (13 personnes, soit 31%) attribuent une note de 4 ou moins, signalant un manque de confiance important dans leur appareil. Inversement à leur

poste de travail, les médecins ont moins confiance en leur smartphone.

Si on regroupe les réponses :

- Faible confiance (0-4) : 13 répondants (31,0 %)
- Confiance moyenne (5-6) : 16 répondants (38,1 %)
- Forte confiance (7-10) : 13 répondants (31,0 %)

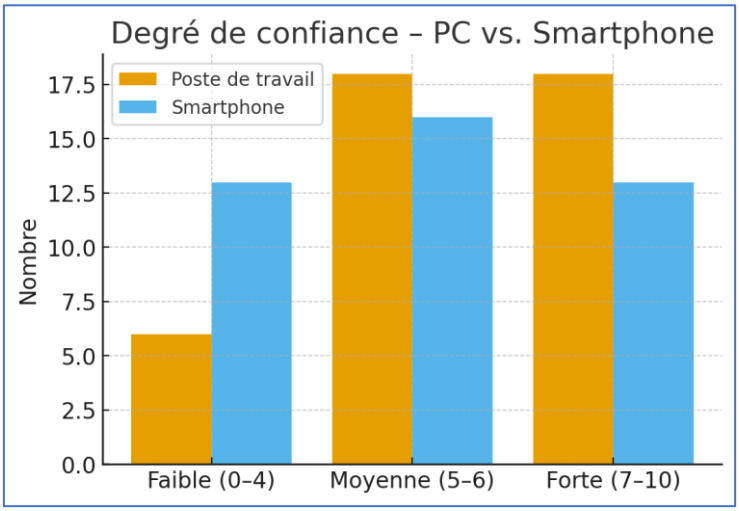



**Figure 4 : Degré de confiance ordinateur vs smartphone**

## 2) Sécurité du système informatique

### 2a) Personne en charge de la sécurité des systèmes informatiques du cabinet :

**Q7-Avez-vous désigné une personne en charge de la sécurité des systèmes d'information de votre cabinet ?*

- *Oui, en interne, par une personne ou une organisation spécifique intervenant physiquement au cabinet*
- *Oui en externe par une personne tierce professionnalisée, audit ou contrat d'assistance informatique*
- *Oui en externe et interne*
- *Non je gère moi-même*

La majorité des médecins : 42.86% (18 répondants) gèrent eux-mêmes la sécurité de leur cabinet

33.33% (14 répondants) ont recours à un professionnel tiers externe sous forme d'audit ou de

contrat d'assistance informatique.

14.29% (6 répondants) font appel à une personne ou une organisation spécifique qui intervient au cabinet.

9.52% (4 répondants) combinent solutions interne et externe.

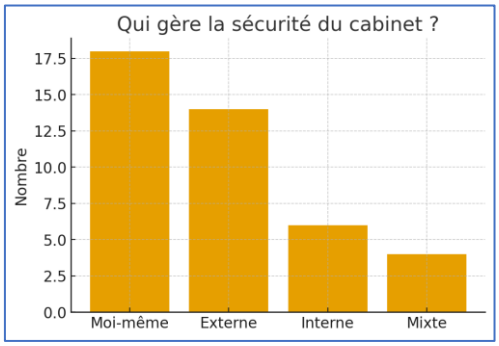



**Figure 5 : gouvernance de la sécurité informatique**

**2b) Antivirus et/ou pare-feu :**

**Q8-Votre système informatique dispose-t-il d'un antivirus et/ou pare-feu ?*

*- Oui / Non / Je ne sais pas*

Sur les 42 médecins interrogés, 33 (soit 78,57 %) d'entre eux utilisent un antivirus et/ou un pare-feu. Six répondants (14,29 %) ne savent pas s'ils en avaient un. Trois médecins confirment ne pas en avoir.

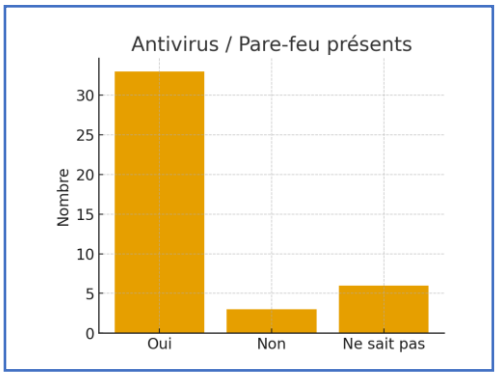



**Figure 6 : Utilisation d'un antivirus et pare-feu**

**2c) Changement régulier des mots de passe (mails, logiciels médicaux) et session d'ordinateur**

**Q9-Changez-vous régulièrement vos mots de passe de boîte(s) mail(s), logiciels médicaux ?*

*- Oui au moins une fois par an / Oui moins d'une fois par an / Non / Préfère ne pas le dire*

*Q10-Changez-vous régulièrement votre mot de passe de session d'ordinateur ?*

*- Oui / Non / Je n'en ai pas (touche entrée pour accéder au bureau au démarrage) / Préfère ne pas le dire*

La majorité des participants (73,81 %, soit 31 personnes) ne changent pas régulièrement les mots de passe de leurs boîtes mail et logiciels médicaux. Parmi eux, 14,29 % (6 personnes) les mettent à jour moins d'une fois par an, et seulement 4,76 % le font au moins une fois par an. Concernant les sessions d'ordinateur, 83,33 % des participants (35 répondants) ne changent pas régulièrement leur mot de passe. Trois répondants (7,14 %) n'en ont même pas, se connectant avec la touche "Entrée".

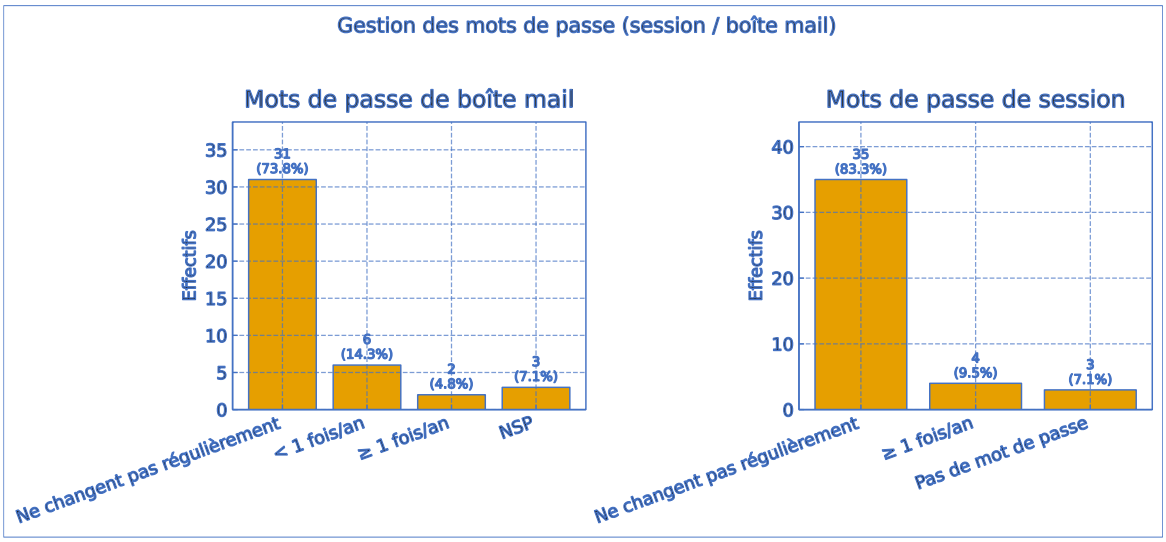



**Figure 7 : Gestion des mots de passes (session/boîte mail)**

## 2d) Chiffrement des données et Authentification à deux facteurs

**Q11-Savez-vous ce qu'est un "chiffrement des données" ?*

*Oui / Non / Je ne sais pas*

**Q12-Utilisez-vous l'authentification à deux facteurs (2FA) pour protéger vos accès aux systèmes médicaux ?*

*Oui la plupart du temps / Non / Je ne sais pas ce que c'est*

**Q13-Cette authentification à double facteur est configurée le plus souvent via :*

*SMS / Une application / Réception d'un mail / Préfère ne pas le dire*

L'authentification à deux facteurs (2FA), une mesure de sécurité essentielle, est très peu utilisée par les participants à l'étude. En effet, la moitié des répondants (50 %, soit 21 personnes) ne l'utilisent pas pour leurs systèmes médicaux.

Un tiers des participants (33,33 %, soit 14 personnes) ignore même ce qu'est la 2FA.

Seule une petite minorité, 16,67 % des répondants (7 personnes), l'utilisent la plupart du temps. Ces derniers ont majoritairement recours à la réception d'un SMS (3 répondants) ou, dans une moindre mesure, à une application ou un e-mail (2 répondants pour chaque méthode) pour configurer leur double authentification.

La majorité des participants, soit 52,38 % (22 répondants), ont une bonne compréhension de ce qu'est le chiffrement des données. Cependant, une proportion significative (42,86 %, soit 18 répondants) n'est pas familière avec ce terme technique.

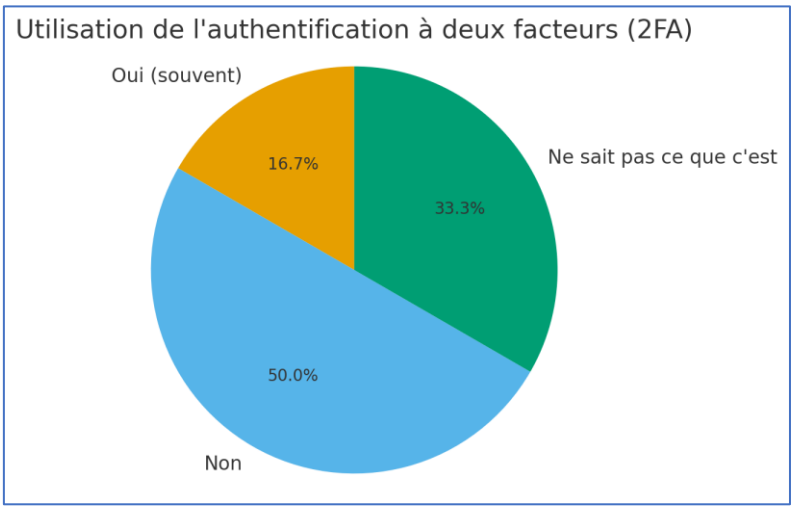



**Figure 8 : Utilisation de la 2FA**

## 3) Connaissance des principales cybermenaces

*Q14-Avez-vous connaissance de ces différentes attaques informatiques ?*

*(Si oui, cochez)*

*- L'hameçonnage ou Phishing*

*- L'attaque par rançongiciel (Ransomware)*

*- Le cheval de Troie*

*- L'attaque de l'homme du milieu (MitM)*

*- L'attaque par déni de service (DdoS)*

*- La fraude au président (= usurpation d'identité)*

Les participants sont particulièrement familiarisés avec des menaces courantes comme le Cheval de Troie (85,71 %) et l'hameçonnage (78,57 %).

Cependant, leur connaissance est moins étendue pour les cyberattaques plus sophistiquées. Un peu plus de 40 % des répondants connaissent les rançongiciels (*ransomware*) et 38,10 % la fraude au président mais, encore plus techniques, le déni de service (DDoS) et l'homme du milieu (MitM) sont presque inconnues. Seuls 7,14 % des participants ont pu identifier la première, et un seul répondant (2,38 %) a reconnu la seconde.

