UNIVERSITE PARIS 7 – DENIS DIDEROT
FACULTE DE MEDECINE XAVIER BICHAT

[Thèse pour le Doctorat en Médecine]
(Diplôme d'état)

Par BRAMI Grégory
Né le 20 novembre 1978 à Paris XIIIe

Protection des données patients informatisées en médecine générale.

Etude transversale - Département du Val d'Oise
septembre - décembre 2007

Président : M. le Professeur Bergmann Jean-Francois
Directeur : M. le Docteur Wasniewski Alain

[Présentée et soutenue publiquement le 10 juin 2009]

RESIDENT

Remerciements

A ma femme, dont la patience et la compréhension sont infinies,
A mes parents,
A ma grand-mère, qui a toujours été à mes côtés,
A ma famille, en particulier à ma tante, Véronique Moracchini,
A mon directeur de thèse : Dr Alain Wasniewski,
Au président du jury,
Aux membres du jury,
A mes maîtres de stage : Dr Jean Marie Lieges, Dr Nicole Boucherie, Dr Corinne Amoun, Dr Thierry Ouvrard, Dr Vincent Gay, Dr Martine Binelli, Dr Michel Camagna.
A mes amis avec un remerciement particulier à David et Maud Hajage ainsi qu'à Cécile et Arnaud Rochefort,
A M. Jean Paul Le Guigner,
Au Dr Richard Birene,
Au Dr Alain Lavrut,
Au Dr Christine Vaussue.

PROTECTION DES DONNEES PATIENTS INFORMATISEES EN MEDECINE GENERALE

BRAMI Gregory
1 rue Paul Eluard 95120 Ermont
Tel : 06 19 65 46 49
Tel : 01 34 37 01 93
Email : dr_gbrami@yahoo.fr

Madame, Monsieur,

Je prépare actuellement une thèse de doctorat de médecine portant sur la sécurité et la protection des données liées à l'informatisation des cabinets de médecine générale.

A l'heure actuelle, selon les chiffres de l'assurance maladie, près de 80% des médecins libéraux (généralistes et spécialistes) télétransmettent des feuilles de soin électroniques grâce au système SESAM-VITAL. Ce qui implique un certain degré d'informatisation des cabinets médicaux.

Le but de cette thèse, dont vous trouverez le questionnaire ci-joint, est de chercher à savoir si les médecins généralistes libéraux sont sensibilisés à certaines notions de base (nous sommes médecins avant tout et non pas informaticiens) de sécurité et de protection des données informatisées concernant les patients.

En vous remerciant pour le temps que vous passerez à répondre à ces questions.

Confraternellement

PS : Pour répondre aux questions à choix multiple, veuillez cocher la ou les cases correspondantes.
Pour les questions où il faut répondre par oui ou par non, veuillez entourer la réponse correspondante
« ? » Correspond à la réponse : je ne sais pas

Pour les questionnaires sous forme email :
Pour valider vos réponses après avoir rempli le questionnaire merci de sauvegarder le document sur votre disque dur avant de le renvoyer par email sous forme de pièce jointe à l'adresse suivante :
dr_gbrami@yahoo.fr
Le tiret correspond à un underscore (celui que vous trouvez sur la touche numérique 8 en haut de votre clavier).

Protection des données patients informatisées en médecine générale

Le « ? » correspond à la réponse : « je ne sais pas »
Pour chaque réponse exacte, merci de cocher la case prévue à cet effet
Un lexique des termes informatiques est disponible en fin de questionnaire.
Pour les questionnaires sous forme Email, merci de lire la lettre accompagnant le questionnaire afin de connaitre les modalites pour le renvoyer.

Partie I : Généralités

A/ Epidémiologie

Sexe : Homme ☐ Femme ☐ **Année de thèse :**

Date de naissance (JJ/MM/AAAA) : **Année d'installation :**

Exercez vous en groupe ? oui ☐ non ☐

B/ Matériel utilisé

En quelle année avez-vous informatisé votre cabinet ?

Quel matériel utilisez-vous dans votre cabinet ? *(plusieurs choix possibles)*

☐ordinateur fixe	☐écran plat	☐clef USB
☐ordinateur portable	☐scanner	☐graveur de DVD
☐Macintosh	☐imprimante	☐graveur de CD
☐PC	☐assistant personnel (PDA)	☐onduleur

Quand avez-vous renouvelé votre matériel informatique ?
☐Moins de 1 an ☐Entre 1 et 2 ans ☐Entre 2 et 5 ans ☐Plus de 5 ans

	oui	non
Utilisez-vous une connexion Internet pour votre usage professionnel ?	☐	☐

De quel type de connexion s'agit-il ?
☐ADSL ☐câble ☐modem

C/ Utilisation du matériel informatique

	oui	non
Avez-vous des dossiers patient informatisés ?	☐	☐
Utilisez-vous un logiciel de gestion des informations concernant vos patients (ex : Hello doc, Axisanté,…) ?	☐	☐
Utilisez-vous votre ordinateur pour planifier vos rendez-vous ?	☐	☐
Avez-vous un Email professionnel ?	☐	☐
Faites-vous de la télétransmission de feuilles de soin ?	☐	☐
Archivez-vous les résultats des examens complémentaires sous format informatique ?	☐	☐
Avez-vous une comptabilité informatisée ?	☐	☐
Utilisez-vous votre ordinateur comme outils didactique pour vos patients ?	☐	☐
Utilisez-vous une assistance informatique au diagnostic ?	☐	☐
Utilisez-vous une assistance informatique pour vos prescriptions ?	☐	☐
Utilisez-vous votre ordinateur pour rédiger :		
➢ Vos ordonnances ?	☐	☐

➢ Vos demandes d'examens complémentaires ?	oui ☐	non ☐	
➢ Vos certificats ?	oui ☐	non ☐	
Utilisez-vous un aide mémoire informatique pour le suivi de vos patients (vaccins, examens de surveillance…) ?	oui ☐	non ☐	
Utilisez-vous			
➢ le Vidal papier ?	oui ☐	non ☐	
➢ le Vidal CD ?	oui ☐	non ☐	
Avez-vous des dossiers papier ?	oui ☐	non ☐	

Si oui, pour quel type de données ? **zone de texte**

Partie II : Protection des données patients informatisées

A/ Modalités d'accès aux données de vos patients

Avez-vous un mot de passe pour accéder :			
➢ à votre ordinateur ?	oui ☐	non ☐	
➢ à votre logiciel de gestion des données patients ?	oui ☐	non ☐	
Si oui, est-il (sont-ils) alphanumérique(s) (chiffres + lettres) ?	oui ☐	non ☐	
Comporte(nt)-t-il(s) plus de 8 caractères ?	oui ☐	non ☐	? ☐

A quelle fréquence modifiez vous vos mots de passe ?

☐Toutes les semaines ☐Tous les trois mois ☐Jamais
☐Tous les mois ☐Tous les six mois

Utilisez-vous le même mot de passe pour toutes les applications ? (E-mail, session, logiciel de gestion….)	oui ☐	non ☐	? ☐
Utilisez-vous un (des) mot(s) de passe en rapport avec des données personnelles (nom de proche, date de naissance…) ?	oui ☐	non ☐	? ☐
Est-ce que vous notez vos mots de passe pour pouvoir vous en rappeler (sur un post-it par exemple) ?	oui ☐	non ☐	? ☐
Votre ordinateur se met-il en veille après un temps donné sans l'utiliser ?	oui ☐	non ☐	? ☐
Si oui, devez vous rentrer à nouveau votre mot de passe pour pouvoir accéder à vos données patients ?	oui ☐	non ☐	? ☐
Si vous exercez dans un groupe médical :			
➢ **Les ordinateurs des médecins de ce groupe sont ils reliés en réseau ?**	oui ☐	non ☐	? ☐
➢ **Partagez-vous des données patients informatisées avec les autres médecins du groupe ?**	oui ☐	non ☐	? ☐
➢ **Avez-vous un mot de passe commun ?**	oui ☐	non ☐	? ☐
➢ **Chaque médecin a-t-il un mot de passe personnel ?**	oui ☐	non ☐	? ☐
➢ **Avez-vous le même logiciel de gestion des donnees patient pour tout le groupe médical ?**	oui ☐	non ☐	? ☐

B/ Les sauvegardes de vos données patients

Faites-vous des sauvegardes régulières des données concernant vos patients ?

☐Jamais ☐Souvent ☐Je ne sais pas.
☐Parfois ☐Tous les jours

	oui	non
Conservez-vous des sauvegardes sur un support autre que le disque dur de votre ordinateur ?	☐	☐

Si oui, quel(s) support(s) utilisez vous pour vos sauvegardes ?

☐disquettes ☐DVD ☐disque dur externe
☐CD ☐clefs USB ☐autre :zone de texte

Faites-vous des essais de restauration des données sauvegardées pour vérifier leur validité ?

☐Jamais ☐Souvent ☐Je ne sais pas.
☐Parfois ☐Tous les jours

C/ Protection physique

	oui	non	?
Afin d'assurer la protection physique des données patients stockées dans l'unité centrale de votre ordinateur avez-vous placé l'unité centrale dans une zone peu exposée aux variations de température ?	☐	☐	☐
Avez-vous pris des dispositions pour protéger votre unité centrale du vol (ex : local ou meuble de bureau fermé à clef) ?	☐	☐	☐
Afin d'assurer la protection physique des sauvegardes de vos données patients prenez vous une ou plusieurs des précautions suivantes :			
➢ **Avez-vous pris des dispositions pour protéger vos sauvegardes du vol (ex : local ou meuble de bureau fermé a clef)**	☐	☐	☐
➢ **Conservez vous des copies de vos sauvegardes en dehors de votre cabinet (ex : à votre domicile)**	☐	☐	☐

D/ Les logiciels de protection

	oui	non	?
Avez-vous un antivirus ?	☐	☐	☐
Si oui, faites-vous la mise à jour régulière des bases de données antivirus ?	☐	☐	☐
Utilisez-vous :			
➢ un logiciel contre les spyware (espiogiciel) ?	☐	☐	☐
➢ un firewall (logiciel pare-feu) ?	☐	☐	☐
➢ un logiciel d'effacement sécurisé des données ?	☐	☐	☐

E/ Assistance informatique

	oui	non	?
Avez-vous souscrit une garantie lors de l'achat de votre matériel informatique ?	☐	☐	☐
Si oui, cette garantie vous propose-t-elle, des solutions de rechange en cas de défaillance de votre matériel ou de votre système informatique ?	☐	☐	

Avez-vous déjà fait appel à une assistance téléphonique pour :

☐votre matériel ☐votre logiciel de gestion des données patients

Si oui, avez-vous été satisfait par les réponses fournies ?	☐	☐
Avez-vous déjà fait appel à un technicien sur place ?	☐	☐
Si oui, a-t-il résolu votre problème ?	oui	non

Partie III : Votre expérience personnelle

A/ Perte de données patients informatisées

Avez-vous déjà perdu des données patients informatisées ? oui ☐ non ☐ ? ☐

Si oui, combien de fois ?

Quelle a été la quantité de données patients perdue « en jours » :

- **La première fois que vous avez perdu des données :**
- **La dernière fois que vous avez perdu des données :**

Exemple : si lors de la perte de vos données la dernière sauvegarde datait de 15 jours, on considère que la perte de données est de 15 jours.

B/ Accès non autorisé à vos données patients

Est-il déjà arrivé qu'un tiers (extérieur au cabinet médical) accède à vos données patient informatisées :

- **En utilisant votre mot de passe ?** oui ☐ non ☐ ? ☐
- **Par d'autres moyens ?** oui ☐ non ☐ ? ☐

C/ Perte de données d'origine criminelle

A-t-on déjà volé le disque dur de votre ordinateur ? oui ☐ non ☐ ? ☐

A-t-on déjà détruit le disque dur de votre ordinateur ? oui ☐ non ☐ ? ☐

A-t-on déjà détruit le support des sauvegardes de vos données patients ? oui ☐ non ☐ ? ☐

Avez-vous déjà été victime d'un virus informatique ? oui ☐ non ☐ ? ☐

D/ Perte de données d'origine accidentelle

Avez-vous déjà subi la destruction accidentelle du disque dur de votre ordinateur ? oui ☐ non ☐ ? ☐

Avez vous déjà perdu des sauvegardes contenant des données patients informatisées ? oui ☐ non ☐ ? ☐

Si oui, comment :

☐perte de la sauvegarde ☐perte du support
☐effacement de la sauvegarde ☐destruction du support ☐autre : ……..…

Avez-vous déjà été dans l'impossibilité de restaurer des données patients sauvegardées ? oui ☐ non ☐ ? ☐

E/ Vos impressions personnelles

Avant de vous équiper, avez-vous eu des réticences liées à la protection de vos données patients informatisées ? oui ☐ non ☐ ? ☐

Aujourd'hui, avez-vous confiance dans la protection de vos données patients informatisées ? oui ☐ non ☐ ? ☐

Pensez-vous que votre système informatique soit compatible avec le respect du secret médical ? oui ☐ non ☐ ? ☐

Lexique informatique

clé USB

Loc. f. périphérique] Dispositif de la taille d'une clé, se branchant sur un port USB et contenant généralement de la mémoire flash. On peut y stocker ses données personnelles et les emporter avec soi.