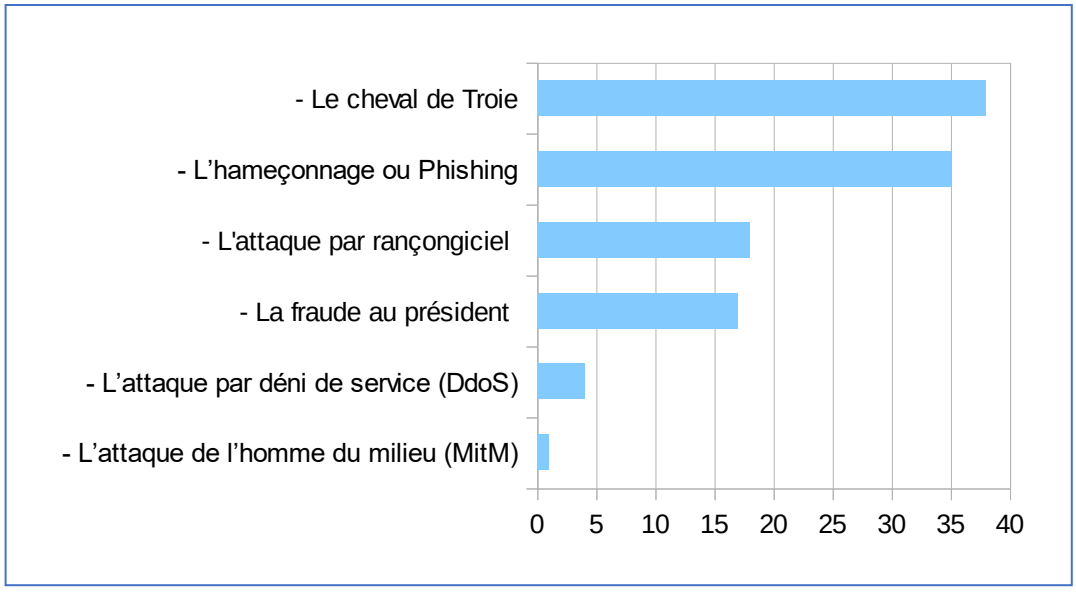



**Figure 9 : principales attaques informatiques**

## 4) Habitudes pratiques en cybersécurité

### 4a) Gestion des sauvegardes

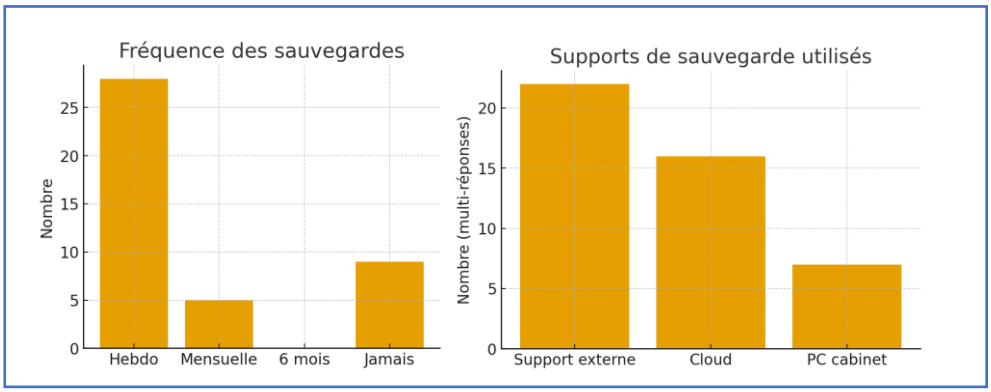
**Q15 À quelle fréquence organisez-vous vos sauvegardes ?*
*- De façon hebdomadaire ou moins*
*- De façon mensuel ou moins*
*- Tous les 6 mois au minimum*
*- Jamais*

**Q16 Sur quel(s) type(s) de support ?*
*- Ordinateur du cabinet*
*- Support de stockage physique externe (clef USB ou disque dur externe)*
*- Support de stockage en ligne (Cloud)*

**Q17 Où stockez-vous le disque dur servant de sauvegarde des données ?*
*- Au cabinet*
*- Au domicile*
*- Autre lieu*

**Q18 Les données sauvegardées sont-elles cryptées ?*
*Oui*
*Non*

Concernant la fréquence et supports des sauvegardes seuls 66,67 % des répondants (28 personnes) réalisent des sauvegardes de leurs données au moins une fois par semaine, et 21,43 % d'entre eux (9 personnes) ne les effectuent jamais.




**Figures 10 : Fréquence des sauvegardes et supports de sauvegarde utilisés**

Les supports physiques externes (52,38 %) et le cloud (38,10 %) sont les méthodes de sauvegarde les plus populaires. Toutefois, 16,67 % des participants (7 personnes) sauvegardent

leurs données directement sur l'ordinateur du cabinet, ce qui les expose à un risque en cas de panne ou de vol.

Quant au lieu de stockage et du cryptage des données, parmi ceux qui utilisent un support physique, près de 28,57 % (12 personnes) le conservent au cabinet. 16,67 % (7 personnes) le gardent à domicile et 7,14 % (3 personnes) dans un autre lieu. Un problème majeur ressort du cryptage des données : parmi les 33 participants réalisant des sauvegardes, la moitié (50 %) ne sait pas si leurs données sont cryptées. Seuls 16,67 % des répondants affirment que leurs sauvegardes sont cryptées, contre 11,90 % qui déclarent qu'elles ne le sont pas.

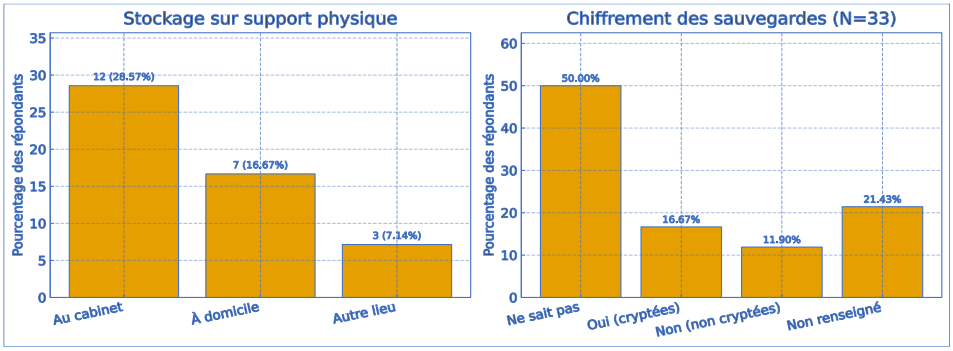



**Figure 11 : Stockage sur support physique et chiffrement des sauvegardes**

## 4b) Mise à jour des logiciels et système d'exploitation

**Q19 Mettez-vous régulièrement à jour vos logiciels et systèmes d'exploitation ?*
*Oui*
*Non*

Presque la totalité des médecins interrogés, soit 97,62 % (41 personnes), mettent régulièrement à jour leurs logiciels et systèmes.

## 4c) Fermeture de session d'ordinateur en quittant le cabinet

**Q20- Lorsque vous quittez le cabinet, fermez-vous systématiquement votre session d'ordinateur ?*
*- Oui*
*- Non, parfois j'oublie*
*- J'ai configuré une fermeture de session après une période d'inactivité*
*- Préfère ne pas le dire*

La majorité des répondants, soit 64,29 % (27 personnes), ferme systématiquement leur session après utilisation. Cependant, 26,19 % (11 personnes) l'oublient occasionnellement.
Pour 7,14 % d'entre eux (3 personnes), la fermeture est gérée automatiquement.

### 4d) Moyens de communication avec patients/professionnels de santé et précautions lors du téléchargement de pièces jointes

**Q21- Quel(s) moyen(s) de communication utilisez-vous pour contacter vos patients ou autre professionnel de santé ?*

*- Téléphone mobile professionnel exclusivement dédié à l'émission et à la réception d'appels (non connecté)*

*- Téléphone fixe au cabinet*

*-Téléphone mobile à usage mixte professionnel et personnel (type smartphone connecté)*

*- Email d'une boîte personnelle (type Google©, Orange© etc.)*

*-Email d'une messagerie professionnelle et sécurisée (ex Apicrypt©, Lifen©, Mailiz©)*

*- Messagerie privée, individuelle ou de groupe (Whatsapp©, Telegram©, Messenger© etc.)*

*- SMS, MMS*

*- Messagerie sécurisée professionnelle (Omnidoc©, Doctolib Siilo©, TeamDoc©, Pandalab pro© etc.)*

**Q22- Concernant l'envoi des mails, sont-ils envoyés depuis un appareil mobile (téléphone, tablette ...) ?*

*Oui / Non / Parfois*

**Q23- Prenez-vous des précautions supplémentaires lors du téléchargement de pièces jointes par mail (En vérifiant par exemple si le nom d'expéditeur est connu...) ?*

*Toujours / Souvent / Rarement / Jamais*

Pour les échanges professionnels, les médecins privilégient majoritairement les messageries sécurisées (69.05%, soit 29 répondants) et les e-mails professionnels sécurisés (66.67%, soit 28 répondants). Le téléphone fixe au cabinet est également un outil courant utilisé par 25 médecins interrogés, soit 59,52%

Malgré cela, les communications non sécurisées restent très utilisées :

- 47.62%, soit 20 répondants se servent d'un téléphone mobile à usage mixte.
- 35.71%, soit 15 répondants utilisent des e-mails personnels.
- 26.19%, soit 11 répondants envoient des SMS/MMS.
- 16.67%, soit 7 répondants recourent à des messageries privées.

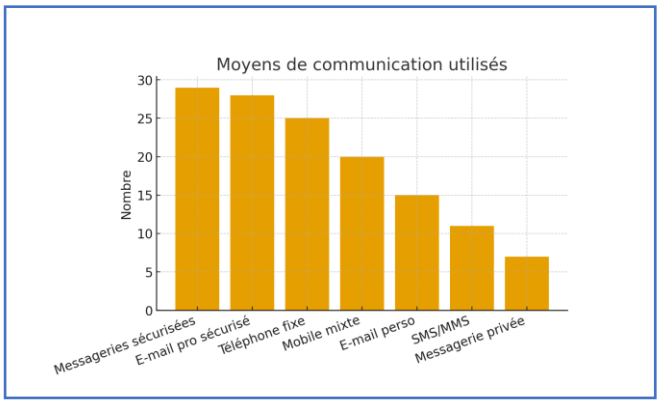



**Figure 12 : Moyens de communication utilisés**

Par ailleurs, les précautions prises lors de téléchargements de pièces jointes varient grandement. Si 47,62 % (20 répondants) des participants déclarent "toujours" prendre des précautions, 28.57% (12 répondants) en prennent "souvent", et 23.81% (10 répondants) en prennent "rarement" ou même "jamais" (4,76 % soit 2 répondants).

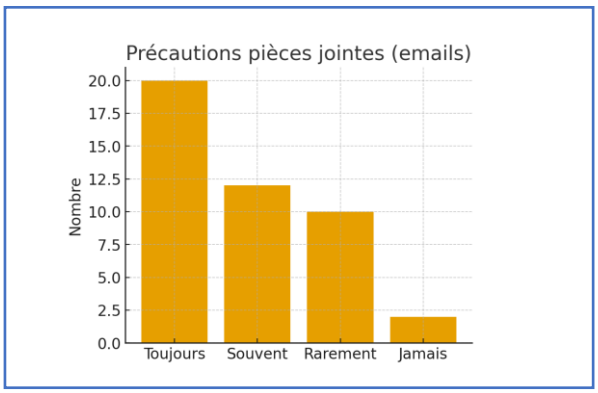



**Figure 13 : précautions lors du téléchargement de pièces jointes**

### 4e) Type de connexion au cabinet et en visite à domicile

**Q24- Quel type de connexion internet utilisez-vous au cabinet ?*

*Ethernet (par câble) / Wifi (sans fil) / Bluetooth / Clef 3G/4G/5G sécurisée / Partage de connexion avec votre mobile*

**Q25- Quelles sont les caractéristiques de votre point d'accès Wifi ?*

- *Wifi publique*
- *Wifi sécurisée avec mot de passe (WEP, WPA, WPA 2 etc.)*
- *Nom du réseau Wifi (SSID) visible*
- *Nom du réseau Wifi (SSID) invisible, caché via les options de la Box internet*
- *Préfère ne pas le dire*

**Q26- Pendant les visites à domicile, quel(s) type(s) de connexion utilisez-vous ?*

- *N'importe quel réseau wifi disponible à proximité (public par exemple)*
- *Réseau de mon opérateur mobile*
- *Clef 3G/4G/5G sécurisée*
- *Un partage de connexion*
- *Le réseau wifi sécurisé des patients*

Concernant la connectivité au cabinet, la majorité des cabinets utilise une connexion Ethernet par câble (66,67 % soit 28 répondants), mais le Wi-Fi est également très répandu (47,62 % soit 20 répondants). 7,14 % des répondants (3 personnes) utilisent le Bluetooth pour accéder à Internet. De plus, un participant se sert du partage de connexion de son téléphone mobile.

Quant à la sécurité du Wi-Fi au cabinet parmi les utilisateurs de la technologie Wi-Fi, 45,24 % (19 répondants) ont mis en place un réseau sécurisé (WPA ou WPA2, plus avancés que le WEP, moins sécurisé). Une seule personne a pris la précaution de cacher le nom de son réseau (SSID) pour le rendre invisible aux patients et aux autres utilisateurs.

Enfin, pour la connexion lors des visites à domicile, la moitié des répondants (50 % soit 21 répondants) se connecte via le réseau de leur opérateur mobile. Environ 26,19 % (11 répondants) des participants au questionnaire utilisent le partage de connexion de leur téléphone. Seulement un répondant se connecte à des réseaux Wi-Fi publics.

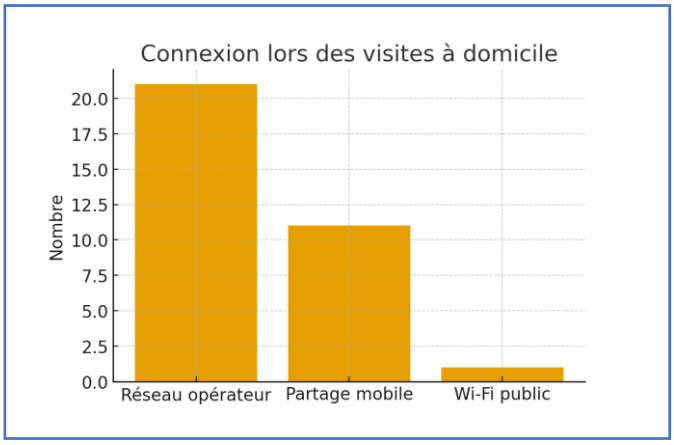



**Figure 14 : Type de Connexion en visite**

### 4f) Partage d'identifiants et moyen(s) de transmissions

**Q27- Partagez-vous vos identifiants de connexion à un ordinateur, carte CPS ou messagerie (sécurisée ou non) avec d'autres personnes (collègues, secrétaires, remplaçants ...) ?*

*Oui / Non*

**Q28- Comment ces informations sont-elles transmises ?*

*- Sur support physique (post-it, feuille de papier, etc.)*

*- Sur support dématérialisé (SMS, Whatsapp, Messenger etc.)*

*- A l'oral*

*- Autre moyen*

Le partage des identifiants de connexion (ordinateur, carte CPS, messagerie) est une pratique courante, mais risquée : 71,43 % des répondants (30 personnes) le font.
Les identifiants sont le plus souvent transmis sur un support physique comme un post-it ou une feuille (47,62 % des cas soit 20 répondants). D'autres sont partagés oralement (12 répondants soit 28,57 %), tandis qu'une minorité les envoie via des supports dématérialisés tels que SMS ou WhatsApp (4,76 % soit 2 répondants).