Espiogiciel (anglais: spyware)
n. m.
[Classe d'application] Contraction de « espion » et de « logiciel ».
Logiciel espion, qui vous surveille et transmet vos données sur le serveur de celui qui vous a fourni ce logiciel. Ils sont de plus en plus répandus.

Firewall
n. m.
[Police] Barrière permettant d'isoler un ordinateur d'un réseau. Pour éviter tout piratage. Versions françaises : coupe-feu, pare-feu.

xDSL

sg. m. [télécom][norme] x Digital Subscriber Line. x peut valoir A (ADSL), HS (HSDSL), RA (RADSL), S (SDSL), A (VHSDSL), I (IDSL)n ou rien du tout (DSL). Famille de techniques qui permettent de disposer de débits de plusieurs Mbit/s sur des lignes de téléphone normales.

1. INTRODUCTION

Depuis la fin des années 90, l'informatique s'est peu à peu imposée en médecine générale. En 2008, près de neuf médecins généralistes libéraux sur dix sont informatisés. La majorité d'entre eux conservent des données professionnelles sur un support numérique.

Cette informatisation a entraîné une modification des habitudes des médecins généralistes dans leur exercice quotidien. Ils ont progressivement fait la transition entre les dossiers papier et les dossiers informatisés. (1) (2) (3) (4)

Après plus de dix ans d'utilisation de l'informatique au cabinet, je souhaite faire un point sur la conservation et la protection des données médicales en médecine générale.

Les questions que je me suis posées avant d'entreprendre mon étude sont les suivantes :

- Quelles sont les obligations légales des médecins généralistes vis-à-vis des données concernant leurs patients (en particulier celles conservées sous forme numérique) ?
- Est ce qu'il existe un risque pour ces données (est ce que les médecins perdent des données informatisées) ?
- Et si oui quelles sont les mesures simples à prendre pour éviter ou limiter ses pertes ?

1.1. Recherche bibliographique

Les données en informatique (surtout en sécurité informatique) sont difficiles à recueillir. Compte tenu du caractère particulier de mon sujet de thèse, la recherche bibliographique sur les banques de données médicales telles que PUBMED ou le réseau SUDOC (système universitaire de documentation) s'est révélée peu informative. Je me suis appuyé sur plusieurs sources.

La partie traitant de la tenue du dossier patient par le médecin généraliste a été la plus simple à documenter. J'ai trouvé de nombreux articles du code de la santé publique traitant du sujet ainsi que la loi relative à l'informatique, aux fichiers et aux libertés.

Pour les données concernant l'informatisation en médecine générale, une recherche sur le site Internet de la BIUM (Bibliothèque Interuniversitaire de Médecine) m'a permis de

consulter plusieurs articles et thèses de confrères sur le sujet. Il existe par ailleurs des rapports gouvernementaux et certaines informations peuvent être consultées sur le site Internet de l'assurance maladie.

Le recueil de données relatives à la sécurité informatique m'a posé un problème. Je n'ai pas trouvé de sources de données scientifiquement recueillies comme on peut en trouver en médecine. En particulier parce que les entreprises ayant pour activité la sécurité en informatique ou la conservation des données ont tendance à ne pas partager leurs informations. Les ouvrages universitaires que j'ai pu trouver et qui traitent de la sécurité informatique se sont souvent révélés trop complexes et sans rapport avec ce qui est requis dans le cadre d'un cabinet de médecine générale. Je me suis donc appuyé sur d'autres sources : quelques ouvrages et plusieurs sites Internet spécialisés sur ce sujet, en particulier celui de la CNIL (Commission Nationale de l'Informatique et des Libertés), du CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques) et du CLUSIF (Club de la Sécurité de l'Information Français), ainsi que de recommandations issues de la norme ISO/IEC 17799 (Technologies de l'information – Techniques de sécurité – Code pratique pour la gestion de sécurité d'information).

1.2. Définition

J'ai limité mon champ d'étude à la conservation et à la protection des « données patients informatisées ». Cette expression comprend toutes les informations concernant les patients (cela peut être une simple liste de noms) conservées sous forme informatique par le médecin généraliste sur son ordinateur ou sur tout autre support numérique.

D'après la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *« Constitue une donnée à caractère personnel toute information relative à une personne physique*

identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.» (5)

1.3. L’informatisation en médecine générale

1.3.1 Quelques chiffres

L’entrée de la médecine de ville dans l’ère numérique a été considérablement accélérée par l’ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de santé, qui a facilité la généralisation rapide de l’usage des feuilles de soins électroniques.

Actuellement, près de 90% des médecins utilisent l’informatique au cabinet à des fins professionnelles. Plusieurs sources me permettent d’étayer les chiffres de l’informatisation en médecine libérale. D’après le site Internet de l’assurance maladie (6) et une étude de juin 2006 émanant du conseil de l’ordre de médecins (7), 52 058 Médecins généralistes télétransmettent (8) sur un total de 104 783 généralistes en activité mais dont seulement 56 784 exercent une activité libérale exclusive et 6 210 une activité libérale partielle (7).

Par ailleurs, d’après l’étude IPSOS de novembre 2007, 89% des médecins interrogés utilisent un équipement informatique sur leur lieu d’exercice pour un usage professionnel (9).

1.3.2 Atouts et failles de l’informatisation.

L’informatique a permis de réduire considérablement le volume de stockage des dossiers patients. La dématérialisation des données facilite leur accès ainsi que leur transfert par le biais des réseaux de l’information (comme Internet par exemple). Un autre avantage est une meilleure lisibilité des informations.

Physiquement, l’information prend donc moins de place. Elle est mieux accessible et se transmet plus facilement.

Malgré ces avantages, on peut se demander si les conditions sont réunies pour assurer l’intégrité des données médicales.

L'informatique génère ces propres problèmes. La technique et le matériel évoluent vite alors que l'exercice médical nécessite une conservation de données à long terme. Cette évolution implique une adaptation constante aux nouveaux formats de stockage de données, aux nouveaux matériels et logiciels. Au contraire, s'il laisse son système informatique devenir obsolète, le médecin sera confronté à des problèmes de compatibilité et d'interopérabilité et donc, par extension, à des pertes de données.

D'autre part, on a très peu de données fiables sur la durée de vie des différents supports informatiques. Souvent, celles-ci sont fournies par les constructeurs, ce qui laisse un doute sur leur objectivité. Et, elles laissent à penser que la durée de vie moyenne de ces supports ne dépasse pas une quinzaine d'années. (10)

Enfin, la simplification des échanges de données et la miniaturisation des supports exposent celles-ci à être partagées à des tiers non soumis au secret médical.

1.3.3 Les échanges de données.

La sécurité informatique est un sujet vaste, autant qu'une spécialité en médecine. J'ai donc réduit mon champ d'étude à la protection des données concernant les patients au cabinet du médecin généraliste. J'ai volontairement exclu l'échange de données par l'intermédiaire des réseaux de l'information, comme Internet par exemple. La raison est simple : il existe des systèmes de protection indépendants du médecin généraliste et qui sont gérés par des organismes habilités (c'est le cas du RSS [Réseau Santé Social] par exemple).

Cependant, vous pourrez constater qu'une partie de ma thèse porte sur certains logiciels de protection qui supposent une connexion Internet. Je considère que cela entre dans le cadre de ma thèse dans la mesure où il existe une menace portant sur la protection des données patients informatisées et que des mesures simples effectuées par le médecin libéral permettent d'y remédier.

1.4. Le dossier médical

1.4.1 Le cadre légal.

Dans le chapitre suivant sont regroupés les articles de lois qui me semblent pertinents pour définir le cadre légal du dossier médical informatisé en médecine libérale ainsi que les obligations du médecin généraliste pour la conservation des informations concernant ses patients.

1.4.1.1 Le secret médical.

Selon l'article 1 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (version consolidée au 24 janvier 2006) *« L'informatique doit être au service de chaque citoyen. (…). Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » (5)*

L'article L1110-4 du Code de la santé publique précise que *« Toute personne prise en charge par un professionnel (de santé) (…) a droit au respect de sa vie privée et du secret des informations la concernant. » (5)*

1.4.1.2 Le dossier médical en médecine générale.

La définition du dossier médical en médecine libérale est moins précise qu'en milieu hospitalier (11) (12), mais selon l'article 45 du code de la santé publique (article R.4127-45 du code de la santé publique), *« Indépendamment du dossier de suivi médical prévu par la loi, le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques. »* (5)

1.4.1.3 La protection et la conservation des données concernant les patients : une obligation légale quel que soit le support.

Plusieurs articles du code de déontologie et de la loi informatique et libertés soulignent l'obligation du médecin de protéger les données qui lui sont confiées par ses patients quel que soit le support sur lequel celles-ci sont conservés. (13) (14)

D'une manière générale l'article 34 de la Loi n°78-17 du 6 janvier 1978 (Loi relative à l'informatique, aux fichiers et aux libertés) explique que *« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.» (5) (14)*

Plus spécifiquement en médecine, l'article 45 du code de déontologie (article R.4127-45 du code de la santé publique) précise que *« dans tous les cas, ces documents sont conservés sous la responsabilité du médecin.» (13)*

Selon l'article 73 du code de déontologie (article R.4127-73 du code de la santé publique) *« le médecin doit protéger contre toute indiscrétion les documents médicaux concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents. » (7)*

1.4.1.4 La durée de conservation dans le cadre de l'exercice de la médecine libérale individuelle.

Les recommandations spécifiques émis par l'ANAES (concernant la tenue des dossiers médicaux en médecine générale) précisent : « Selon la règle

prescription trentenaire (maintenant décennale) un médecin est effectivement responsable d'un acte commis pendant au moins 30 ans (+ pour les mineurs). Il est donc fortement conseiller de conserver pendant cette période les dossiers médicaux (…). En cas d'informatisation des dossiers il parait souhaitable d'archiver les documents originaux essentiels afin d'être à même de les produire en cas de litige ». (15)

D'autre part, selon l'article 2262 du code civil, « Toutes les actions, tant réelles que personnelles, sont prescrites par trente ans, sans que celui qui allègue cette prescription soit obligé d'en rapporter un titre ou qu'on puisse lui opposer l'exception déduite de la mauvaise foi. » (5)

1.4.2 Interprétation des textes de loi.

Le médecin généraliste est donc tenu de rédiger une « fiche d'observation » qui est personnelle à chaque patient. Celui-ci est responsable du traitement et de la protection des données qui lui sont confiées quel que soit leur support, et leur mode de conservation et ceci pour une durée pouvant dépasser 30 ans.

1.5. La protection des données informatisées concernant les patients.

1.5.1 La sécurité informatique.

1.5.1.1 La notion de risque.

Le risque désigne un danger bien identifié, associé à l'occurrence d'un événement ou d'une série d'événements, parfaitement descriptibles, dont on ne sait pas s'ils se produiront mais dont on sait qu'ils sont susceptibles de se produire. (…) Savoir anticiper, traquer les débordements potentiels, mettre en place un système de surveillance et de collecte systématique des données pour déclencher les alertes dès que les événements bizarres se produisent. » (16)

1.5.1.2 Les enjeux de la sécurité informatique.

En informatique, le matériel devient obsolète et tombe en panne. De nouvelles mises à jour logicielles apparaissent sans cesse. Même sans craindre une action criminelle extérieure, un système informatique nécessite un entretien pour continuer à fonctionner. Les hôpitaux et les cliniques ont souvent un service qui assure la maintenance et l'entretien du parc informatique. Celui-ci doit fournir un service qui répond à des normes et une partie concernant la gestion des systèmes d'information est prévu dans l'accréditation des services hospitaliers. Au contraire, au cabinet et alors que les risques sont comparables, le médecin est responsable de la tenue des dossiers et de l'entretien de son système informatique. L'intérêt de ma thèse est de savoir si les médecins généralistes installés en ville assurent cet entretien et d'autre part si leurs mesures sont efficaces. Et si non, de leur proposer une liste de mesures simples à mettre en œuvre (ou à vérifier, si ils font appel à un prestataire) pour assurer la conservation et la protection des données concernant leurs patients.

1.5.1.3 Les normes.

Il n'existe pas de norme à respecter pour la sécurité informatique en médecine libérale. Lors de l'élaboration de ma thèse, je me suis basé sur la norme ISO/IEC 17799 (technologies de l'information – techniques de sécurité – code de pratique pour la gestion de sécurité d'information) qui est la norme communément utilisée en matière de sécurité informatique. (17)

1.5.2 La protection des données médicales.

1.5.2.1 La sensibilité des données médicales.

La sécurité des données nominatives est une obligation imposée par la loi informatique fichiers et liberté du 6 janvier 1978 à tout détenteur d'un traitement informatisé d'informations nominatives.

Le professionnel de santé doit donc mettre en œuvre une véritable politique de sécurité des données permettant d'assurer :

1. la confidentialité des informations, au moyen de mots de passe. La commission nationale de l'informatique et des libertés (CNIL) recommande un mot de passe d'au moins huit caractères connus du seul praticien.
2. l'intégrité, en disposant d'un système de protection antivirus ainsi que d'un dispositif « coupe feu » (firewall) surtout si le système utilise une connexion vers d'autres systèmes (internet, réseau local, wifi…)
3. la fiabilité de l'exploitation en signant un contrat de maintenance.
4. la lutte contre les conséquences financières liées à la perte d'information, en souscrivant un contrat d'assurance spécifique à l'informatique. (18)

La loi informatique fichiers et liberté du 6 janvier 1978 protège les libertés individuelles en réglementant les fichiers et en mettant en place un statut des données nominatives.

« Les médecins généralistes ou spécialistes sont aussi bien concernés par ces obligations que les centres hospitaliers, les pharmaciens ou les laboratoires d'analyse médicale. (14) »

La loi recouvre les traitements automatisés d'informations nominatives, c'est-à-dire « tout ensemble d'opérations réalisées par des moyens

automatiques relatif, à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que de tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou de bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives. (14) »

Les informations à caractère nominatif sont définies comme « … les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ». Le caractère nominatif des informations est d'interprétation large et concerne toutes les données qui permettent d'établir un lien avec la personne physique concernée. (14)

La collecte des données nominatives est libre dès lors qu'elle fait l'objet d'une déclaration préalable à la CNIL et ne porte pas sur des données dites sensibles (race, opinion, mœurs). (14)

La loi du 6 août 2004 renforce la protection des données à caractère personnel. La collecte des informations relatives à la santé relève maintenant du régime de protection renforcé applicable aux données dites « sensibles » pour se conformer à la directive européenne du 24 octobre 1995. (5)

1.5.2.2 Les différents risques au cabinet du médecin généraliste.

Différents facteurs interviennent dans la protection des données informatises.

- le facteur humain.

Comme souvent le facteur le plus aléatoire reste le facteur humain. A mon sens, cette partie peut se diviser en deux sous parties.

a) le médecin généraliste.

Une citation bien connue dans le milieu informatique affirme que « le plus gros bug est celui qui se trouve entre la chaise et l'ordinateur » (Problem Exists Between Keyboard And Chair) (16)! Celui-ci peut être à l'origine d'une perte de données à la suite d'une erreur de manipulation.

b) la malveillance.

Je citerai comme exemples le vandalisme, le vol de matériel ou encore les attaques virales informatiques.

- le facteur matériel.

Les données ne sont pas protégées par les habitudes. Le matériel peut tomber en panne et nécessite des mises à jour régulières. Un système informatique nécessite d'être entretenu pour continuer à remplir son rôle.

Le facteur matériel peut se diviser en plusieurs sous parties.

a) le matériel proprement dit dans son environnement physique, qui inclut les différents supports de sauvegarde des données.
b) les applications qui gèrent les données médicales.
c) les données médicales proprement dites.

1.6. Problématique

La question posée et à laquelle je tente de répondre est la suivante : est ce que le médecin généraliste assure les mesures minimum nécessaires à la protection des données médicales qui lui sont confiées et qu'il conserve sur un support informatique?

Parallèlement à cette question et pour la mettre en valeur, je cherche à savoir si les médecins généralistes perdent des données informatisées et si oui, quelle est la proportion de perte d'origine criminelle et accidentelle ?

2. MATERIEL ET METHODE

Pour répondre à cette question, j'ai réalisé une étude transversale en adressant un questionnaire à 280 médecins généralistes libéraux du département du Val d'Oise entre septembre et décembre 2007.

2.1. Critère d'exclusion

Mon seul critère d'exclusion m'a conduit à ne pas prendre en compte les médecins non informatisés ou informatisés mais n'ayant pas de données patients sur leur ordinateur.

J'ai choisis 370 médecins de manière aléatoire parmi les 902 références retrouvées sur le site www.Pages-jaunes.fr en effectuant une recherche avec les mots clefs « médecin généraliste » et « Val d'Oise ». J'ai téléphoné à chaque cabinet de médecine générale pour m'assurer que le ou les médecins du cabinet remplissaient ses critères avant d'envoyer le questionnaire. 280 médecins généralistes libéraux (75% des médecins interrogés par téléphone) correspondaient aux critères de l'étude.

2.2. La liste de médecins

Le questionnaire de l'étude a donc été adressé à 280 médecins généralistes libéraux du Val d'Oise (250 par voie postale et 30 par courriel) entre septembre et décembre 2007.

2.3. Le questionnaire

Le questionnaire comprend 71 questions réparties en trois chapitres.

Le premier chapitre tente de faire un point sur l'informatisation en 2007 parmi les médecins sondés avec une première partie comprenant des questions d'épidémiologie et une seconde partie définissant le matériel utilisé ainsi que son degré d'utilisation. Ces « items » me permettent de suivre l'évolution du « parc informatique » des médecins généralistes.

Le deuxième chapitre aborde de manière générale les connaissances des médecins interrogés sur « la protection des données patients informatisées ». Il se divise en plusieurs parties : « les modalités d'accès au données de vos patients », « les sauvegardes de vos données patients », « la protection physique » du ou des supports contenant ces données, « les logiciels de protection », « l'assistance informatique » pour les médecins ayant souscrit à une offre comprenant le logiciel et une assistance.

Le troisième chapitre aborde « l'expérience personnelle » de chaque médecin en posant des questions sur « la perte de données patients informatisées », « l'accès non autorisé à vos données patients », « la perte de données d'origine criminelle », « la perte de données d'origine accidentelle » et pour finir recueille les « impressions personnelles » de chacun sur la protection de ses données.

2.4. La lettre accompagnant le questionnaire

Chaque questionnaire est envoyé avec une lettre expliquant l'objectif de l'étude ainsi qu'une enveloppe pré timbrée pour ré adresser le questionnaire. La lettre et le questionnaire sont reproduits en page 7 à 12.

2.5. Le taux de réponses

Le questionnaire était initialement fait pour être envoyé sous forme courriel afin d'être rempli, sauvegardé et renvoyé par ce moyen. Mais devant le nombre de médecins de bonne volonté n'ayant pu me renvoyer de questionnaire exploitable par Internet j'ai préféré par la suite l'envoyer que par voie postale.

Sur les 30 questionnaires envoyés par courriel, 10 m'ont été ré adressés remplis, mais seuls 6 étaient exploitables. Soit un taux de réponse de 33% et un taux de réponse exploitable de 20%

Sur les 250 questionnaires envoyés sous forme papier, 144 m'ont été ré adressés et tous étaient exploitables. Soit un taux de réponses exploitables de 57%.

Cela me fait un total de 149 questionnaires et un taux de réponses exploitables global de 54%.

3. RESULTATS DE L'ETUDE.

Abbréviations

NR Non réponses
na Données manquantes

3.1. Démographie et matériel informatique des médecins interrogés.

3.1.1 Le sexe et l'âge.

Les données recueillies sur le sexe et l'âge des médecins ayant répondu au questionnaire sont regroupées sur les tableaux 1-2-3 et les figures 1-2. On constate une prédominance de médecins hommes (74%) et une proportion plus élevée des médecins ayant un âge compris entre 50 et 54 ans. L'âge médian des médecins interrogés est de 51 ans.

	Effectif (na = 2)	Proportion
Femme	38	0.259
Homme	109	0.741

TAB. 1 – Sexe

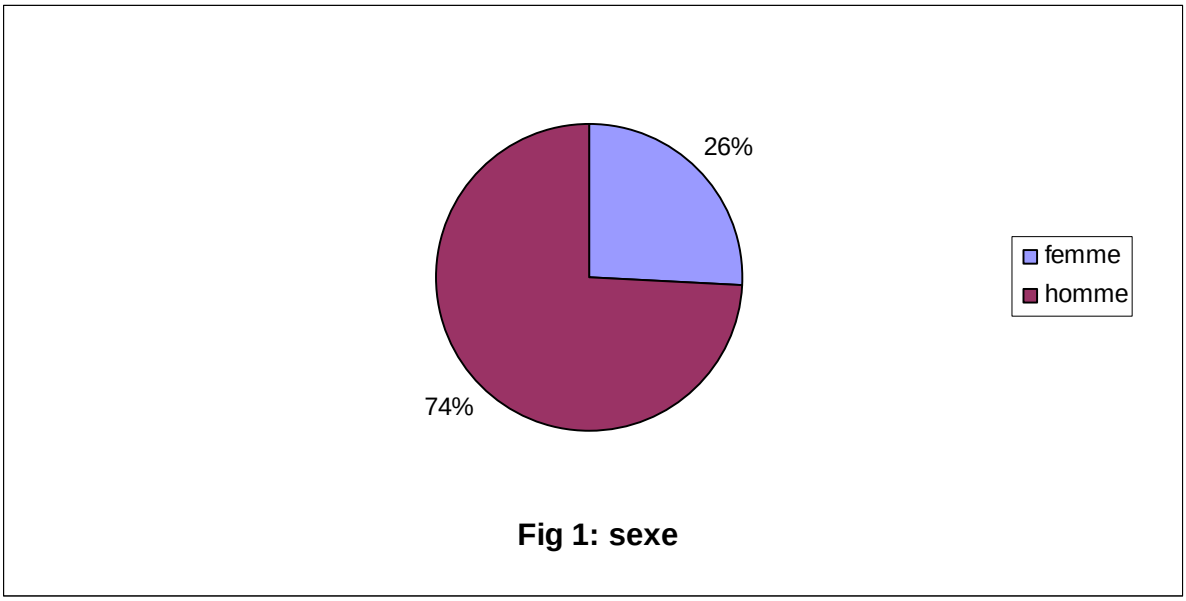


Fig 1: sexe

	Moyenne	Mediane	Ecart-type	Min	Max	NA
Age	50.77	51	7.95	31	66	28

TAB. 2 – Age

	Femme	Femme (%)	Homme	Homme (%)	na
Age < 30	0		0		28
30 <= Age < 35	3	0.600	2	0.400	
35 <= Age < 40	3	0.250	9	0.750	
40 <= Age < 45	3	0.375	5	0.625	
45 <= Age < 50	9	0.375	15	0.625	
50 <= Age < 55	8	0.250	24	0.750	
55 <= Age < 60	5	0.185	22	0.815	
Age >= 60	2	0.154	11	0.846	

TAB. 3 – Age par sexe

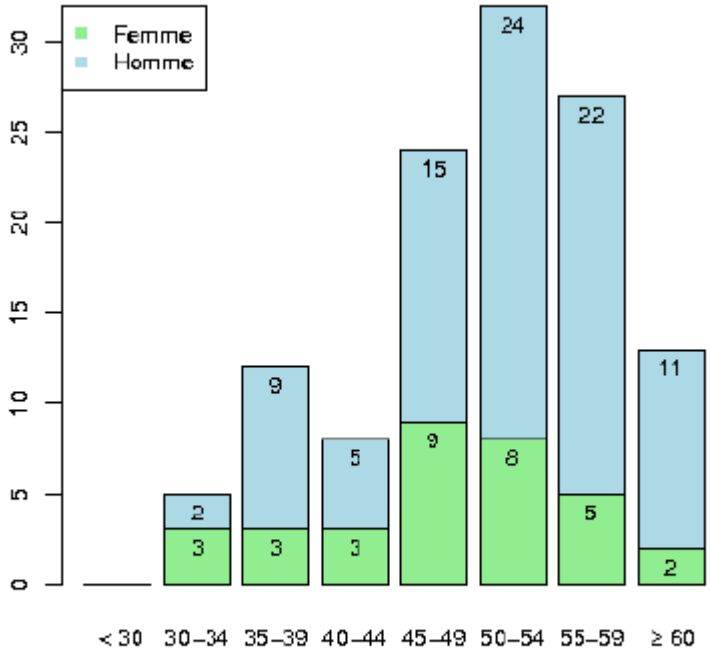


FIG. 2 – Pyramide des âges

3.1.2 L'année d'installation.

J'ai regroupé les années d'installation des médecins interrogés par décennies. On remarque un pic d'installation des médecins généralistes entre 1980 et 1989 qui correspondent à 47% des médecins interrogés.