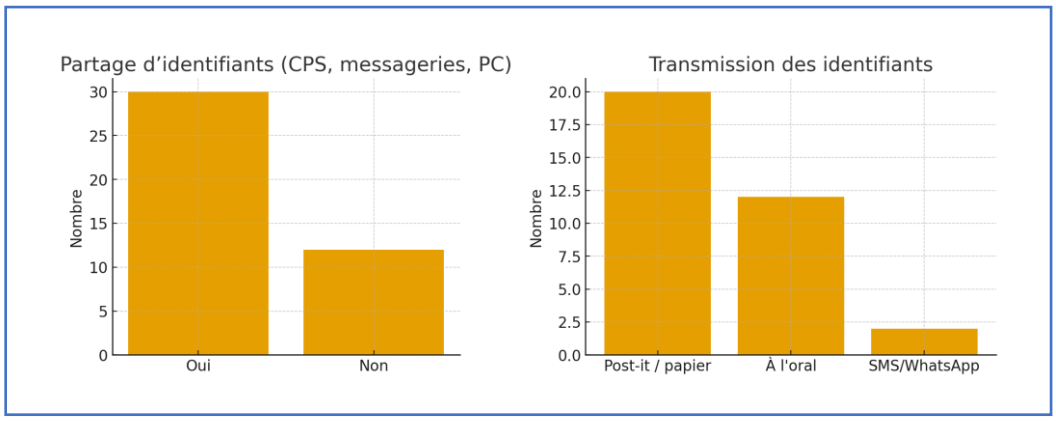



**Figure 15 : transmission des identifiants**

### 4g) Téléconsultation et matériel utilisé

**Q29- Vous arrive-t-il de travailler à domicile avec un ordinateur (téléconsultation par exemple) ?*

*- Oui avec mon ordinateur personnel*

*- Oui avec mon ordinateur professionnel*

*- Non*

**Q30- Vous avez déclaré utiliser votre ordinateur professionnel à domicile.*

*Vous arrive-t-il de l'utiliser à des fins personnelles ?*

*Oui / Non*

Bien que 33,33 % des répondants (14 personnes) utilisent leur ordinateur professionnel pour le télétravail, près d'un quart d'entre eux (23,81 %, soit 10 personnes) l'utilisent également à des fins personnelles.

## 4h) Moyens de partage de documents aux patients

*Q31- Par quel(s) moyens transmettez-vous vos documents aux patients ?*

- *Sur leur mail personnel*
- *En leur envoyant un sms/mms*
- *Clef USB*
- *Via une plateforme sécurisée (exemple Doctolib)*
- *Autre*

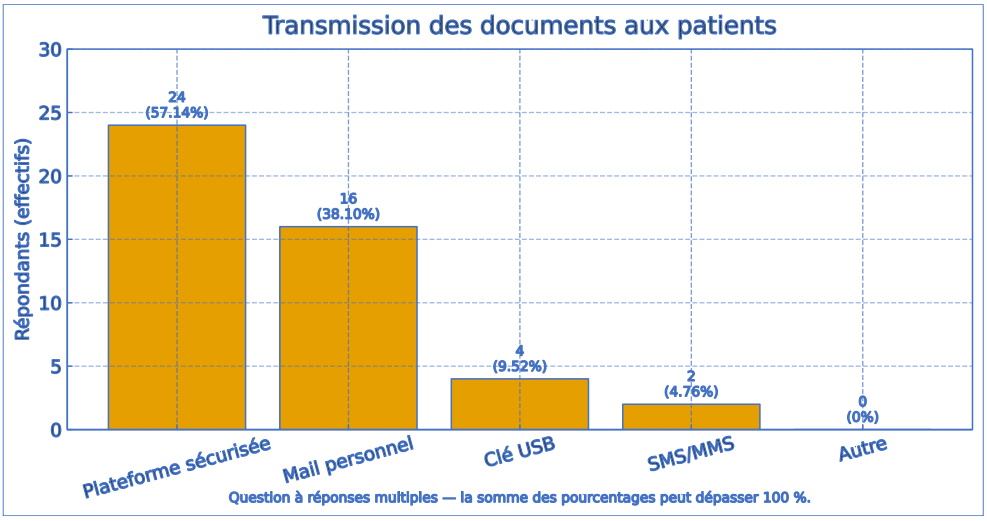



**Figure 16 : Transmission des documents aux patients**

Pour partager des documents médicaux avec leurs patients, plus de la moitié des répondants (57,14 %, soit 24 personnes) utilise une plateforme sécurisée comme Doctolib.
Cependant, des pratiques moins sécurisées sont encore courantes :
- 38,10 % des répondants (16 personnes) envoient des documents sur l'e-mail personnel du patient.
- 9,52 % (4 personnes) utilisent une clé USB.
- 4,76 % (2 personnes) se servent même de SMS ou de MMS.

## 5) Profil des répondants

*Q32- Dans quelle tranche d'âge vous situez vous ?*

*25-35 ans / 36-45 ans / 46-55 ans / 56-65 ans / 66 ans et plus*

*Q33- Exercez-vous dans un de ces secteurs : Boulogne, Calais, Dunkerque et alentours (à moins de 20 kms de ces villes) ?*

*Oui / Non*

*Q34- Quel est votre mode d'exercice ?*

*Libéral seul / libéral en groupe / maison de santé / salarié*

### 5a) Age, mode et lieu d'exercice

La population de notre étude est relativement jeune, avec une majorité de répondants ayant moins de 45 ans. Plus d'un tiers (38.10%, soit 16 répondants) se situe dans la tranche 36-45 ans, suivi par les 25-35 ans (26.19%, soit 11 répondants). Les tranches d'âge plus avancées (56-65 ans à 19.05% et 66 ans et plus à 7.14%) sont moins représentées. Tous les répondants ont affirmé exercer dans le secteur de la côte d'Opale.

La plupart des médecins qui ont répondu au questionnaire exercent en libéral dans un cabinet en groupe (45.24%, soit 19 répondants), et en libéral seul (33.33%, soit 14 répondants).

Les médecins exerçant en maison de santé représentent 19.05% (8 répondants), et un seul répondant (2.38%) est salarié.

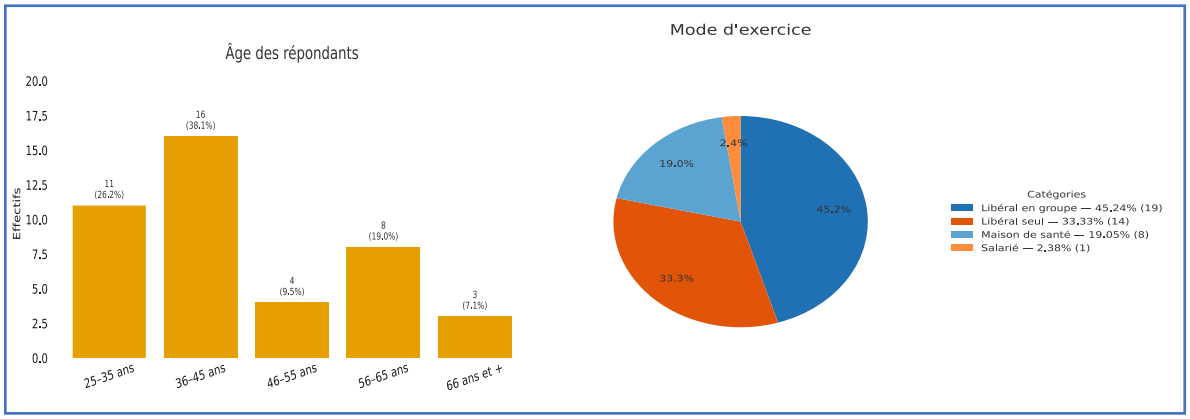



**Figure 17 : Age des répondants et mode d'exercice**

## 6) Ethique et cadre légal autour de la cybersécurité

### 6a) Cyberattaque subie et réaction en cas d'attaque

**Q35- Vous ou la structure dans laquelle vous exercez a-t-elle subi une cyberattaque (phishing, malware, etc...)*

*Oui / Non*

**Q36- Sauriez-vous immédiatement réagir en cas de cyberattaque ?*

*Oui / Non*

La grande majorité des participants (97,62 % soit 41 répondants) n'a jamais subi de cyberattaque. Un seul répondant (2,38 %) déclare en avoir été victime.
La plupart des participants reconnaissent ne pas être préparés à cette éventualité. En effet, 80,95 % des répondants (34 personnes) avouent qu'ils ne sauraient pas comment réagir immédiatement s'ils étaient la cible d'une cyberattaque.

### 6b) Connaissance / conscience du RGPD des obligations légales et juridiques

**Q37- Connaissez-vous le Règlement Général sur la Protection des Données (RGPD) ?*

*Oui / Non / Un peu*

**Q38- Avez-vous conscience des obligations légales concernant la protection des données des patients ?*

*Oui, très bien / En partie / Non*

**Q39- Connaissez-vous les conséquences juridiques d'une fuite de données médicales ?*

*Oui / Non*

**Q40- Si vous êtes victime d'une cyberattaque, pensez-vous que votre responsabilité puisse être engagée vis-à-vis de vos patients à cause des données personnelles compromises ?*

*Oui / Non*

La majorité des participants 45.24% (19 répondants) a une connaissance "partielle" du RGPD, tandis qu'un peu plus d'un tiers 35.71% (15 répondants) ne le connaît pas du tout. Seuls 19.05% (8 répondants) des répondants déclarent bien connaître ce règlement.

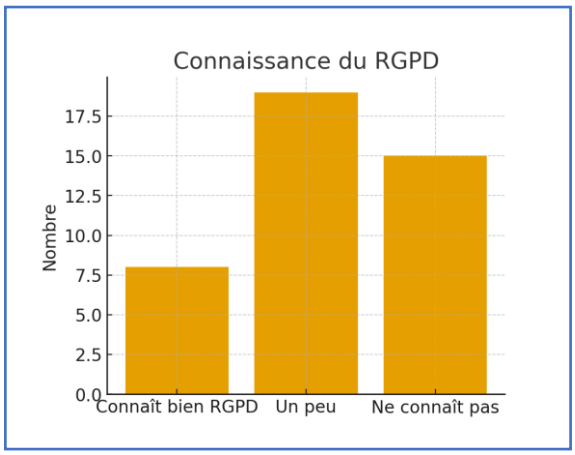



**Figure 18 : connaissance du RGPD**

Cette méconnaissance se reflète dans la conscience des obligations légales :
80.95% (34 répondants) des participants en ont conscience "en partie".
14.29% des répondants (6) n'en ont aucune conscience.
Seuls 4,76 % (6 médecins) se disent "très bien" informés de leurs obligations en matière de protection des données patients.

## 6c) Conséquences d'une fuite de données

En cas de fuite de données, une écrasante majorité des participants (90,48 %, soit 38 répondants) ne connaît pas les conséquences juridiques qui en découlent. Seuls 9,52 % (4 répondants) des répondants en sont conscients.

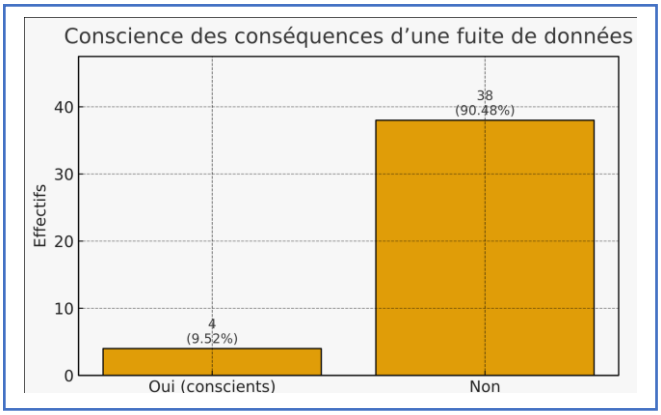



**Figure 19 : Conscience des conséquences d'une fuite de données**

## 7) Impact du questionnaire

**Q41- Ce questionnaire vous a-t-il donné envie de modifier vos habitudes informatiques ou de suivre une formation spécifique en cybersécurité ?*

*Oui / Non*

66.67% (28 répondants) déclarent que le questionnaire leur a donné envie de modifier leurs habitudes informatiques ou de suivre une formation spécifique en cybersécurité.