	Effectif (na = 2)	Proportion
1970-1979	24	0.163
1980-1989	69	0.469
1990-1999	32	0.218
2000-2007	22	0.150

TAB. 4 – Année d'installation

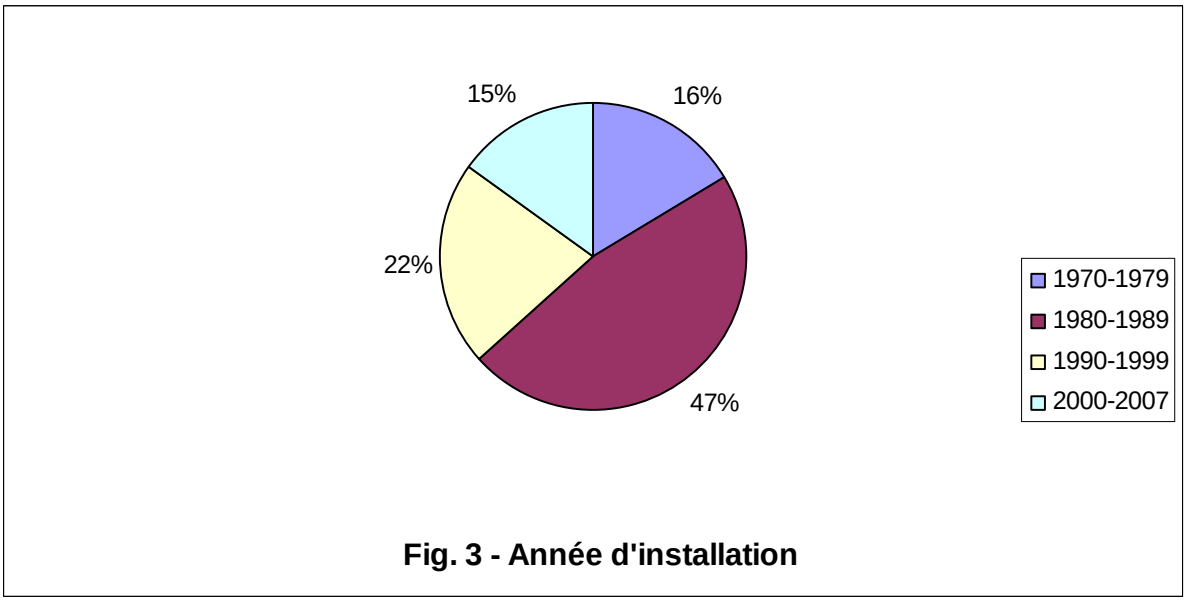


Fig. 3 - Année d'installation

3.1.3 L'année d'informatisation.

57% des médecins ayant répondu à cette question ont informatisé leur cabinet dans la deuxième moitié des années 90.

	Effectif (na = 73)	Proportion
1990-1994	16	0.211
1995-1999	43	0.566
2000-2004	14	0.184
2005-2007	3	0.039

TAB. 5 – Année d'informatisation

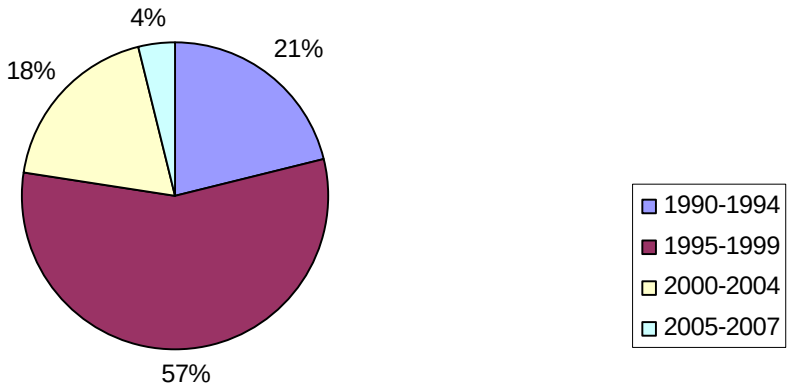


Fig. 4 - Année d'informatisation

3.1.4 Le type d'exercice.

66% des médecins interrogés exercent en groupe.

	Effectif (na = 1)	Proportion
Oui	97	0.655
Non	51	0.345

TAB 6 – Travaille en groupe

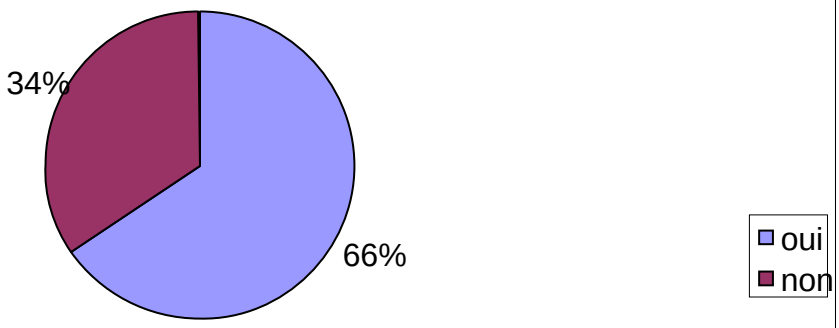


Fig. 5 - Organisation en cabinet de groupe

3.2. Le matériel utilisé.

3.2.1 Le type d'ordinateur.

La plus grande partie (83%) des ordinateurs utilisés dans les cabinets de médecins généralistes sont des« ordinateurs fixes » (ou « de bureau ») par opposition aux ordinateurs portables. Il s'agit à 89% de Personal Computer (PC) et à 10% de Macintosh

	Effectif (na = 10)	Proportion
Fixe	116	0.835
Portable	12	0.086
Les deux	11	0.079

TAB 7 – Type d'ordinateur

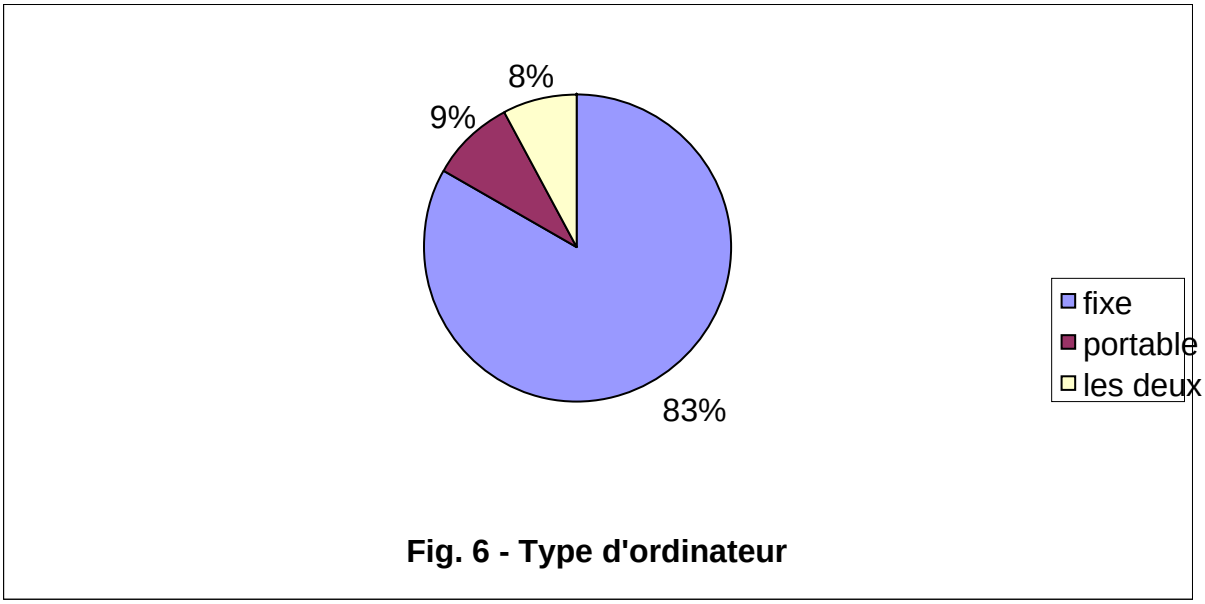


Fig. 6 - Type d'ordinateur

	Effectif (na = 27)	Proportion
PC	109	0.893
Mac	12	0.098
Les deux	1	0.008

TAB 8 – PC ou Mac

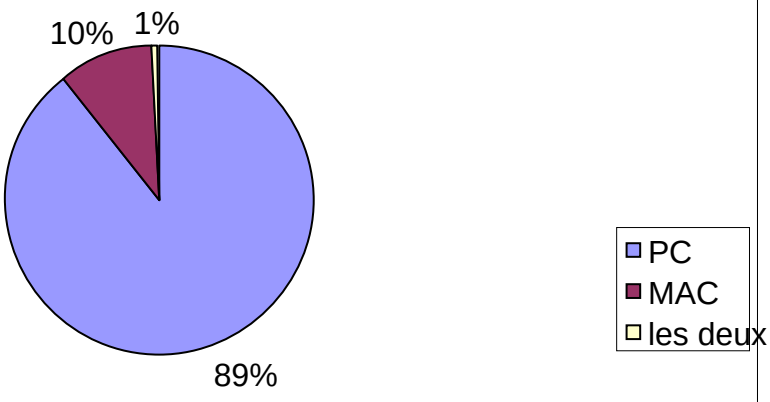


Fig. 7 - PC ou Mac

3.2.2 Les périphériques.

Ces questions reflètent l'équipement des médecins informatisés. L'ensemble des réponses est regroupé dans la figure 8.

	Effectif	Proportion	NA
Ecran plat	122	0.830	2
Scanner	69	0.469	2
Imprimante	133	0.905	2
PDA	19	0.129	2
Clef USB	90	0.612	2
Graveur DVD	49	0.333	2
Graveur CD	55	0.374	2
Onduleur	51	0.347	2

TAB 9 – Equipement

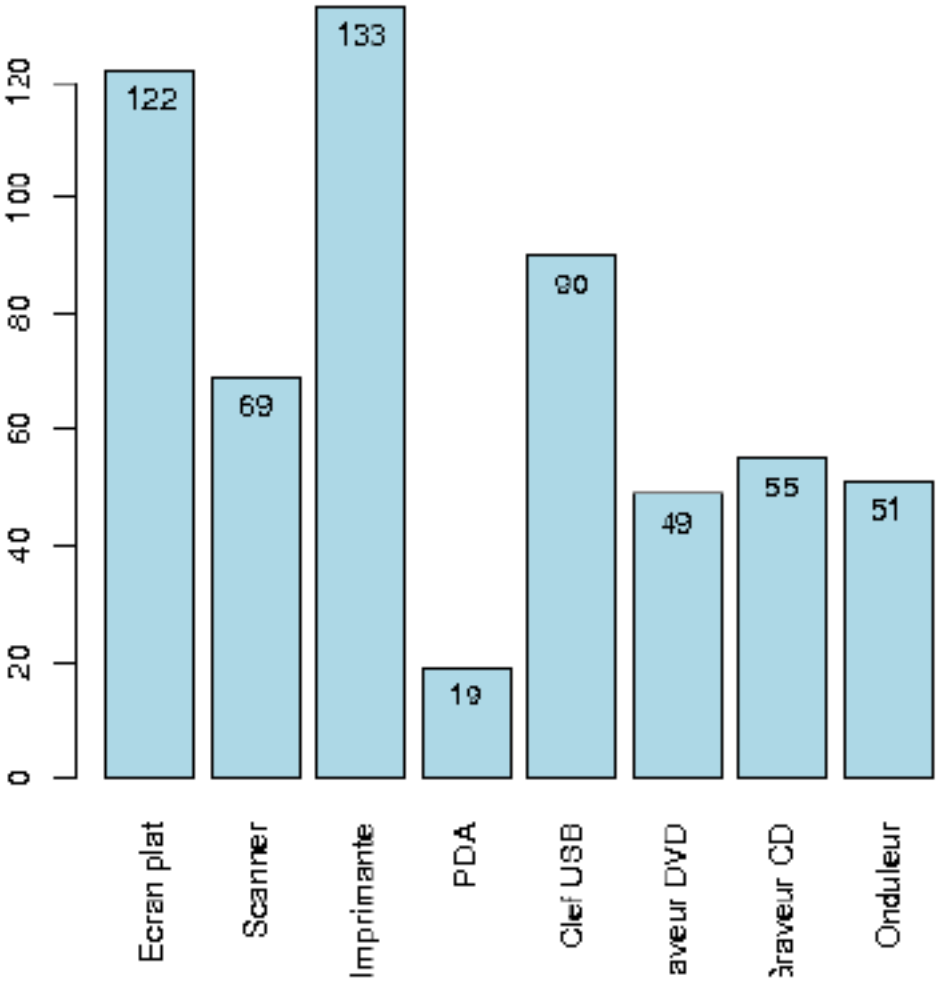


FIG 8 – Equipement

3.2.3 Le renouvellement du matériel informatique.

Plus de 50% des médecins interrogés ont un matériel informatique renouvelé il y a moins de 2 ans.

	Effectif (na = 5)	Proportion
Moins de 1 an	31	0.215
Entre 1 et 2 ans	45	0.312
Entre 2 et 5 ans	57	0.396
Plus de 5 ans	11	0.076

TAB 10 – Renouvellement du matériel informatique

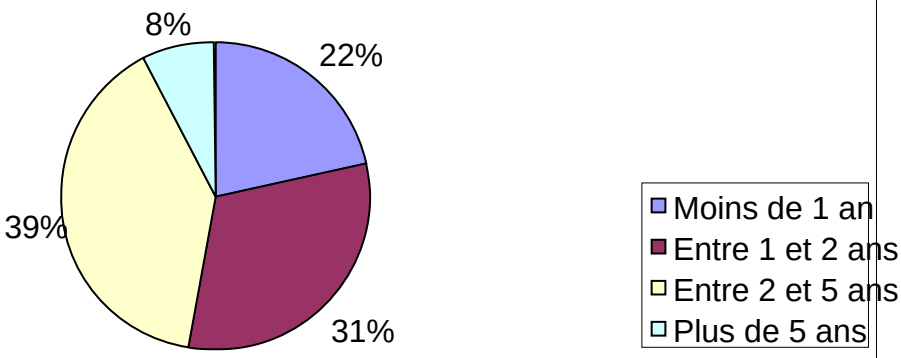


Fig. 9 - Renouvellement du matériel informatique

3.2.4 La connexion internet.

91% des médecins interrogés ont une connexion Internet dédiée à leur usage professionnel. Parmi ces médecins, 64% ont une connexion haut débit et 34% une connexion bas débit.