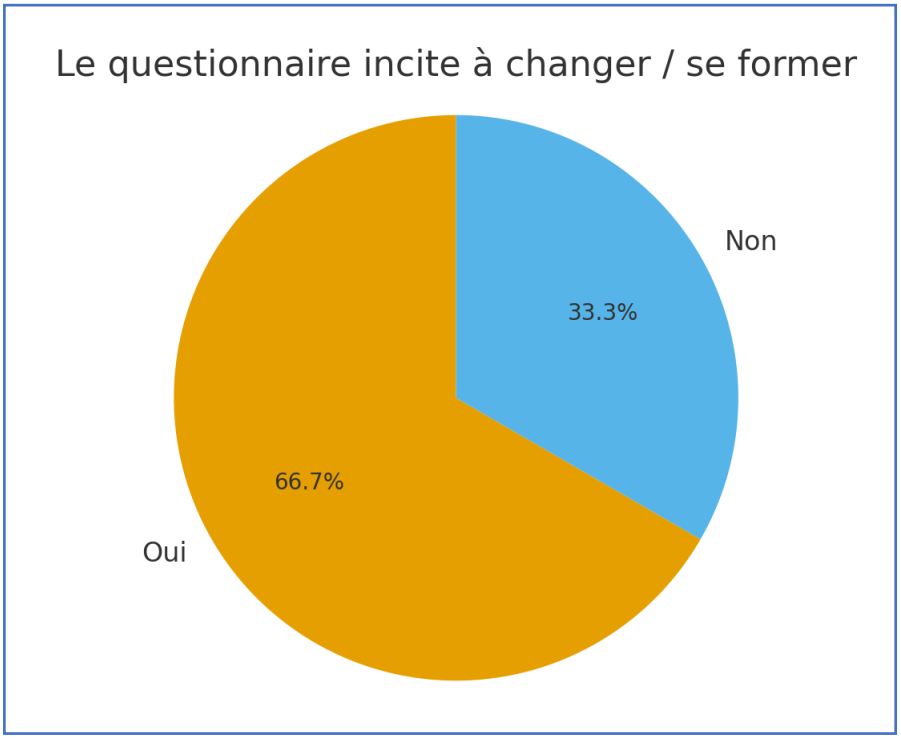



**Figure 20 : Impact du questionnaire**

# DISCUSSION

Les quatre grandes finalités des cyberattaques sont l'appât du gain, la déstabilisation, l'espionnage ou encore le sabotage. A l'aide d'un questionnaire composé de 41 questions organisées en 4 axes principaux, nous avons tenté de faire un état des lieux des connaissances et des pratiques relatives à la cybersécurité des médecins généralistes de la côte d'Opale.

La première observation issue de notre étude est que l'échantillon est particulièrement jeune, en effet la majorité des répondants est âgée de moins de 45 ans. En France, la population générale des médecins généralistes est âgée en moyenne de 52 ans, et le nombre de médecins de plus de 60 ans représentait environ 34 % en 2021[18]. On peut envisager plusieurs hypothèses explicatives : nous avons sélectionné une population ciblée, la région pourrait être particulièrement attractive pour les jeunes diplômés, ou tout simplement, les jeunes seraient plus enclins à répondre à ce type de questionnaire. Il convient de noter que la grande majorité des jeunes générations de médecins présentent certaines compétences intrinsèques au fait d'avoir souvent grandi dans un environnement technologique, où l'appropriation des outils numériques est bien sûr un enjeu individuel (en France, le grand public découvre Internet à partir de 1994), mais également social. Cette relative jeunesse peut également influencer le niveau de cybersécurité des jeunes générations qui ont généralement un rapport plus facilité, au numérique et à l'internet, mais pas forcément une meilleure formation préalable aux risques ou aux bonnes pratiques de sécurité.

D'autre part, les modes d'exercice sont majoritairement libéraux et en groupe, suivis du libéral seul. L'exercice en maison de santé, bien que moins représenté dans notre échantillon, témoigne de l'évolution des pratiques et des structures d'organisation des soins primaires en France. [19]. La quasi-absence de médecins salariés (2,4%, soit 1 médecin) dans notre échantillon est notable et reflète la part minoritaire qu'occupe ce mode d'exercice dans la pratique de la médecine générale en France.

Nos résultats mettent en évidence un faible niveau de connaissances en cybersécurité des médecins généralistes sollicités. La très grande majorité estime leurs connaissances « médiocres » et près d'un tiers « moyennes ». Ce constat rejoint les investigations d'autres études montrant un manque de sensibilisation des professionnels de santé à la cybersécurité. [20, 21]

Les sources de connaissances des médecins en cybersécurité sont diverses mais peu structurées. Une part importante (66,7 %) n'a pas mentionné de source, et parmi celles données, l'expérience professionnelle antérieure, l'intérêt personnel ou les conseils de professionnels extérieurs sont rapportées par une grande majorité des répondants. Les formations continues reconnues comme celles proposées dans le cadre du Développement Professionnel Continu (DPC) sont très peu évoquées (2,4 %), et pour 83,3 % des répondants, il n'y a pas eu de formation personnelle récente.

Il existe une grande diversité de cyberattaques, les plus connues sont résumées dans l'encart n°2.**[22]**

*Encart 2 : Liste non-exhaustive des principales attaques [22]*

**Hameçonnage ou phishing**

« Démarche consistant à transmettre une communication frauduleuse qui semble émaner d'une source de confiance, le plus souvent par courriel, en vue de récupérer des données sensibles comme des informations de carte de crédit ou d'identifiants de connexion ou de propager un logiciel malveillant sur l'appareil de la victime. L'hameçonnage est une des cybermenaces les plus répandues » [22]

**Attaque de l'homme du milieu**

Les attaques de l'homme du milieu (HDM) ou « attaque de l'intercepteur » se produisent lorsque les agresseurs s'insèrent au milieu d'une connexion entre deux machines à distance. Les agresseurs peuvent filtrer et voler des données une fois le trafic de la connexion sous contrôle. [22]

**Attaque par déni de service**

« Une attaque par déni de service consiste à inonder les systèmes, les serveurs ou les réseaux de trafic dans le but d'épuiser les ressources et la bande passante. Le système n'est donc plus en mesure de répondre aux demandes légitimes. Les agresseurs peuvent également utiliser plusieurs appareils compromis pour lancer ce type d'attaque. Il s'agit alors d'une attaque par déni de service distribué (DDoS). » [22]

**Injection SQL**

« Une injection SQL (*Structured Query Language*) se produit lorsqu'un agresseur insère du code malveillant dans un serveur qui utilise le langage SQL et force le serveur à révéler des informations qu'il ne devrait pas. Un agresseur peut effectuer une injection SQL en soumettant simplement du code malveillant dans une case de recherche de site Web vulnérable. » [22]

**Cheval de Troie**

Installation sur l'ordinateur de la victime d'un programme pour remplir une tâche malveillante (espionnage, envoi massif de spam *etc*.) [22].

**Programmes malveillants (dont rançongiciel, menace la plus courante)**

Un programme malveillant est une expression utilisée pour décrire les logiciels malveillants (logiciels espions, les rançongiciels, les virus et les vers). Il s'introduit dans un réseau par le biais d'une faille, généralement lorsqu'un utilisateur clique sur un lien dangereux ou sur une pièce jointe qui installe ensuite un logiciel à risque. Une fois dans le système, le logiciel malveillant peut :

- Bloquer l'accès aux composants clés du réseau (rançongiciel),
- Installer d'autres logiciels pirates
- Obtenir des informations sur la victime en transmettant des données depuis le disque dur infecté (logiciel espion),
- Perturber certains composants et rendre le système inutilisable. [22]

**Exploit du jour zéro**

« Un exploit du jour zéro se produit après l'annonce d'une vulnérabilité dans un réseau mais avant l'implémentation d'un correctif ou d'une solution. Les agresseurs ciblent la vulnérabilité révélée pendant ce court laps de temps. La détection des menaces de vulnérabilité du jour zéro nécessite une efficacité permanente. » [22]

**Tunnellisation DNS**

« La tunnellisation DNS utilise le protocole DNS pour communiquer le trafic non DNS sur le port 53. Il envoie le trafic HTTP et tout autre trafic de protocole via DNS. Il existe diverses raisons légitimes d'utiliser la tunnellisation DNS. Cependant, il existe également des raisons malveillantes d'utiliser des services de réseau privé virtuel (RPV) de tunnellisation DNS. Ils peuvent être utilisés pour déguiser le trafic sortant en DNS, masquant les données qui sont généralement partagées via une connexion Internet. Dans le cadre d'une utilisation malveillante, les requêtes DNS sont manipulées pour exfiltrer les données d'un système compromis vers l'infrastructure de l'agresseur. Ils peuvent également être utilisés pour effectuer des rappels de commande et de contrôle depuis l'infrastructure de l'agresseur vers un système compromis. » [22]

Concernant la connaissance des attaques informatiques, si le cheval de Troie et l'hameçonnage (*phishing*) sont relativement bien identifiés (85,71% et 78,57% respectivement), la connaissance des rançongiciels (*ransomware*) est moins répandue (40,48%). Cette lacune peut être dommageable car les attaques par ransomware constituent une menace majeure et récurrente contre les établissements de santé et les cabinets médicaux, capables d'entraîner des interruptions de service et des fuites de données [23] [24] **(voir Annexe 4)**. Il existe des assurances spécifiques mais qui exigent une conformité stricte avec le RGPD et toutes les mesures « cyber-responsables » (Sauvegardes externalisées et testées, mises à jour régulières, etc…). Le risque étant exponentiel, seuls les frais d'accompagnement et de récupération sont parfois payés et non la rançon demandée par les pirates et, seulement sur dépôt de plainte de la victime (au plus tôt). [25]

La très faible identification d'attaques plus techniques comme le déni de service (DDoS) ou l'homme du milieu (MitM) (7,14% et 2,38% respectivement) confirme un besoin de sensibilisation plus approfondie. La connaissance du chiffrement des données est partagée (52,38% le connaissent), mais celle du Règlement Général sur la Protection des Données (RGPD) reste insuffisante. Moins de la moitié des répondants (45,24%) le connaissent "un peu", et seulement 19,05% déclarent le connaître. Il s'agit d'un point inquiétant car le RGPD impose une obligation de conformité légale en matière de protection des données personnelles, avec des sanctions financières en cas de non-conformité [26]. Certes, la majorité des répondants (80,95%) n'ont qu'une « prise de conscience » partielle de leurs obligations légales concernant la protection des données des patients, mais, par contre, 90,48% des médecins interrogés ne savent pas quels sont les effets juridiques pouvant résulter d'une fuite de données médicales.

Ce décalage entre une conscience générale de l'importance de la protection des données à caractère personnel et une méconnaissance des détails légaux ainsi que des effets qui s'ensuivent est une source de vulnérabilité importante.

## Pratiques en cybersécurité : des habitudes à risque et des vulnérabilités critiques

Les pratiques du quotidien en cybersécurité de notre échantillon mettent en avant des manques importants. La gestion de la sécurité des systèmes informatiques est principalement assurée par les médecins eux-mêmes (42,86 %) puis par un tiers professionnel (33,33 %). 78,6% des cabinets disposent d'un antivirus et/ou pare-feu, mais une part non négligeable (14,29 %)

ignore s'ils en possèdent un ou non.

Les pratiques concernant les mots de passe sont également préoccupantes avec 73,8 % qui ne changent pas régulièrement leurs mots de passe de leur boîte mail et de leurs logiciels médicaux.83,3 % des praticiens interrogés ne changent pas ceux de leur session sur leur ordinateur. Pour finir 7,1 % qui n'ont aucune session protégée par mot de passe. Des chiffres supérieurs à ceux relevés dans d'autres secteurs professionnels [27]. Des recommandations comme celles de posséder un mot de passe robuste (un bon mot de passe doit contenir au minimum 12 signes mélangeant lettres majuscules, lettres minuscules, chiffres et caractère spéciaux) sont pourtant primordiales pour sécuriser son poste de travail [28].

Les boîtes mail encore plus ciblées, surtout lorsqu'elles sont reliées à de nombreux comptes en ligne, imposent davantage un mot de passe robuste. En effet si la boîte mail tombe dans les mains d'un cybercriminel, les conséquences peuvent être désastreuses dans le sens où il suffit de cliquer sur « mot de passe oublié » et le pirate pourra en quelque sorte "contrôler votre vie numérique". **(Annexe 5 : Mémo/conseils gestion des mots de passe [29])**

L'authentification à deux facteurs (2FA) est sans aucun doute une mesure de sécurité essentielle ; pourtant la moitié des répondants ne l'emploie pas et un tiers (33,3%) n'en a jamais entendu parler. Son emploi insuffisant expose gravement les systèmes à des accès non autorisés, même en cas de mot de passe compromis. Pour renforcer la sécurité de nos accès, de plus en plus de services proposent cette option. « En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), *via* une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pouvez autoriser un nouvel appareil à se connecter aux comptes protégés. » [30]

La gestion des sauvegardes, cruciale pour la résilience face aux cyberattaques, présente également des faiblesses. Bien que 66,7% effectuent des sauvegardes hebdomadaires ou moins, 21,4% n'en n'effectuent jamais. Le stockage des sauvegardes sur des supports physiques externes (52,4%) ou le cloud (38,1%) est courant, mais 28,6% des médecins répondants stockent leur disque dur de sauvegarde au cabinet, le rendant vulnérable à un incident unique. La méconnaissance du cryptage des données sauvegardées par la moitié des répondants (50%) est également préoccupante, car cela expose les données à la confidentialité en cas de vol du support. **(Annexe 6 : 10 conseils pour la réalisation de sauvegardes [31])**

Si la mise à jour régulière des logiciels et systèmes d'exploitation est une pratique quasi universelle (97,7%), la fermeture de session d'ordinateur en quittant le cabinet est moins systématique (64,3% systématiquement, 26,2% oublient parfois). Dans un système en constante évolution, l'importance de mettre à jour les logiciels et systèmes d'exploitation permet de lutter contre de nouvelles failles de sécurité qui peuvent compromettre l'ensemble du système informatique. De nos jours, il semble facile de réaliser cette action, en activant l'option de mis à jour automatiques.

Les modes de communication avec les patients et les professionnels de santé sont révélateurs d'une disparité entre une sécurisation par des outils avérés (messageries, courriels professionnels sécurisés) et la persistance de pratiques risquées. La part élevée des téléphones mobiles à usage mixte (47,7 %), l'usage d'adresses électroniques personnelles (35,7 %), des SMS/MMS (26,2 %) ou des messageries privées (16,7 %) pour échanger des données susceptibles d'être sensibles ne sont pas compatibles avec la règlementation en matière de sécurité et de confidentialité des données de santé [32].

Le partage des identifiants de connexion (71,4 %) et leur transmission sur support physique (47,6 %) ou oralement (28,6 %) représentent un usage à risque très élevé où tout dispositif de sécurité individuelle devient obsolète. Ce constat semble illustrer un besoin urgent de former et sensibiliser aux pratiques organisationnelles de sécurité. Enfin, l'usage de l'ordinateur professionnel sur le lieu du domicile est récurrent (33.3 %), et est également utilisé à des fins personnelles pour 23,8 %, élargissant le périmètre d'exposition à la menace.

La transmission de documents aux patients par mail personnel (38,1 %), USB (9,5 %) ou SMS/MMS (4,8 %) persiste malgré l'existence de solutions professionnelles sécurisées comme Doctolib, pourtant utilisé par 57,1 % des participants.

## Perception des risques et besoins : un potentiel de sensibilisation

La perception du cyber-risque dans notre échantillon est globalement faible, ne comptabilisant que 2,4% des répondants ayant déjà été victime d'une cyber-attaque. Ce chiffre, potentiellement sous-estimé en raison d'une méconnaissance des principales formes de cyberattaque, pourrait expliquer une certaine apathie vis-à-vis des mesures de sécurité. Néanmoins, l'élément marquant vient de ce haut pourcentage (80,9%) de répondants ne sachant pas réagir immédiatement en cas de cyber-attaque. Une grande majorité (90,5%) des répondants estiment qu'ils pourraient être mis en cause en cas de fuite des données. Cet aveu de responsabilité légale, malgré la faible exposition au risque perçu, est un levier possible à

exploiter pour la mise en place d'actions de formation. Malgré les lacunes identifiées, plus de la moitié des répondants (54,8 %) ne ressent pas le besoin de suivre ou de poursuivre une formation en cybersécurité en début de questionnaire. L'absence d'intérêt, possiblement liée à une surcharge de travail ou à la priorité accordée à certaines formations médicales, constitue un défi de premier ordre. La bonne nouvelle est néanmoins que 66,67 % des répondants déclarèrent à la fin du questionnaire qu'il leur a donné envie de modifier leurs usages informatiques ou de suivre une formation au choix. Ce qui montre que le simple fait d'être attentif aux questions et enjeux de la cybersécurité, même au travers d'un questionnaire, peut contribuer à une prise de conscience et stimuler une demande de formation.

## Limites de l'étude et perspectives

Notre étude comporte plusieurs limites. La taille modeste de l'échantillon (n=42) limite la possibilité de généraliser nos résultats à l'ensemble des médecins généralistes français. De surcroît, le choix du terrain d'étude, la Côte d'Opale, et le fait que nos répondants se caractérisent par un profil démographique plus jeune que la moyenne nationale peut également introduire un biais. Notons enfin que les pratiques étudiées reposent sur les auto déclarations des participants, qui peuvent être différentes de leurs comportements réels. N'oublions pas que même si le médecin est seul maître et garant de son système informatique, celui-ci est souvent partagé (secrétariat, remplaçants, étudiants…). De ce fait, cette composante n'a pas pu être étudiée finement.

Cependant, notre étude apporte des éléments significatifs sur les connaissances et pratiques des médecins généralistes dans une région spécifique. Elle met en lumière de nombreuses vulnérabilités qui imposent une intensification des efforts de sensibilisation et de formation à destination des professionnels de santé. Des formations pragmatiques, interactives et accessibles, s'attachant aux risques les plus fréquents (ransomware, phishing par exemple), aux bonnes pratiques (gestion de mots de passe forts, authentification à double facteur, sauvegardes effectives, etc.) et aux implications juridiques du RGPD sont plus qu'un impératif. L'effet « déclic » observé par le questionnaire témoigne du fait que des interventions éducatives bien pensées peuvent améliorer les comportements en matière de cybersécurité et contribuer à la protection des données de santé des patients [33].

## Charge de Travail Accablante et Contraintes de Temps

Les médecins généralistes en France font face à des horaires de travail qui sont très denses. Ils déclarent réaliser en moyenne 54 heures de travail à la semaine, dont environ 44,5 heures sont consacrées aux patients. Environ deux tiers des généralistes libéraux déclarent travailler au moins 50 heures par semaine. [34]

La mission principale des médecins généralistes est d'assurer un service de prévention, de dépistage précoce, la prise en charge des maladies chroniques et la coordination des soins. Ces responsabilités déjà très chronophages, limitent d'emblée le temps dédié aux tâches non cliniques, comme l'informatique et la cybersécurité. Il faut donc que toute stratégie de cybersécurité efficace conçue pour les médecins généralistes tende à minimiser l'investissement en temps et à être intégrée de manière fluide dans les flux de travail cliniques et administratifs. Elle doit offrir des avantages immédiats et clairs pour ne pas être considérée comme une tâche administrative de plus à ajouter au planning déjà trop chargé des médecins généralistes. [35][36][37][38]

## Cyberattaque, cadre légal et conséquences

Une cyberattaque réussie contre un cabinet médical peut avoir des conséquences dramatiques telles que la perte ou l'altération des données patients, l'interruption de l'activité, l'atteinte à la réputation. De plus, en cas de non-respect du RGPD des sanctions légales encadrent le traitement des données personnelles sur le territoire de l'Union européenne (Cf. **Encart 3** : Obligations légales spécifiques en médecine générale). Par exemple, le 11 mai 2023, la CNIL a prononcé une sanction de 380 000 euros à l'encontre du site web doctissimo.fr pour avoir manqué à des obligations du RGPD, entre autres l'obligation de recueillir le consentement des personnes à la collecte et à l'utilisation de leurs données de santé [39][40].

***Encart 3 : Obligations légales spécifiques en médecine générale***

**(RGPD et données de santé)**

- **Sécurité et confidentialité des données de santé :** Vous avez obligation d'assurer la sécurité et la confidentialité des données de santé de vos patients, données sensibles par nature, et qui dès lors, doivent faire l'objet de mesures de sécurité renforcées.
- **Consentement explicite :** Obtenez le consentement explicite de vos patients afin d'effectuer le traitement de leurs données.
- **Hébergeur de Données de Santé (HDS) :** Si vous faites appel à un hébergeur tiers pour vos données de santé, il doit être HDS certifié.
- **DPO (Délégué à la Protection des Données)** : La désignation d'un DPO (Délégué à la Protection des Données) n'est pas obligatoire pour tous les cabinets de médecine générale mais elle peut vous être utile pour vous aider à répondre aux exigences du RGPD. [41]

Une cyberattaque peut laisser penser aux patients que le médecin n'a pas mis en place les mesures de sécurité nécessaires pour protéger leurs données. Cela peut mettre en doute les compétences du professionnel et sa capacité à gérer les informations sensibles. Les risques sont tous aussi importants pour le professionnel de santé lui-même. En effet, en cas de fuite de données, le médecin peut faire l'objet de poursuites judiciaires et être tenu pour responsable des dommages causés aux patients. Cela peut entraîner des sanctions financières importantes. Il peut être tenu pour responsable s'il :

- N'a pas mis en place les mesures de sécurité requises : L'absence de pare-feu, de mises à jour régulières des logiciels, de sauvegardes ou de mots de passe forts peut être considérée comme une faute.

- N'a pas notifié la violation de données dans les délais impartis : En cas de fuite de données, le médecin est tenu de notifier la Commission Nationale de l'Informatique et des Libertés (CNIL) et les personnes concernées dans les 72 heures.

- N'a pas pris les mesures nécessaires pour limiter les conséquences de l'attaque : Le médecin doit mettre en œuvre toutes les actions possibles pour limiter les dommages causés par la cyberattaque.

Les sanctions encourues en cas de non-respect des obligations légales peuvent être importantes. La CNIL peut en effet infliger des amendes pouvant atteindre 4% du chiffre d'affaires mondial annuel de l'entreprise ou 20 millions d'euros, le montant le plus élevé étant retenu [42]. En cas de faute grave, le médecin peut faire l'objet de poursuites pénales pour violation de la vie privée, atteinte à l'intimité ou diffusion de données personnelles. Les

personnes physiques encourent 5 ans de prison et jusqu'à 300 000 euros (article 226-16 du Code pénal) d'amende tandis que les personnes morales peuvent payer jusqu'à 1,5 million d'euros de pénalités [43]. Le médecin peut être tenu de réparer les préjudices causés aux patients en raison de la cyberattaque, notamment les préjudices matériels et immatériels.

Avec la multiplication récente des cyberattaques, notamment dans le domaine de la santé, l'Etat a mis en place, en 2023, un plan d'action : le programme CaRE. Celui-ci a pour but de renforcer massivement la cybersécurité des établissements sanitaires et médico-sociaux avec un plan d'action concret et ambitieux pour la période de 2023 à 2027. Le programme, doté d'un budget de 230 millions d'euros, a pour principaux objectifs d'accompagner des établissements à faire face à la cybermenace, favoriser la mutualisation des ressources et des moyens entre les établissements et de sensibiliser et former le personnel des établissements [44].

## Amélioration/optimisation de la gestion de la cybersécurité au cabinet

Afin de limiter le risque de cyberattaque, la prévention est primordiale et des mesures simples doivent être appliquées telles que les mises à jour de sécurité du système d'exploitation et des logiciels. Il est également recommandé d'effectuer des sauvegardes régulières, automatisées et chiffrées des données puis stockage sur des supports déconnectés du réseau principal (hors ligne).

Il faut aussi s'assurer d'avoir des solutions antivirus et pare-feu à jour et actives. Il convient également d'utiliser des mots de passe complexes et uniques pour chaque service, et activez la double authentification si disponible et enfin privilégier les messageries sécurisées de santé (type MSSanté) pour l'échange de données sensibles [45][46][47].

Il est également nécessaire d'intégrer dans le quotidien de chaque cabinet la sensibilisation du personnel aux bonnes pratiques de cybersécurité (reconnaissance des tentatives de phishing, ne pas cliquer sur des liens douteux, etc.). Pour les cabinets utilisant le Wi-Fi (47,62% des répondants), il est particulièrement important de s'assurer que le réseau est sécurisé au minimum avec la norme WPA2 et d'envisager de masquer le nom du réseau (SSID) pour le rendre invisible. Lors des visites à domicile, il est absolument recommandé de ne pas utiliser de réseaux Wi-Fi publics non sécurisés mais de se connecter avec le réseau de l'opérateur mobile ou au moyen du partage de connexion sécurisé par exemple. Conjuguées à la sensibilisation, en suivant comme ci-dessus certaines de ces bonnes pratiques en cybersécurité, les perturbations et l'impact sur la sécurité des patients en cas d'attaque seraient limités voir contrés.

## Perspectives de Recherche et Actions à Long Terme

Notre étude sur la cybersécurité des médecins généralistes de la Côte d'Opale, dont les limites de l'échantillon et sa concentration géographique restreignent le champ d'interprétation, nous semble pourtant fournir des données d'ores et déjà mobilisables. En effet, elle appelle à des perspectives de recherches approfondies et des stratégies d'actions à long terme pour l'ensemble du secteur de la santé. La cybersécurité est un domaine en constante évolution qui cherche à s'adapter aux nouvelles menaces mais également aux avancées technologiques. Une telle dynamique suppose que la recherche tout comme les actions à entreprendre ne peuvent-être statiques : elles doivent être agiles et évolutives.