La connexion câble est souvent haut débit, mais apparaît négligeable en quantité dans l'étude.

	Effectif (na = 0)	Proportion
Oui	135	0.906
Non	14	0.094

TAB 11 – Connexion Internet

	Effectif (na = 14)	Proportion
ADSL	86	0.637
Modem	46	0.341
Cable	3	0.022

TAB 12 – Type de connexion

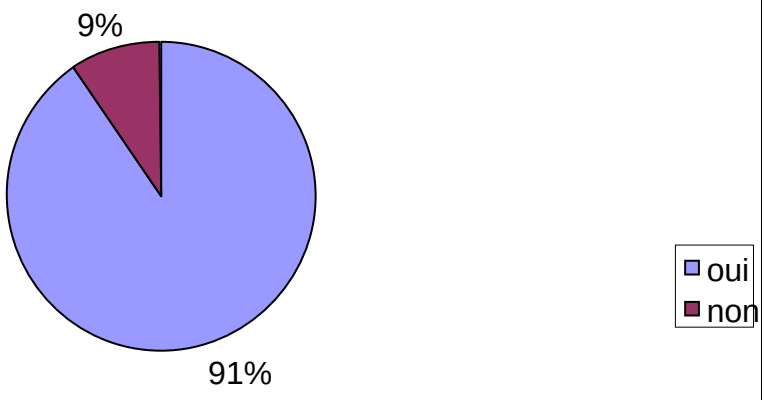


Fig. 10 - Connexion Internet

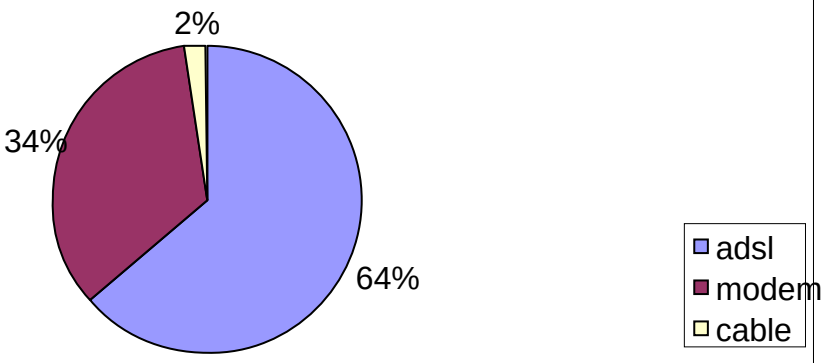


Fig. 11 -Type de connexion Internet

3.3. Utilisation du matériel informatique.

3.3.1 La gestion des données patients.

93% des médecins ayant répondu au questionnaire utilisent un logiciel pour gérer les données concernant leurs patients.

	Effectif (na = 1)	Proportion
Oui	137	0.926
Non	11	0.074

TAB 13 – Utilisez-vous un logiciel de gestion de données patients ?

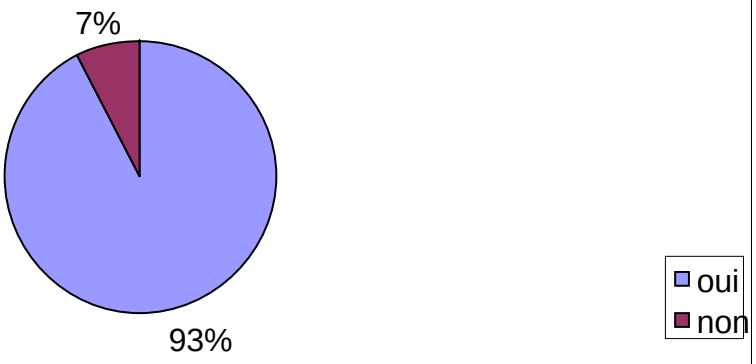


Fig. 12 - Utilisez vous un logiciel de gestion des données patient ?

3.3.2 Utilisation de l'ordinateur au cabinet du médecin généraliste.

- ✓ 97% font de la télétransmission de Feuilles de Soin Electroniques.
- ✓ 82% utilisent une assistance informatique pour rédiger les ordonnances.
- ✓ 82% utilisent une assistance informatique pour rédiger les demandes d'examens complémentaires.
- ✓ 74% utilisent une assistance informatique pour rédiger les certificats
- ✓ 67% utilisent un courriel professionnel.
- ✓ 62% utilisent un aide mémoire informatique pour le suivi des patients.
- ✓ 61% font leur comptabilité sur informatique.
- ✓ 60% archivent les résultats des examens complémentaires sous format informatique.
- ✓ 43% utilisent une aide informatique pour la prescription.
- ✓ 31% utilisent leur ordinateur comme outils didactique pour leurs patients.

- ✓ 28% des médecins interrogés planifient leurs rendez au moyen de leur ordinateur.

- ✓ 11% utilisent une assistance informatique au diagnostic.

L'ensemble de ces informations est regroupé dans la figure 13.

	Effectif	Proportion	NA
A : Plannification RDV	41	0.275	0
B : Email pro	100	0.671	0
C : Télétransmission FS	142	0.966	2
D : Archivage EC	89	0.605	2
E : Comptabilité	91	0.611	0
F : Outil didactique	45	0.306	2
G : Assistance au diagnostic	16	0.107	0
H : Assistance pour les prescriptions	64	0.432	1
I : Rédaction des ordonnances	122	0.819	0
J : Rédactions des demandes d'EC	122	0.819	0
K : Rédaction des certificats	110	0.738	0
L : Aide mémoire	92	0.617	0

TAB 14 – Utilisation de l'ordinateur

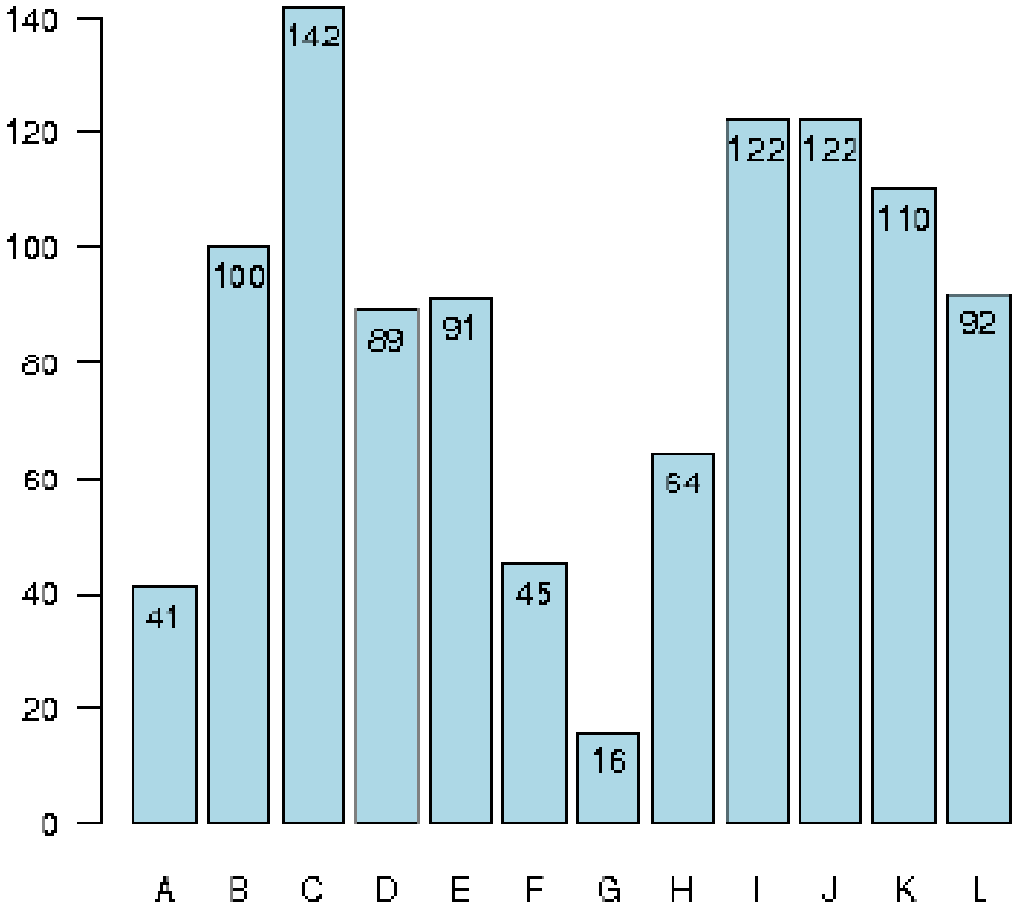


FIG 13 – Utilisation de l'ordinateur

3.3.3 Le Vidal.

56% des médecins ayant répondu au questionnaire utilisent le Vidal sur support informatique.

	Effectif (na = 7)	Proportion
Vidal papier	40	0.282
Vidal CD	44	0.310
Les deux	52	0.366
Aucun	6	0.042

TAB 15 – Le Vidal

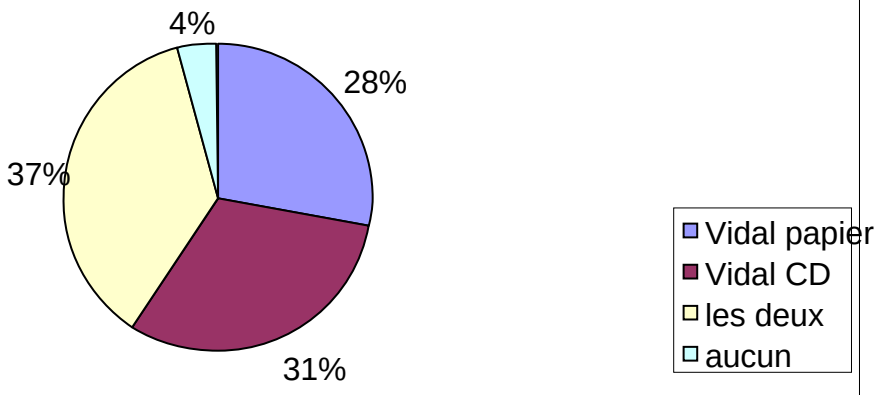


Fig. 14 - Le Vidal

3.3.4 Les dossiers papiers.

Malgré l'informatisation, 65% des ces médecins conservent des dossiers papiers. Sur les 94 médecins ayant répondu oui à la question, 83 ont précisé pour quel type de données. Ces informations sont regroupées dans la figure 14. Dans une majorité de cas la persistance des dossiers sur support papier concerne l'archivage des examens complémentaires.

	Effectif (na = 4)	Proportion
Oui	94	0.648
Non	51	0.352

TAB 16 – Les dossiers papier

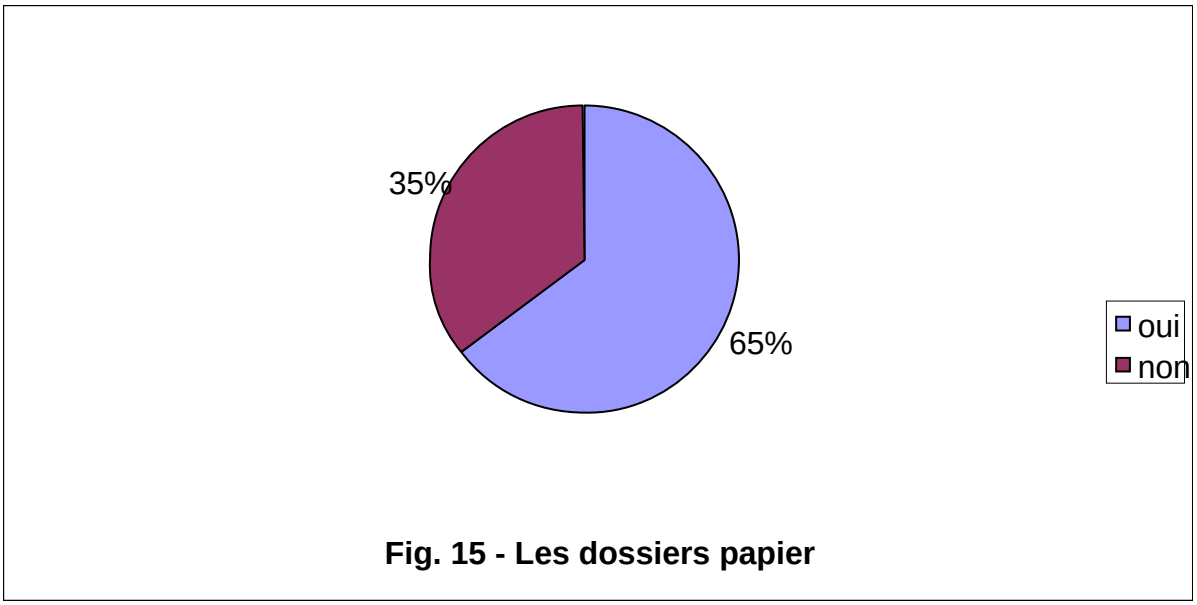
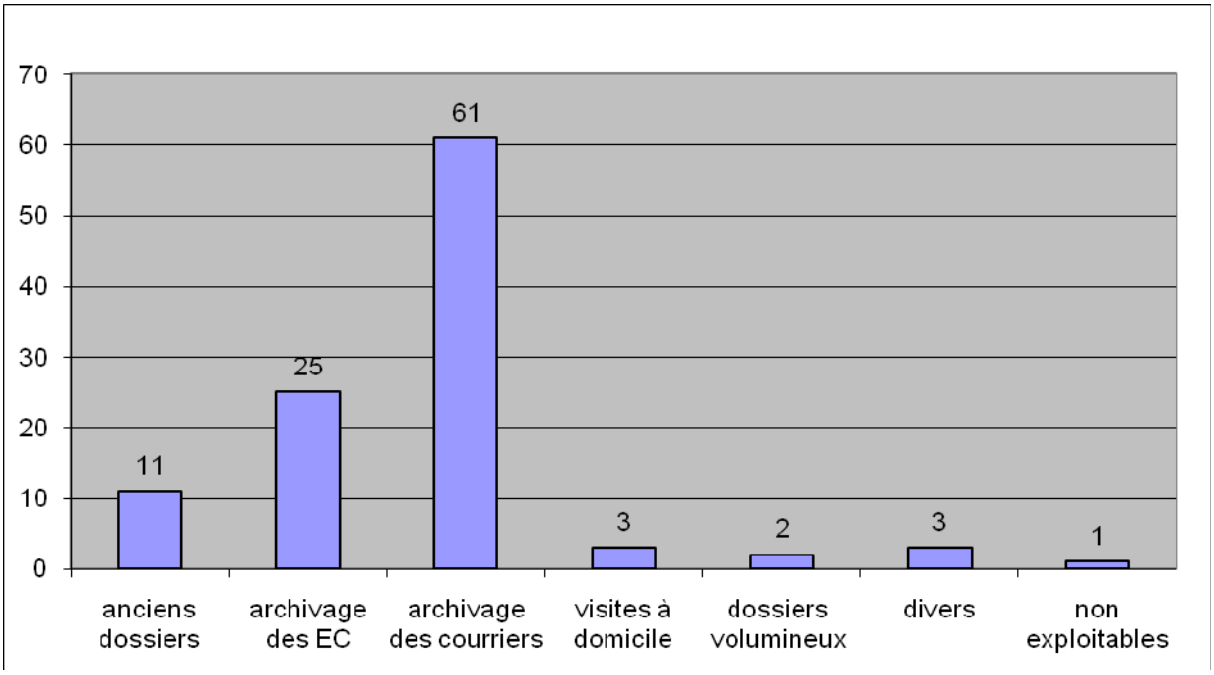