Plusieurs axes de recherche futurs sont essentiels pour une compréhension plus complète et généralisable de la situation. À plusieurs titres, il reste important de mener des études, avec des échantillons beaucoup plus larges et géographiquement plus diversifiés, non seulement en France mais peut-être dans d'autres pays. Pour finir, la généralisation des résultats permettrait de se doter d'une image nationale ou internationale plus précise des connaissances et des pratiques en matière de sécurité informatique des médecins généralistes. La recherche actuelle repose sur des auto-évaluations dont les résultats peuvent diverger des pratiques réelles mises en œuvre par les médecins généralistes. Il conviendrait qu'un futur travail intègre des données plus objectives (par exemple des audits techniques des systèmes informatiques des cabinets médicaux, en tenant compte des problématiques éthiques et des consentements à recueillir, ou bien des tests d'hameçonnage simulés). Cela permettrait d'évaluer à la fois les vulnérabilités réelles, mais aussi le respect des bonnes pratiques, offrant une compréhension plus robuste de la posture de sécurité effective. Un élément à souligner est que le questionnaire utilisé a aussi constitué un catalyseur d'intérêt vis-à-vis de la formation puisque 66,67 % des répondants affirment vouloir changer leurs habitudes ou se former. Des recherches longitudinales devraient être conduites afin d'apprécier les effets durables et l'impact d'une formation ciblée en cybersécurité. Cela permettrait d'identifier les méthodologies de formation les plus efficaces et leur influence durable sur le comportement. De plus, des actions stratégiques prolongées dans le temps doivent être mises en œuvre pour inscrire résolument la cybersécurité comme un enjeu majeur de la santé numérique.

Pour prévenir les risques ainsi, il serait judicieux d'intégrer dès le début des études de médecine, l'éducation à la cybersécurité comme module nécessaire. Au début de leur carrière, les futurs médecins auraient des connaissances de base et des pratiques en sécurité numérique. Par ailleurs, la formation continue en cybersécurité devrait être rendue obligatoire et intégrée aux dispositifs de Développement Professionnel Continu (DPC) (adaptée aux contraintes des praticiens, avec des formats flexibles).

Il est essentiel d'offrir, dans le cadre d'une plateforme (nationale ou régionale), des guides, outils, aides simples et accessibles. Cette plateforme devrait être spécifiquement adaptée au quotidien numérique du médecin généraliste. Elle pourrait inclure des modèles de politiques de protection des données, des recommandations pour des solutions de cybersécurité certifiées et abordables (antivirus, pare-feu, plateformes de communication sécurisées). Elle guiderait également le médecin sur les procédures claires pour le signalement des incidents et l'accès à une assistance experte. Toutes démarches entreprises par le médecin généraliste, en lien avec la cybersécurité, s'effectuerait via cette unique plateforme qui lui serait réservée.

# CONCLUSION

Plusieurs facteurs expliquent pourquoi les médecins généralistes sont des cibles privilégiées des cyberattaques. Les cabinets médicaux constituent un réservoir d'informations personnelles et médicales sur leurs patients. Ces données sensibles et lucratives, telles que leurs noms, leurs adresses, numéro de sécurité sociale, numéro de retrait sont extrêmement précieuses sur le marché noir. Elles peuvent être utilisées pour des fraudes, des usurpations d'identité, du chantage ou encore revendues à des fins commerciales. Certains cabinets de médecine générale, en particulier les plus petits, disposent parfois de systèmes informatiques moins sophistiqués (anti-virus obsolète, pare-feu inefficace…). Ils sont par conséquent moins bien protégés que les praticiens des grandes structures hospitalières et donc potentiellement plus vulnérables. Par ailleurs, l'utilisation des outils numériques s'accroît. Les médecins généralistes utilisent de plus en plus d'outils numériques pour la gestion des dossiers patients comme la télétransmission des feuilles de soins, devenue la norme, simplifiant les démarches administratives et accélérant les remboursements. Ces pratiques informatiques reposent entièrement sur l'utilisation d'outils numériques et de connexions internet qui doivent être sécurisés [48].

La prise de rendez-vous en ligne est également omniprésente : De nombreux médecins utilisent des plateformes de prise de rendez-vous en ligne, facilitant la gestion de leurs agendas et l'accès aux soins pour les patients. Ces plateformes centralisent des données personnelles et médicales, ce qui soulève des questions de sécurité et de confidentialité [49].

Les enjeux de la cybersécurité au sein du secteur médical sont d’une importance considérable. L’une des conséquences d’une cyberattaque est de rendre l’accès aux systèmes informatiques impossible, donc d’empêcher les outils de prise de rendez-vous, de prescription, de facturation etc… L’un des objectifs directs ou indirects des assaillants étant de détériorer la prise en charge des patients avec un risque de retard important dans les soins. Des dossiers médicaux électroniques de patients peuvent êtres dérobés, ou rendus inaccessibles ; cela compromet la confidentialité des informations personnelles et médicales et complique le suivi. Parallèlement, la coordination entre professionnels de santé, patients et autres acteurs du système de santé peut en être perturbée, entrainant des erreurs dans la conduite du diagnostic et du traitement. Dès lors, ce type d’attaque peut atteindre directement les dispositifs médicaux connectés et affaiblir la prise en charge des patients avec de graves conséquences.

Elle peut également nuire à la relation entre les patients et le médecin généraliste en augmentant le risque de perte de confiance concernant la sécurité de leurs données et la qualité des soins. Il est donc essentiel d'investir dans la formation et la sensibilisation des

professionnels de santé afin d'améliorer les compétences individuelles dans le domaine de la cyberprotection et la cybersécurité. Compte tenu de l'emploi du temps chargé, des formations sont les bienvenues pour les médecins généralistes et de manière générale, aux professionnels de santé. Cependant, des notes d'information, prolixes et régulières sont à privilégier parce que certainement plus attractives que de longues formations en informatique pouvant rapidement noyer des non-informaticiens.

En résumé, pour agir efficacement, prévenir et gérer au mieux une cyberattaque en médecine générale en France, le signalement aux instances dédiées, les bonnes conduites et l'accompagnement par des professionnels de la cybersécurité sont déterminants. (**Annexe 7 : Comment réagir en cas de cyberattaque en 2025)**

# BIBLIOGRAPHIE

**1.** Larousse. Antivirus [Internet]. Paris: Larousse; [cité 26 août 2025]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/antivirus

**2.** Larousse. Chiffrement [Internet]. Paris: Larousse; [cité 26 août 2025]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/chiffrement

**3.** Commission Nationale de l'Informatique et des Libertés. Cloud computing [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cnil.fr/fr/definition/cloud-computing

**6.** Culture.fr. Logiciel espion [Internet]. Ministère de la Culture; [cité 26 août 2025]. Disponible sur: https://fr.wikipedia.org/wiki/Mise_%C3%A0_jour_(informatique)

**5.** Larousse. Hacker [Internet]. Paris : Larousse; [cité le 17 sept 2025]. Disponible chez : https://www.larousse.fr/dictionnaires/francais/hacker/38812

**7.** Wikipédia. Mise à jour (informatique) [Internet]. Paris : Wikimedia Foundation; 2025 [cité le 17 sept. 2025]. Disponible sur : https://fr.wikipedia.org/wiki/Mise_%C3%A0_jour_%28informatique%29

**8.** Kaspersky. Pare-feu (Firewall) [Internet]. Kaspersky France; [cité 26 août 2025]. Disponible sur: https://www.kaspersky.fr/resource-center/definitions/firewall

**10.** Agence du Numérique en Santé. Stratégie nationale cybersécurité [Internet]. Paris: ANS; 2024 [cité 26 août 2025]. Disponible sur: https://esante.gouv.fr/actualites/strategie-nationale-de-cybersecurite

**11.** Tripwire. 750,000 patients' medical records exposed after data breach in French hospital [Internet]. Tripwire; 2024 [cité 26 août 2025]. Disponible sur: https://www.tripwire.com/state-of-security/security-data-protection/750k-patient-records-french-hospital-breach

**9.** Wikipédia. Wired Equivalent Privacy [Internet]. Paris : Wikipédia, la rédaction; [cité le 17 sept 2025]. Disponible chez : https://fr.wikipedia.org/wiki/Wired_Equivalent_Privacy

**12.** Le Quotidien du Médecin. Téléconsultation: 42% de Français conquis en 2024 [Internet]. Paris: Le Quotidien du Médecin; 2024 [cité 26 août 2025]. Disponible sur: https://www.lequotidiendumedecin.fr/actu-medicale/politique-de-sante/teleconsultation-42-des-francais-conquis-en-2024-enquete-tcsware

**13.** SFR Business. Secteur de la santé: défi des cyberattaques [Internet]. Paris: SFR; 2024 [cité 26 août 2025]. Disponible sur: https://www.sfrbusiness.fr/blog/secteur-sante-cyberattaques.html

**14.** Terface. Le marché noir des dossiers médicaux en pleine expansion [Internet]. Terface; 2024 [cité 26 août 2025]. Disponible sur: [10]

**15.** Ministère de l'Économie. La cybersécurité [Internet]. Paris: Gouvernement Français; 2024 [cité 26 août 2025]. Disponible sur: https://www.economie.gouv.fr/entreprises/cybersecurite

**16.** Castellano O. Étude menée en Picardie [thèse de doctorat]. Amiens : Université de Picardie Jules Verne, Faculté de médecine; 2023

**17.** Zerhoui L. Étude menée dans le Nord-Pas-de-Calais [thèse de doctorat]. Lille : Université de Lille, Faculté de médecine; 2020

**18.** Assurance Maladie. La demographie des professionnels de sante au 1er janvier 2021 [Internet]. [cité 26 août 2025]. Disponible sur: https://www.ameli.fr/medecin/actualites/la-demographie-des-professionnels-de-sante-au-1er-janvier-2021

**19.** Direction de la Recherche, des Études, de l'Évaluation et des Statistiques (DREES). (2023). Les maisons de santé pluriprofessionnelles en France. Disponible sur : https://drees.solidarites-sante.gouv.fr/publications/les-maisons-de-sante-pluriprofessionnelles-en-france (Vérifié le 10 juillet 2025)

**20.** Cisco. Common cyberattacks.html [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cisco.com/c/fr_ca/products/security/common-cyberattacks.html

**21.** Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Panorama de la cybermenace [Internet]. 2024 [cité 10 juill 2025]. Disponible sur: https://www.ssi.gouv.fr/

**22.** Cisco. Common cyberattacks.html [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cisco.com/c/fr_ca/products/security/common-cyberattacks.html

**23.** Rieß-Marchive V. Ransomware : un premier semestre 2025 d'une intensité inhabituelle [Internet]. LeMagIT; 15 juil. 2025 [cité le 17 sept. 2025]. Disponible sur : https://www.lemagit.fr/actualites/366627644/Ransomware-un-premier-semestre-2025-dune-intensite-inhabituelle

**24.** Cybermalveillance. Le rancongiciel ransomware [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/le-rancongiciel-ransomware

**25.** Formation Lefebvre-Dalloz. *Cyber-rançons : quelle indemnisation des assurances ?* Paris (France) : Lefebvre-Dalloz; [cité *17 sept 2025*]. Disponible sur : https://formation.lefebvre-dalloz.fr/actualite/cyber-rancons-quelle-indemnisation-des-assurances

**26.** Commission Nationale de l'Informatique et des Libertés. Rgpd en pratique [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cnil.fr/fr/rgpd-en-pratique

**27.** National Institute of Standards and Technology. Digital Identity Guidelines. NIST Special Publication 800-63-3 [Internet]. Gaithersburg (MD): US Department of Commerce; 2020 [cité 26 août 2025]. Disponible sur: https://pages.nist.gov/800-63-3/

**28.** Cybermalveillance.gouv.fr. Bonnes pratiques: mots de passe [Internet]. Paris: Gouvernement Français; 2024 [cité 26 août 2025]. Disponible sur: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

**29.** Cybermalveillance.gouv.fr. Les mots de passe — Fiche Pratique / 10 conseils pour gérer vos mots de passe [Internet]. Paris : Cybermalveillance.gouv.fr; 2024 Mai [cité le 17 sept. 2025]. Disponible sur: https://www.cybermalveillance.gouv.fr/medias/2024/05/220721_FichePratique_MotsDePasse_SCREEN.pdf

**30.** Cybermalveillance.gouv.fr. Pourquoi et comment bien gérer ses mots de passe ? [Internet]. [cité le 18 sept. 2025]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

**31.** Cybermalveillance.gouv.fr. Mémo sauvegardes [Internet]. Paris: Gouvernement Français; 2019 [cité 26 août 2025]. Disponible sur: https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_sauvegardes.pdf

**32.** Ajoodha A. Usage des moyens de communication numérique des médecins généralistes : étude quantitative menée auprès des médecins généralistes installés dans le Nord-Pas-de-Calais [Thèse de médecine]. Lille : Université de Lille, Faculté de médecine Henri Warembourg; 2023 Jan 19. Disponible sur : https://pepite-depot.univ-lille.fr/LIBRE/Th_Medecine/2023/2023ULILM006.pdf

**33.** France-Cybersécurité. Les enjeux de la cybersécurité dans le secteur de la santé : protéger les données des patients [Internet]. [cité 26 août 2025]. Disponible sur : https://www.france-cybersecurite.info/les-enjeux-de-la-cybersecurite-dans-le-secteur-de-la-sante-proteger-les-donnees-des-patients/

**34.** Le Quotidien du Médecin. Agenda 2019 des généralistes : 54 h par semaine, 18 min par consultation et 6,2 semaines de vacances [Internet]. [cité 26 août 2025]. Disponible sur : https://medecine-generale.lequotidiendumedecin.fr/liberal-soins-de-ville/exercice/54-heures-par-semaine-18-mn-par-consultation-et-62-semaines-de-vacances-voila-lagenda-2019-du27.

**35.** Promosante Be. Prevention et promotion [Internet]. [cité 26 août 2025]. Disponible sur: https://promosante.be/prevention-et-promotion

**36.** Maiia. Role [Internet]. [cité 26 août 2025]. Disponible sur: https://www.maiia.com/medecin-generaliste/article/role

**37.** Ars Sante. Download [Internet]. [cité 26 août 2025]. Disponible sur: https://www.ars.sante.fr/media/37685/download

**38.** Caih-sante. Enquete sur le secteur de la sante face au risque cyber [Internet]. [cité 26 août 2025]. Disponible sur: https://www.caih-sante.org/enquete-sur-le-secteur-de-la-sante-face-au-risque-cyber

**39.** CNIL. Décision CNILTEXT000047552103 [Internet]. [cité 26 août 2025]. Disponible sur: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047552103

**40.** Vie-publique. 289281 donnees numeriques de sante quels enjeux pour quel progres medical(Presentation [Internet]. [cité 26 août 2025]. Disponible sur: https://www.vie-publique.fr/eclairage/289281-donnees-numeriques-de-sante-quels-enjeux-pour-quel-progres-medical(Presentation

**41.** CNIL. Sanctions : quelles sanctions peuvent être prononcées par la CNIL ? [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cnil.fr/fr/cnil-direct/question/sanctions-quelles-sanctions-peuvent-etre-prononcees-par-la-cnil

**42.** Conseil National de l'Ordre des Médecins. Protection des données personnelles de santé – FAQ [Internet]. [cité 26 août 2025]. Disponible sur: https://www.conseil-national.medecin.fr/lordre-medecins/conseil-national-lordre/sante/donnees-personnelles-sante/protection-donnees-faq

**43.** Légifrance. Code de la santé publique – Article L.1111-8 [Internet]. 2025 [cité 26 août 2025]. Disponible sur: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049578542/2025-03-24

**44.** Ministère de la Santé. Programme CaRE – Document officiel [Internet]. Paris: Gouvernement Français; 2023 [cité 26 août 2025]. Disponible sur: https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf

**45.** Agence du Numérique en Santé. Mssante [Internet]. [cité 26 août 2025]. Disponible sur: https://esante.gouv.fr/strategie-nationale/mssante

**46.** Nexus-pro-site. Cybersecurite en pharmacie comment proteger vos donnees de sante [Internet]. [cité 26 août 2025]. Disponible sur: https://nexus-pro-site.com/cybersecurite-en-pharmacie-comment-proteger-vos-donnees-de-sante

**47.** CNIL. Données de santé : un impératif, la sécurité [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cnil.fr/fr/donnees-de-sante-un-imperatif-la-securite

**48.** MG France. Système d'information du médecin : 12 règles pour se protéger [Internet]. [cité 26 août 2025]. Disponible sur: https://www.mgfrance.org/actualites/publication/systeme-d-information-du-medecin-12-regles-pour-se-proteger/

**49.** France-assos-sante. Dossier prise de rdv en ligne cet outil pratique est-il veritablement ethique [Internet]. [cité 26 août 2025]. Disponible sur: https://www.france-assos-sante.org/2018/10/10/dossier-prise-de-rdv-en-ligne-cet-outil-pratique-est-il-veritablement-ethique

**50.** France Numérique. Que faire en cas de cyberattaque ? [Internet]. [cité 26 août 2025]. Disponible sur :https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/que-faire-en-cas-de-cyberattaque-5

**51.** Service Public. Actualités – Portail du Gouvernement [Internet]. [cité 26 août 2025]. Disponible sur: https://www.service-public.fr/particuliers/actualites/

**52.** Commission Nationale de l'Informatique et des Libertés. Violations de donnees personnelles les regles suivre [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cnil.fr/fr/violations-de-donnees-personnelles-les-regles-suivre

**53.** Service Public. Actualité: cybersécurité et santé [Internet]. Paris: Gouvernement Français; 2024 [cité 26 août 2025]. Disponible sur: https://www.service-public.fr/particuliers/actualites/A16538

**54.** Cybermalveillance. Le [Internet]. [cité 26 août 2025]. Disponible sur: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/le

# Annexes

## Annexe 1 : Questionnaire, version complète

*Autoévaluation et degré de confiance en votre/vos système(s) informatique(s)*

**1- Comment estimez-vous vos connaissances en Cybersécurité ?**
Médiocres / Moyennes / Bonnes / Excellentes
**2- D'où tenez-vous vos connaissances en Cybersécurité ?**
Expérience professionnelle antérieure / D'une formation dans le cadre du développement professionnel continu / D'un intérêt personnel pour la cybersécurité / De conseils émanant d'un professionnel en cybersécurité / Autre
**3- Vous êtes-vous formé par vos propres moyens en cybersécurité au cours des 2 dernières années ?**
Oui / Non
**4- Eprouvez-vous le besoin de suivre ou poursuivre une formation en cybersécurité ?**
Oui / Non
**5- Attribuez une note de confiance de 0 à 10 à votre système informatique au cabinet (poste de travail)**
0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10
**6- Si vous possédez un smartphone (téléphone connecté à internet), attribuez-lui une note de confiance de 0 à 10**
0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10 / Je n'en ai pas

*La sécurité de votre/vos système(s) informatique(s)*

**7- Avez-vous désigné une personne en charge de la sécurité des systèmes d'information de votre cabinet ?**
Oui, en interne / Oui en externe / Oui en externe et interne / Non je gère moi-même

**8- Votre système informatique dispose-t-il d'un antivirus et/ou pare-feu?**
Oui / Non / Je ne sais pas
**9- Changez-vous régulièrement vos mots de passe de boîte(s) mail(s), logiciels médicaux ?**
Oui au moins une fois par an / Oui moins d'une fois par an / Non / Préfère ne pas le dire
**10- Changez-vous régulièrement votre mot de passe de session d'ordinateur ?**
Oui / Non / Je n'en ai pas / Préfère ne pas le dire
**11- Savez-vous ce qu'est un 'chiffrement des données' ?**
Oui / Non / Je ne sais pas
**12- Utilisez-vous l'authentification à deux facteurs (2FA) pour protéger vos accès aux systèmes médicaux ?**
Oui la plupart du temps / Non / Je ne sais pas ce que c'est
**13- Cette authentification à double facteur est configurée le plus souvent via :**
SMS / Application / Réception d'un mail / Préfère ne pas le dire
**14- Avez-vous connaissance de ces différentes attaques informatiques ?**
Hameçonnage / Phishing / Rançongiciel (Ransomware) / Cheval de Troie / Attaque de l'homme du milieu (MitM) / Déni de service (DDoS) / Fraude au président

*Vos habitudes pratiques de Cybersécurité*

**15- À quelle fréquence organisez-vous vos sauvegardes ?**
Hebdomadaire ou moins / Mensuelle ou moins / Tous les 6 mois / Jamais
**16- Sur quel(s) type(s) de support ?**
Ordinateur du cabinet / Support de stockage externe / Cloud
**17- Où stockez-vous le disque dur servant de sauvegarde des données ?**
Cabinet / Domicile / Autre lieu
**18- Les données sauvegardées sont-elles cryptées ?**
Oui / Non / Je ne sais pas
**19- Mettez-vous régulièrement à jour vos logiciels et systèmes d'exploitation ?**
Oui / Non
**20- Lorsque vous quittez le cabinet, fermez-vous systématiquement votre session d'ordinateur ?**
Oui / Non / Fermeture automatique après inactivité / Préfère ne pas le dire
**21- Quel(s) moyen(s) de communication utilisez-vous pour contacter vos patients ou autres professionnels de santé ?**
Téléphone mobile pro non connecté / Téléphone fixe / Smartphone mixte pro/perso / Email personnel / Email messagerie professionnelle sécurisée / Messagerie privée (WhatsApp, Telegram...) / SMS/MMS / Messagerie sécurisée professionnelle (Omnidoc, Doctolib, etc.)
**22- Concernant l'envoi des mails, sont-ils envoyés depuis un appareil mobile ?**
Oui / Non / Parfois
**23- Prenez-vous des précautions supplémentaires lors du téléchargement de pièces jointes par mail ?**
Toujours / Souvent / Rarement / Jamais
**24- Quel type de connexion internet utilisez-vous au cabinet ?**
Ethernet / Wi-Fi / Bluetooth / Clé 3G/4G/5G / Partage de connexion mobile
**25- Quelles sont les caractéristiques de votre point d'accès Wi-Fi ?**
Wi-Fi public / Wi-Fi sécurisé par mot de passe / SSID visible / SSID caché / Préfère ne pas le dire
**26- Pendant les visites à domicile, quel(s) type(s) de connexion utilisez-vous ?**
Wi-Fi public / Réseau opérateur mobile / Clé 3G/4G/5G / Partage de connexion / Wi-Fi sécurisé patient
**27- Partagez-vous vos identifiants de connexion avec d'autres personnes ?**
Oui / Non
**28- Comment ces informations sont-elles transmises ?**
Support physique (post-it...) / Support dématérialisé (SMS, WhatsApp...) / À l'oral / Autre
**29- Vous arrive-t-il de travailler à domicile avec un ordinateur ?**
Oui avec ordinateur personnel / Oui avec ordinateur professionnel / Non
**30- Si vous utilisez votre ordinateur professionnel à domicile, l'utilisez-vous à des fins personnelles ?**
Oui / Non

**31- Par quel(s) moyens transmettez-vous vos documents aux patients ?**
Mail personnel / SMS/MMS / Clé USB / Plateforme sécurisée / Autre

*Critères démographiques*

**32- Dans quelle tranche d'âge vous situez-vous ?**
25-35 ans / 36-45 ans / 46-55 ans / 56-65 ans / 66 ans et plus
**33- Exercez-vous dans un de ces secteurs (Boulogne, Calais, Dunkerque et alentours) ?**
Oui / Non
**34- Quel est votre mode d'exercice ?**
Libéral seul / Libéral en groupe / Maison de santé / Salarié

*Éthique et cadre légal autour de la cybersécurité*

**35- Vous ou la structure avez-vous déjà subi une cyberattaque ?**
Oui / Non
**36- Sauriez-vous immédiatement réagir en cas de cyberattaque ?**
Oui / Non
**37- Connaissez-vous le Règlement Général sur la Protection des Données (RGPD) ?**
Oui / Non / Un peu
**38- Avez-vous conscience des obligations légales concernant la protection des données des patients ?**
Oui, très bien / En partie / Non
**39- Connaissez-vous les conséquences juridiques d'une fuite de données médicales ?**
Oui / Non
**40- Si vous êtes victime d'une cyberattaque, pensez-vous que votre responsabilité puisse être engagée ?**
Oui / Non
**41- Ce questionnaire vous a-t-il donné envie de modifier vos habitudes ou suivre une formation ?**
Oui / Non

## Annexe 2 : Courrier de demande d'enquête

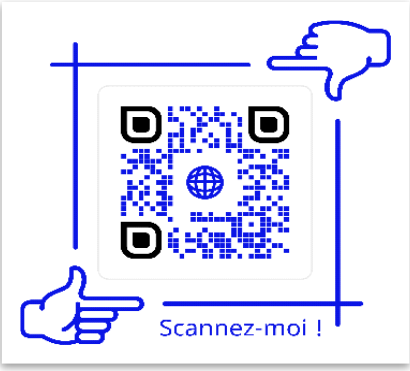
Cher Docteur,

Je me permets de vous solliciter dans le cadre de ma thèse portant sur la cybersécurité au sein de nos cabinets de médecine générale.

Je vous invite à participer à ce questionnaire anonyme en ligne, qui ne vous prendra que 5 min de votre temps.

Le questionnaire est disponible via ce lien :
https://enquetes.univ-lille.fr/index.php/758711

Il est possible également d'y répondre via ce QR code :




L'anonymat de vos réponses est garanti. Aucune information permettant de vous identifier ou d'identifier votre cabinet ne sera collectée. Les données recueillies seront traitées de manière strictement confidentielles et utilisées uniquement à des fins de recherche.

Votre contribution permettra d'enrichir la connaissance sur un enjeu crucial pour la pérennité et la sécurité de notre exercice professionnel, ainsi que pour la protection des données de nos patients. Les résultats de cette étude pourront, à terme, contribuer à l'élaboration de recommandations et de bonnes pratiques adaptées.

Je vous remercie sincèrement pour le temps et l'attention que vous voudrez bien accorder à cette démarche. Votre participation est essentielle. N'hésitez pas à le partager.

Restant à votre disposition pour toute question, je vous prie d'agréer, l'expression de mes salutations distinguées.

Cordialement,

Romain Courtois
Médecine Générale
Université de Lille
romain.courtois.etu@univ-lille.fr

## Annexe 3 : Attestation de conformité avec la CNIL

Université de Lille

**RÉCÉPISSÉ**

**ATTESTATION DE DÉCLARATION**

Délégué à la protection des données (DPO) : Jean-Luc TESSIER

Responsable administrative : Yasmine GUEMRA

La délivrance de ce récépissé atteste que vous avez transmis au délégué à la protection des données un dossier de déclaration formellement complet.

Toute modification doit être signalée dans les plus brefs délais: dpo@univ-lille.fr

**Traitement exonéré**

| |
|---|
| **Intitulé** : Cybersécurité: connaissances et pratiques des médecins généralistes libéraux de la côte d'Opale |
| **Responsable chargé de la mise en œuvre :** M. Adrien DAUZAT<br>**Interlocuteur (s)** : M. Romain COURTOIS |

Votre traitement est exonéré de déclaration relative au règlement général sur la protection des données dans la mesure où vous respectez les consignes suivantes :

- Vous informez les personnes par une mention d'information au début du questionnaire.