Fig. 15 - Les dossiers papier



3.4. L'organisation en cabinet de groupe.

Parmi les médecins interrogés 65% exercent en cabinet de groupe. Parmi ces 97 médecins, 53% partagent les données patients avec leurs confrères du cabinet. Ils disposent dans 14% des cas d'un mot de passe commun et dans 67% des cas d'un mot de passe personnel. 71% utilisent le même logiciel pour tout le groupe médical.

	Effectif (na = 1)	Proportion
Oui	97	0.655
Non	51	0.345

TAB 17 – Travaille en groupe

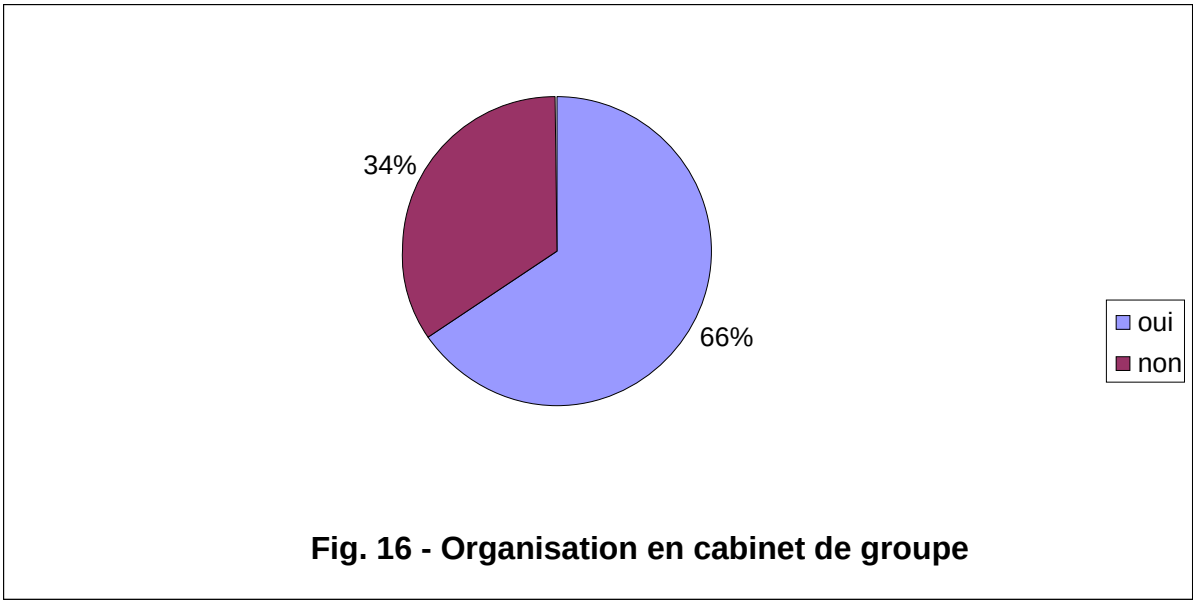


Fig. 16 - Organisation en cabinet de groupe

	Effectif (na = 3)	Proportion
Oui	53	0.564
Non	41	0.436
NSP	0	0.000

TAB 18 – Ordinateurs en réseau

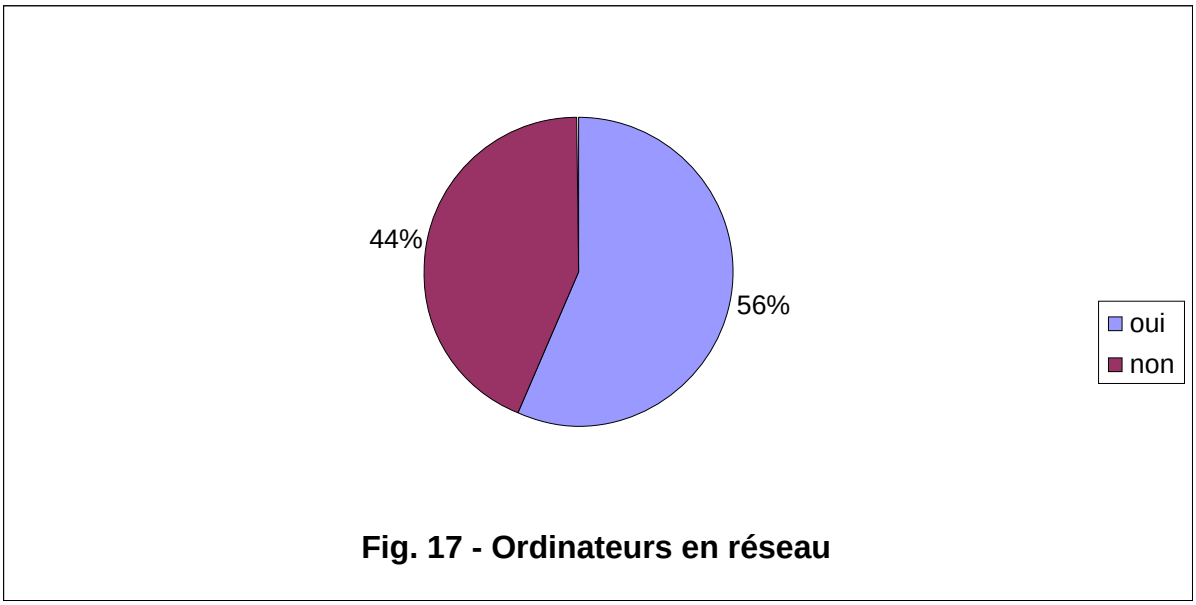


Fig. 17 - Ordinateurs en réseau

	Effectif (na = 3)	Proportion
Oui	50	0.532
Non	44	0.468
NSP	0	0.000

TAB 19 – Partage des données

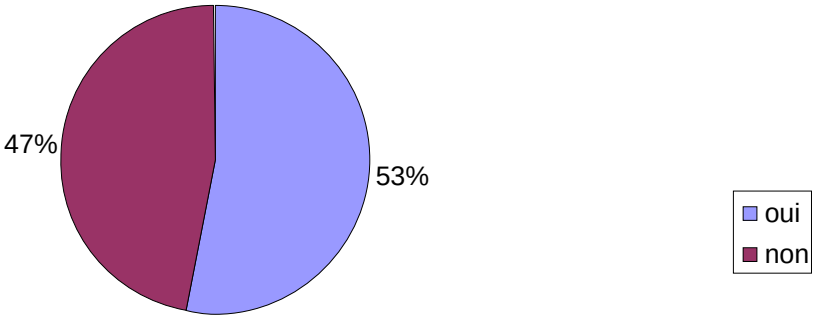


Fig. 18 - Partage des données

	Effectif (na = 5)	Proportion
Oui	13	0.141
Non	77	0.837
NSP	2	0.022

TAB 20 – Mot de passe commun

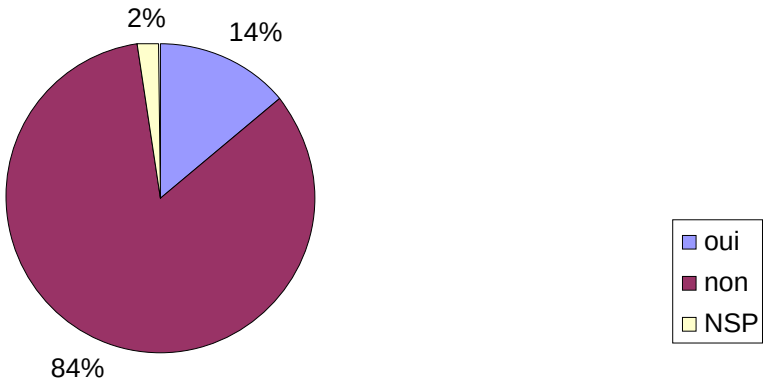


Fig. 19 - Mot de passe commun

	Effectif (na = 4)	Proportion
Oui	62	0.667
Non	24	0.258
NSP	7	0.075

TAB 21 – Mot de passe personnel

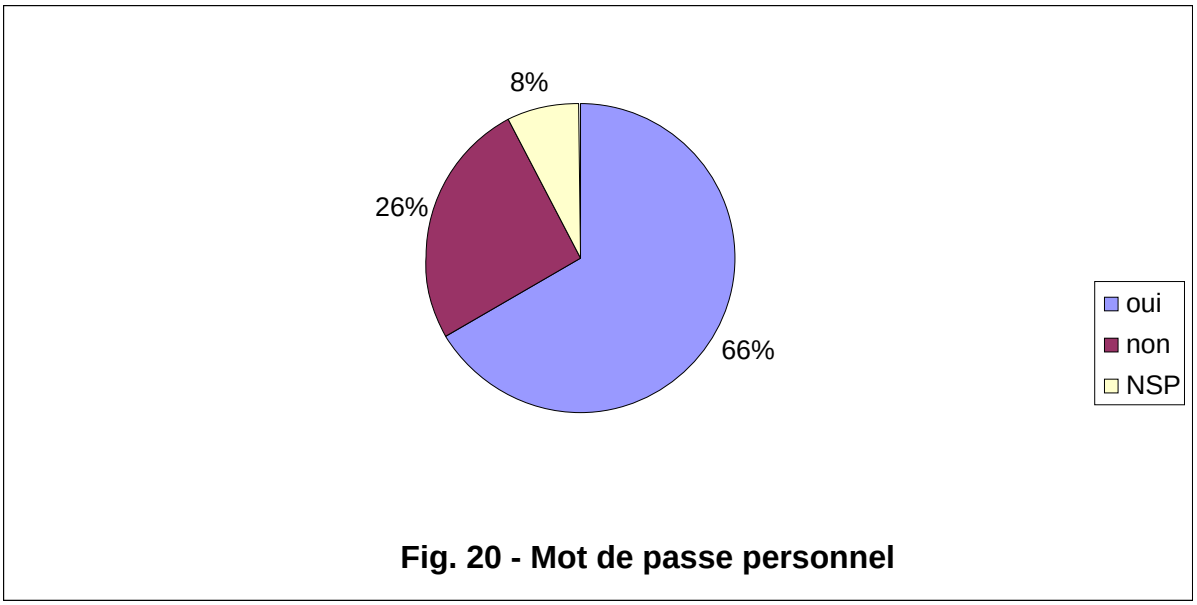


Fig. 20 - Mot de passe personnel

	Effectif (na = 4)	Proportion
Oui	66	0.710
Non	27	0.290
NSP	0	0.000

TAB 22 – Même logiciel de gestion des données patient

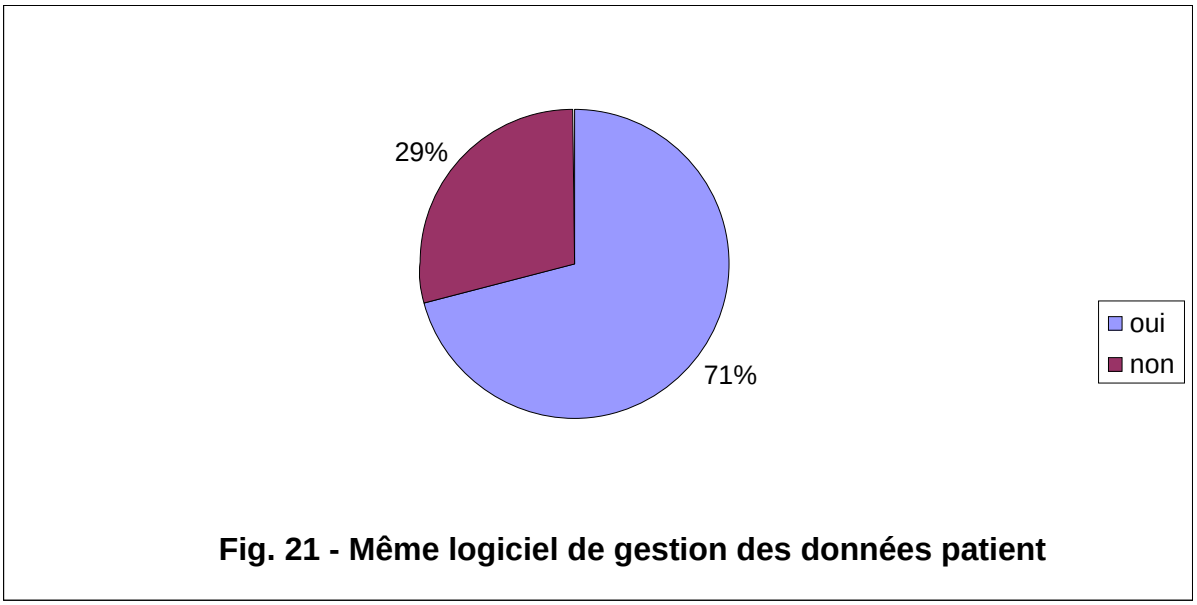


Fig. 21 - Même logiciel de gestion des données patient

3.5. Protection des données patients informatisées.

3.5.1 Les mots de passe pour accéder aux données patients.

Parmi les médecins ayant répondu au questionnaire :

- 91% ne notent pas leurs mots de passe pour pouvoir s'en rappeler.

- 79% ont un mot de passe pour accéder au logiciel de gestion des données patients.
- 75% utilisent un écran de mise en veille mais parmi eux seuls 19% nécessitent de taper le mot de passe pour réactiver leur session.
- 72% n'utilisent pas de mot de passe en rapport avec des données personnelles.
- 66% ont un mot de passe pour accéder à leur ordinateur.
- 46% utilisent différents mots de passe en fonction des applications.
- 46% utilisent un ou des mots de passe alphanumériques.
- 16% utilisent un ou des mots de passe de plus de 8 caractères.
- 4% modifient leurs mots de passe 2 fois par an ou plus.

	Effectif (na = 4)	Proportion
Oui	114	0.786
Non	31	0.214

TAB 23 – Mot de passe pour accéder au logiciel de gestion

	Effectif (na = 8)	Proportion
Oui	54	0.458
Non	64	0.542

TAB 24 – Mot de passe alphanumérique

	Effectif (na = 5)	Proportion
Oui	19	0.157
Non	100	0.826
NSP	2	0.017

TAB 25 – Mot de passe à plus de 8 caractères

	Effectif (na = 22)	Proportion
Jamais	122	0.961
Chaque mois	1	0.008
Tous les 3 mois	3	0.024
Tous les 6 mois	1	0.008

TAB 26 – Fréquence de modification de mot de passe

	Effectif (na = 21)	Proportion
Oui	59	0.461
Non	61	0.477
NSP	8	0.062

TAB 27 – Même mot de passe pour toutes les applications

	Effectif (na = 23)	Proportion
Oui	32	0.254
Non	91	0.722
NSP	3	0.024

TAB 28 – Mot de passe en rapport avec des données personnelles

	Effectif (na = 22)	Proportion
Oui	9	0.071
Non	115	0.906
NSP	3	0.024

TAB 29 – Notation des mots de passe pour pouvoir s'en rappeler

	Effectif (na = 4)	Proportion
Oui	109	0.752
Non	35	0.241
NSP	1	0.007

TAB 30 – Ordinateur en veille

	Effectif (na = 3)	Proportion
Oui	20	0.189
Non	83	0.783
NSP	3	0.028

TAB 31 – Mot de passe après la mise en veille

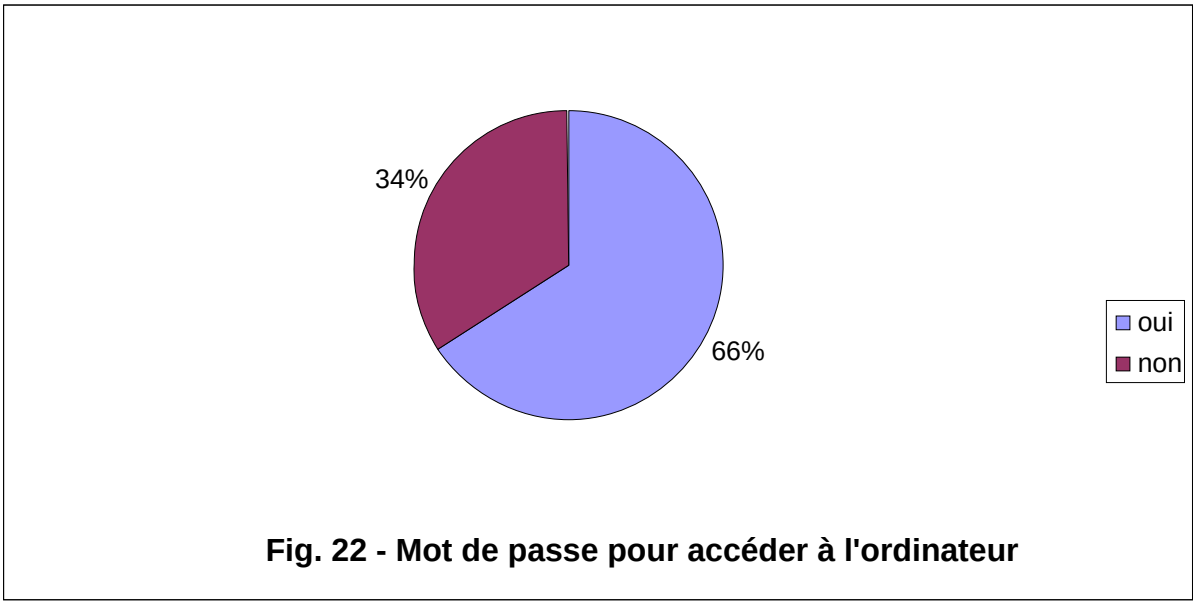


Fig. 22 - Mot de passe pour accéder à l'ordinateur

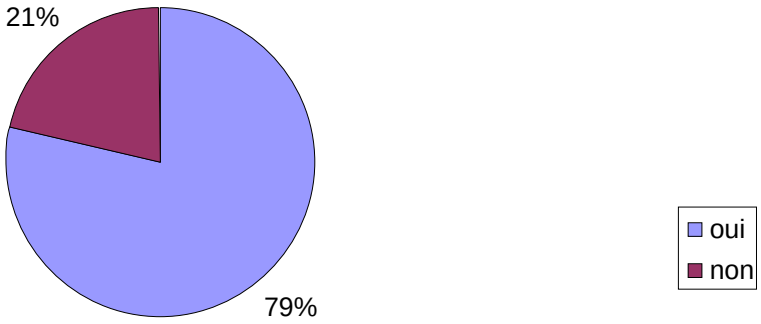


Fig. 23 - Mot de passe pour accéder au logiciel de gestion

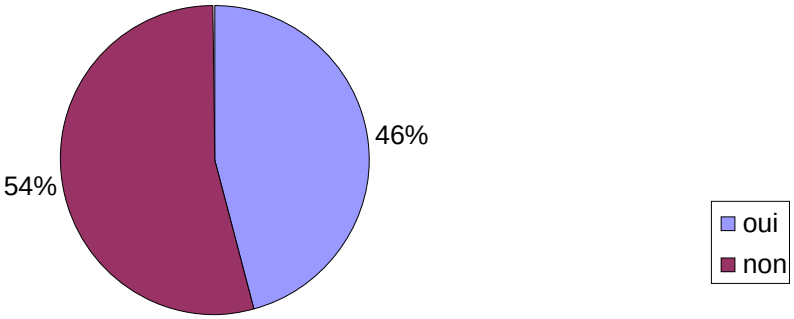


Fig. 24 - Mot de passe alphanumérique

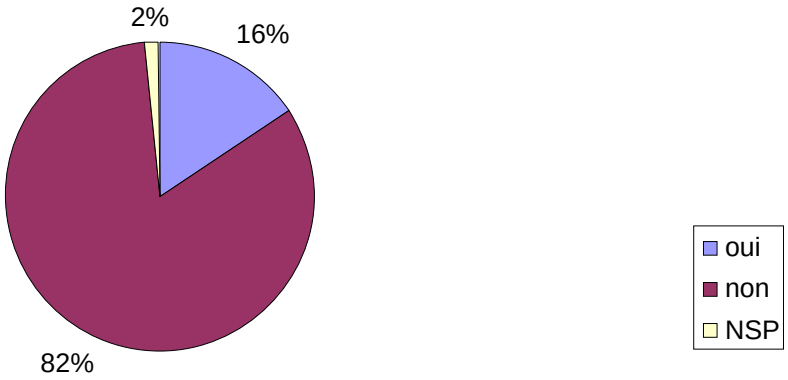


Fig. 25 - Mot de passe à plus de 8 caractères

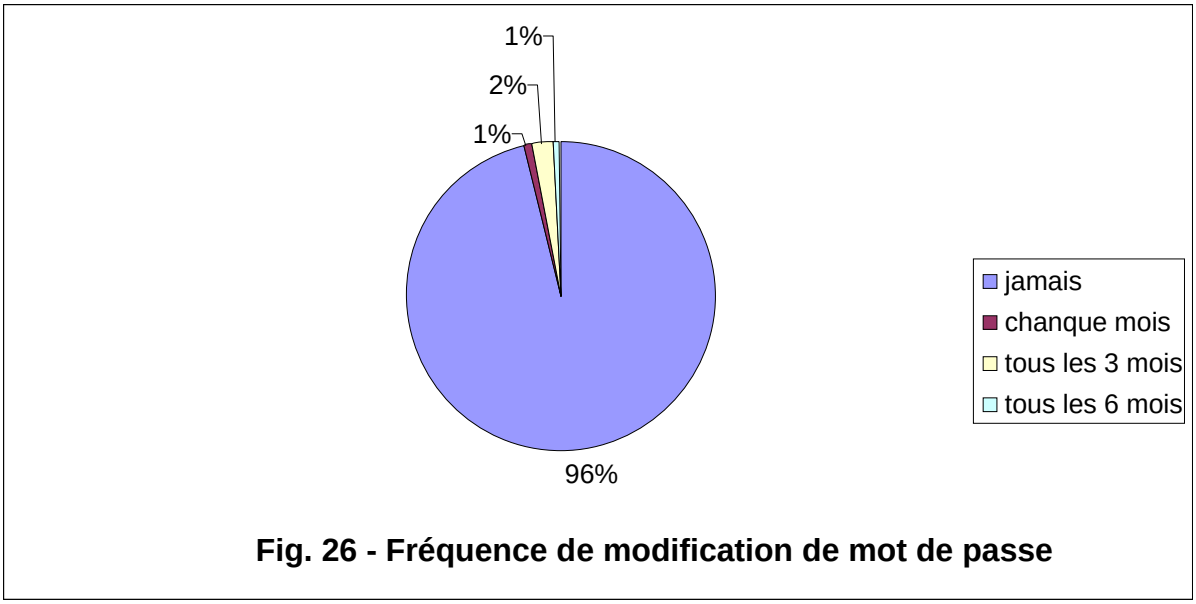


Fig. 26 - Fréquence de modification de mot de passe

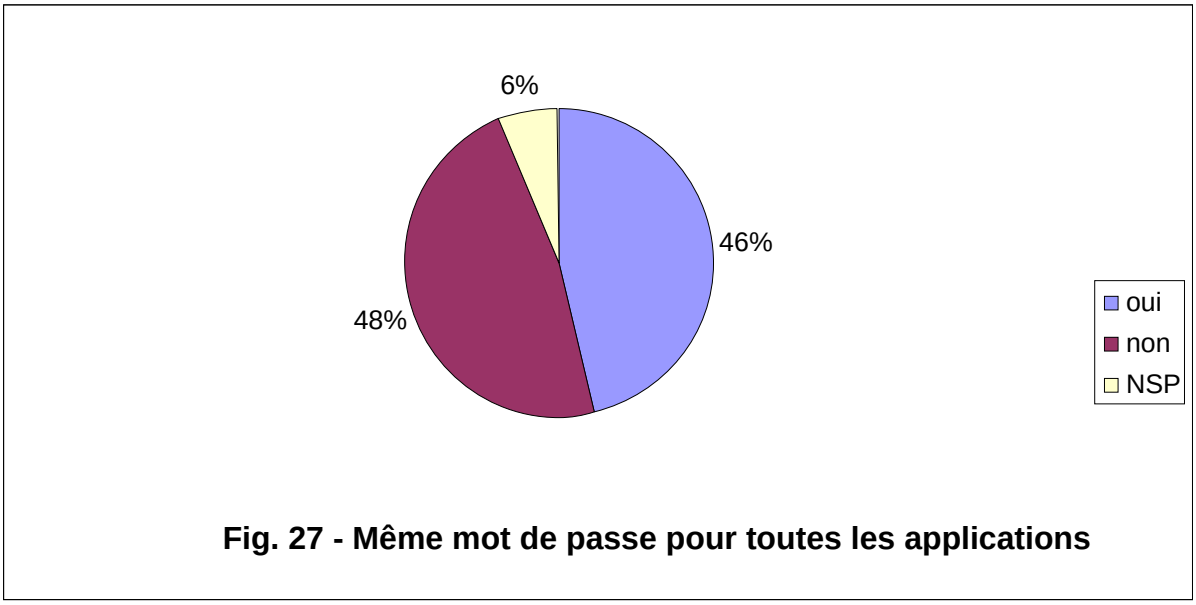


Fig. 27 - Même mot de passe pour toutes les applications

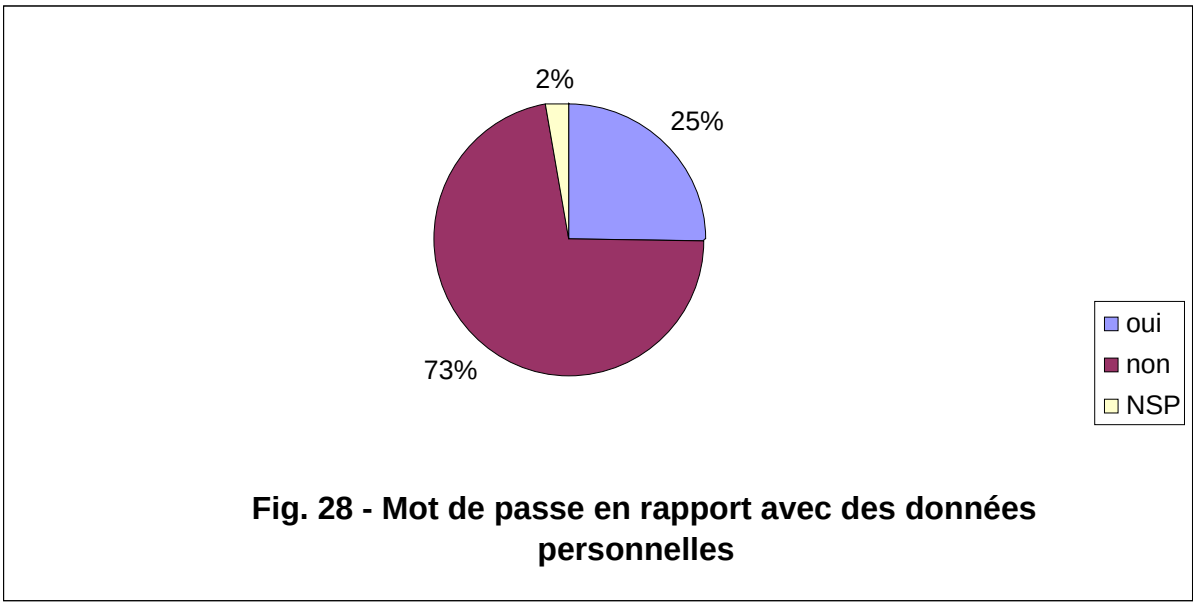


Fig. 28 - Mot de passe en rapport avec des données personnelles

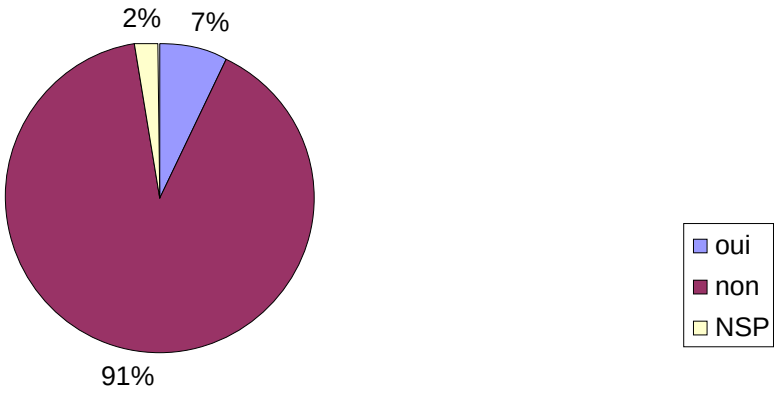


Fig. 29 - Notation des mots de passe pour pouvoir s'en rappeler

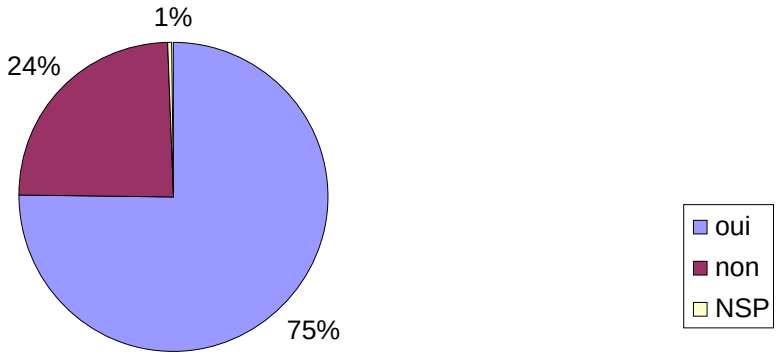


Fig. 30 - Ordinateur en veille

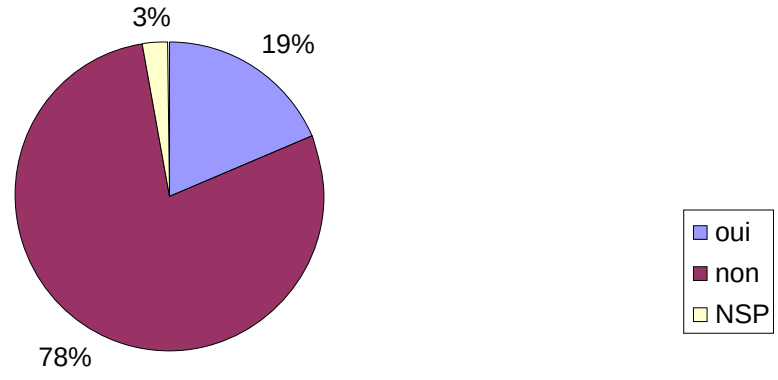