- Vous respectez la confidentialité en utilisant un serveur Limesurvey mis à votre disposition par l'Université de Lille via le lien https://enquetes.univ-lille.fr/ (en cliquant sur "Réaliser une enquête anonyme" puis "demander une ouverture d'enquête").

- Vous garantissez que seul (e) vous et votre directeur de thèse pourrez accéder aux données.

- Vous supprimez l'enquête en ligne à l'issue de la soutenance.

Fait à Lille,

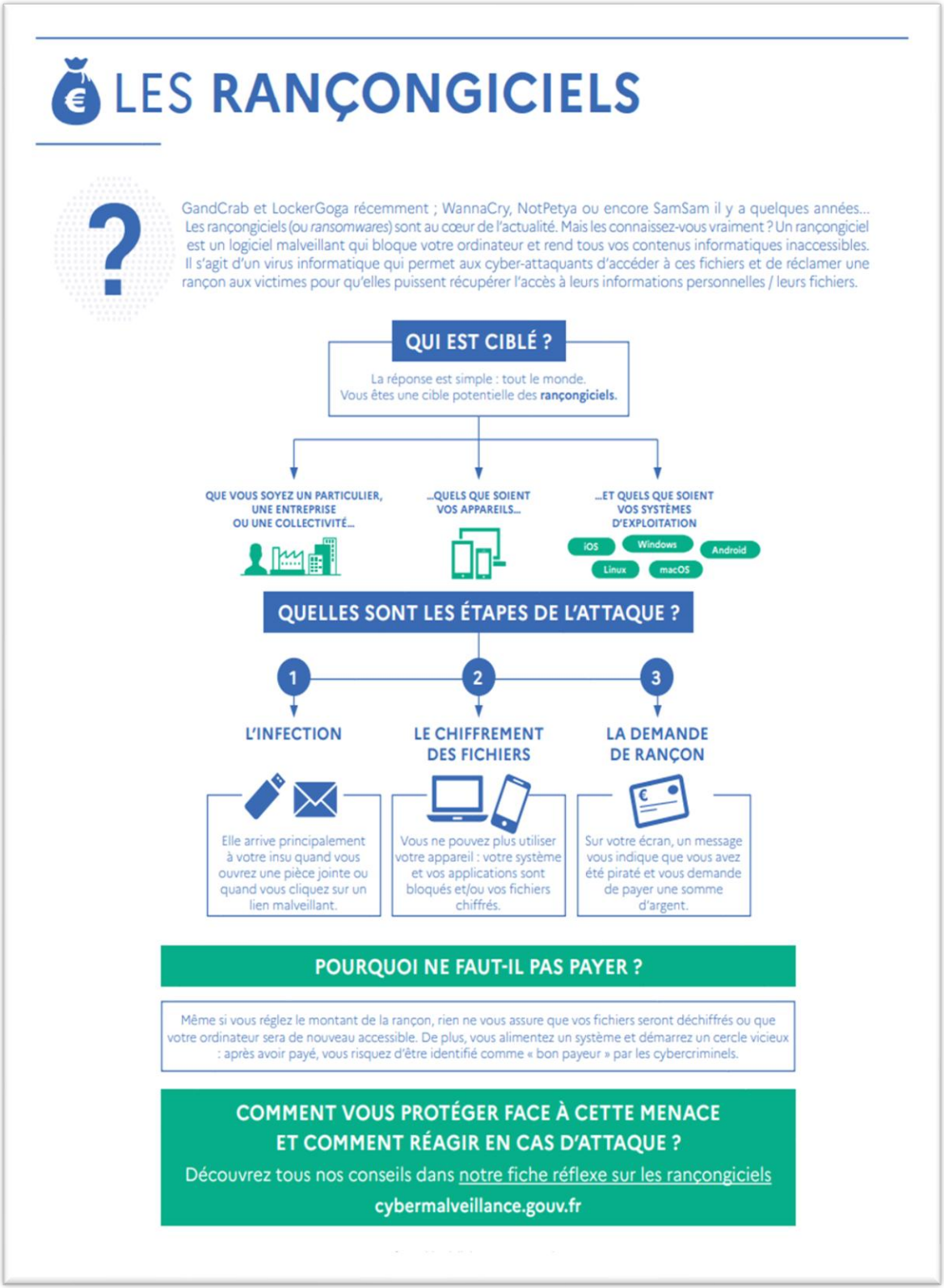
Le 10 février 2025

Jean-Luc TESSIER

Délégué à la Protection des Données

Direction Données personnelles et archives
42 rue Paul Duez
59000 Lille
dpo@univ-lille.fr | www.univ-lille.fr

## Annexe 4 : Fiche réflexe sur les rançongiciels




Source : https://www.cybermalveillance.gouv.fr/medias/2023/06/230531_Kit_sensibilisation.pdf (Licence Ouverte –Etalab v2.0)

## Annexe 5 : Mémo/conseils gestion des mots de passe

# LES MOTS DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.**

### 1 UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

### 2 UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.



### 3 UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

### 4 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès. *Voir notre encadré sur Keepass au dos de cette fiche.*

### 5 CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

### CRÉER UN MOT DE PASSE SOLIDE

**LA MÉTHODE DES PREMIÈRES LETTRES**
Un tiens vaut mieux que deux tu l'auras
**1tvmQ2tl'A**

**LA MÉTHODE PHONÉTIQUE**
J'ai acheté huit CD pour cent euros cet après-midi
**ght8CD%E7am**

**Inventez votre propre méthode connue de vous seul !**

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Source : https://www.cybermalveillance.gouv.fr/medias/2023/06/230531_Kit_sensibilisation.pdf (Licence Ouverte – Etalab v2.0 )

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

## KEEPASS

**UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT**

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires. **https://keepass.info**

### 6 NE COMMUNIQUEZ JAMAIS VOTRE MOT DE PASSE À UN TIERS

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

### 7 N'UTILISEZ PAS VOS MOTS DE PASSE SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

### 8 ACTIVEZ LA « DOUBLE AUTHENTIFICATION* » LORSQUE C'EST POSSIBLE

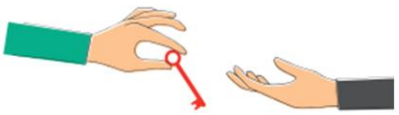
Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option . En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. *Voir encadré.*

### 9 CHANGEZ LES MOTS DE PASSE PAR DÉFAUT DES DIFFÉRENTS SERVICES AUXQUELS VOUS ACCÉDEZ

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

## QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook/Hotmail, Gmail, Yahoo Mail...
- Facebook, Instagram, LinkedIn, Snapshat, Tik Tok, Twitter...
- Skype, Teams, WhatsApp, Zoom...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, OneDrive...



### 10 CHOISISSEZ UN MOT DE PASSE PARTICULIÈREMENT ROBUSTE POUR VOTRE MESSAGERIE

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle. **Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger.**

### POUR ALLER PLUS LOIN

- Par la CNIL: Les conseils de la CNIL pour un bon mot de passe
- Par l'ANSSI: Sécurité des mots

DOCUMENT RÉALISÉ AVEC NOS MEMBRES:
FRANCE ASSUREURS kaspersky LA POSTE signal spam

## Annexe 6 : Conseils/sauvegardes




Source : https://www.cybermalveillance.gouv.fr/medias/2023/06/230531_Kit_sensibilisation.pdf (Licence Ouverte – Etalab v2.0)

## Annexe 7 : Comment réagir en cas de cyberattaque ?

Il convient tout d'abord de réagir vite en respectant des démarches bien précises pour limiter les impacts au sein du cabinet, en protégeant les données à caractère personnel des patients et en respectant nos obligations notamment légales. Si malgré ces efforts, personnels et collectifs, un cabinet médical est victime d'une attaque, une marche à suivre relativement simple est à exécuter.

Il faut immédiatement débrancher les câbles réseau (Ethernet) et désactiver le Wi-Fi des machines potentiellement concernées au risque de laisser repartir de nouvelles communications entre machines (potentiellement infectées). « Il ne faut pas couper l'électricité à l'ordinateur ni aux autres appareils, afin de préserver les traces numériques qui seront restituées à la police judiciaire pour l'analyse forensique. » De plus, il ne faut plus utiliser l'ordinateur infecté [50].

En cas d'attaque par rançongiciel (ransomware), il est fortement déconseillé de payer la rançon. Il n'y a aucune garantie de récupérer les données, ce qui incite les pirates à agir. Bien entendu, les preuves doivent être conservées (aucun fichier ou message ne doit être supprimé ; des captures d'écran des messages de rançon doivent être prises pour l'enquête policière).

Ces éléments seront déterminants pour l'enquête. Il serait également opportun de signaler l'incident auprès de l'outil 17Cyber et de Cybermalveillance.gouv.fr. Les portails 17cyber.gouv.fr et cybermalveillance.gouv.fr offrent une aide en ligne via le chat pour qualifier l'incident et orienter la victime. Il est par ailleurs grandement conseillé de porter plainte auprès de la police ou de la gendarmerie. Le signalement via le site communiquant le 17Cyber peut être utile notamment pour prendre rendez-vous en ligne [51]. En cas de cyberattaque ayant provoqué une violation de données à caractère personnel (perte de disponibilité, d'intégrité ou de confidentialité, d'informations à caractère personnel), la loi impose d'en aviser la CNIL dans les 72 heures suivant la découverte de l'accident [52][53].

La notification s’effectue via le téléservice de notification sur les violations de la CNIL. Selon l’évaluation du niveau de risque, les patients doivent être informés individuellement, ou de manière publique (nom, coordonnées du cabinet, conséquences prévisibles et mesures mises en place).

Pour terminer, il sera aussi nécessaire d'informer le prestataire informatique ou un intervenant en cybermalveillance spécialisés pour résoudre l'incident et le service des assurances. Le site Cybermalveillance.gouv.fr peut mettre en relation la victime avec les organismes spécialisés. Certains contrats d’assurance prévoient la couverture des cyberrisques, et parfois une assistance ou la prise en charge du dommage. Il existe aussi un service d’alerte : le CERT Santé. Il pourra accompagner les structures dans le signalement ; il peut encore les aider par la mise en œuvre de mesures de confinement ou de remédiation [54].

## RESUME

**AUTEUR : Prénom : Romain Nom : Courtois**

**Date de soutenance : 28/11/2025**

**Titre de la thèse : Cybersécurité : connaissances et pratiques des médecins généralistes de la Côte d'Opale**

**Thèse - Médecine - Lille 2025**

**Cadre de classement :** *Médecine Générale*

**DES + FST/option :** *Médecine Générale*

**Mots-clés :** cybersécurité ; médecine générale ; RGPD ; authentification à deux facteurs ; sauvegardes ; messageries sécurisées ; Côte d'Opale

**Résumé :**

**Contexte.** Les cabinets de médecine générale sont de plus en plus exposés aux cybermenaces alors qu'ils traitent des données de santé sensibles.

**Objectif.** Dresser un état des lieux des connaissances et pratiques en cybersécurité des médecins généralistes de la Côte d'Opale.

**Méthodes.** Enquête quantitative, descriptive, transversale par questionnaire en 41 items (LimeSurvey) diffusé aux médecins libéraux de la Côte d'Opale. 316 praticiens contactés ; 42 réponses complètes analysées (taux estimé : 13,2 %).

**Résultats**. Deux tiers jugent leurs connaissances médiocres (66,7 %) ; 83,3 % ne se sont pas formés par eux-mêmes depuis 2 ans. La 2FA est très peu utilisée (16,7 % « la plupart du temps ») et 33,3 % ne savent pas de quoi il s'agit.

Les sauvegardes sont hétérogènes : 66,7 % au moins hebdomadaires, 21,4 % jamais ; supports surtout disque/clé (52,4 %) ou cloud (38,1 %), chiffrement souvent inconnu (≈ 50 %). Les canaux sécurisés progressent (messageries/pro mails sécurisés), mais des usages à risque persistent : téléphone mobile à usage mixte 47,6 %, e-mails personnels 35,7 %, SMS/MMS 26,2 %, messageries privées 16,7 %. Côté organisation, 42,9 % gèrent eux-mêmes la sécurité ; 78,6 % déclarent antivirus/pare-feu (14,3 % ne savent pas). Mots de passe : 73,8 % ne les changent pas régulièrement ; 83,3 % ne changent pas le mot de passe de session, 7,1 % n'en ont pas. Enfin, 80,9 % ne sauraient pas réagir immédiatement en cas d'attaque, mais 66,7 % déclarent que le questionnaire incite à changer leurs pratiques.

**Conclusion.** Les vulnérabilités sont surtout organisationnelles : 2FA, gestion des mots de passe, sauvegardes (3-2-1, chiffrées, externalisées). Les canaux sécurisés doivent être priorisés, avec des actions de sensibilisation/formation ciblées et pragmatiques pour améliorer la conformité RGPD et la continuité des soins.

**<u>Composition du Jury</u> :**

**Président : Professeur Emmanuel CHAZARD**

**Assesseur : Docteur Maurice PONCHANT**

**Directeur de thèse : Docteur Adrien DAUZAT**