Fig. 31 - Mot de passe après la mise en veille

3.5.2 Les sauvegardes.

99% des médecins interrogés font des sauvegardes. A la question « faites vous des sauvegardes régulières des données concernant vos patients ? » 1% des médecins répondent « jamais » et 44% répondent « tous les jours ». 96% des médecins ayant répondu au questionnaire conservent des sauvegardes sur un support autre que le disque dur de leur ordinateur.

	Effectif (na = 3)	Proportion
Jamais	2	0.014
Parfois	18	0.123
Souvent	60	0.411
Tous les jours	65	0.445
NSP	1	0.007

TAB. 32 – Fréquences des sauvegardes

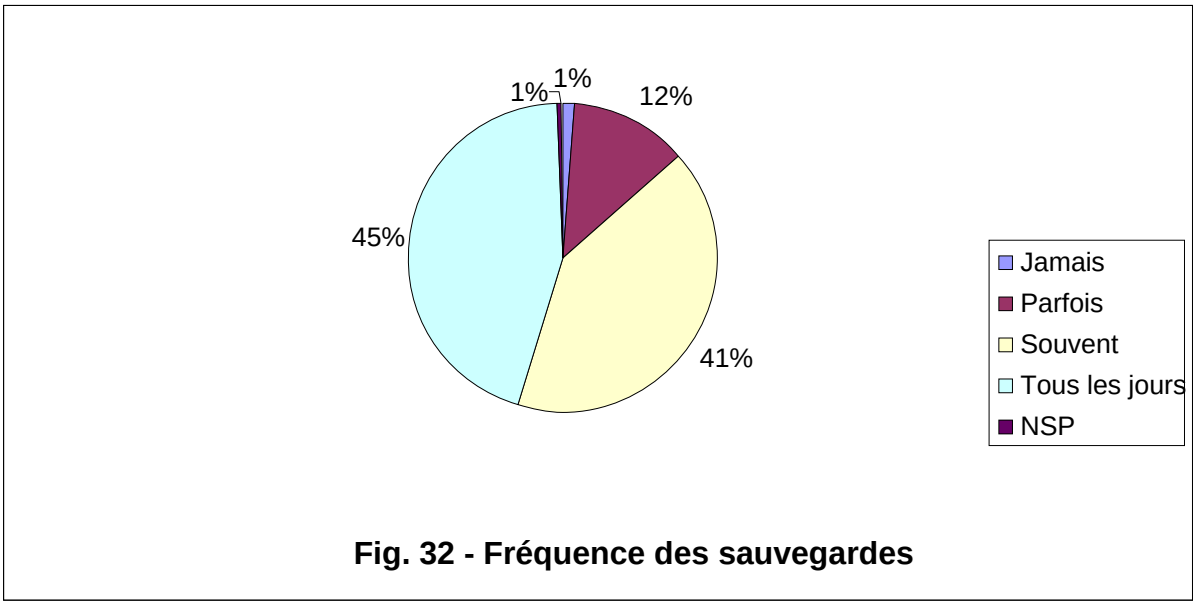


Fig. 32 - Fréquence des sauvegardes

	Effectif (na = 1)	Proportion
Oui	137	0.965
Non	5	0.035

TAB. 33 – Sauvegardes sur un autre support que le disque dur de leur ordinateur

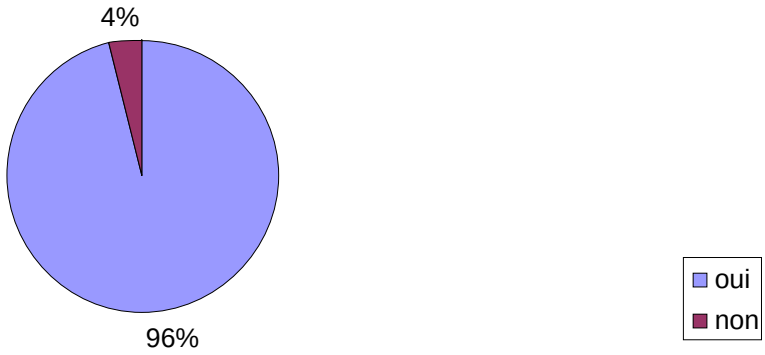


Fig. 33 - Sauvegardes sur un autre support que le disque dur de l'ordinateur

Parmi les différents supports, la clef USB et le disque dur externe sont majoritairement utilisés.

	Effectif	Proportion	NA
A : Disquettes	11	0.080	0
B : CD	16	0.117	0
C : DVD	19	0.139	0
D : Clef USB	59	0.431	0
E : Disque dur externe	61	0.445	0
F : Disquette zip	5	0.036	0
G : Serveur	6	0.044	0
H : Autre	6	0.044	0

TAB. 34 – Type d'autre support

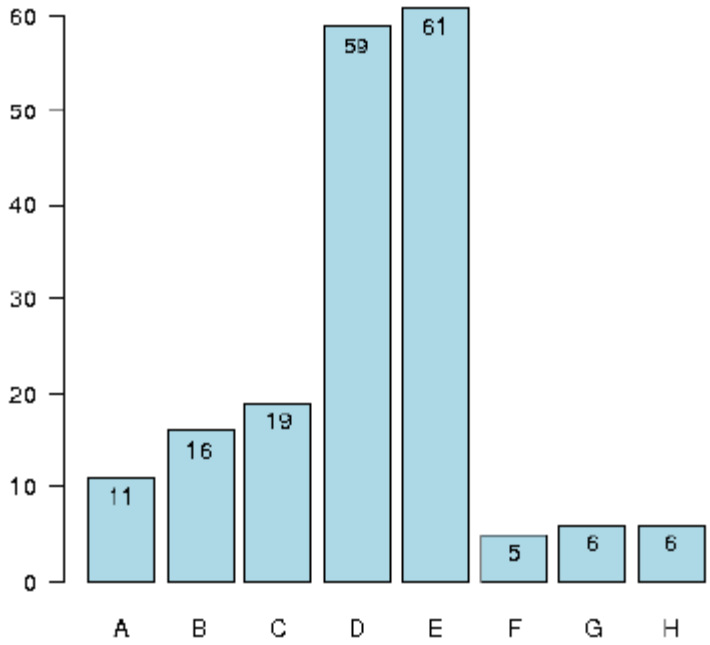


FIG 34 – Type d'autre support

53% des médecins interrogés n'ont jamais essayé de restaurer des données sauvegardées.

	Effectif (na = 2)	Proportion
Jamais	75	0.532
Parfois	46	0.326
Souvent	10	0.071
Tous les jours	3	0.021
NSP	7	0.050

TAB. 35 – Essai de restauration

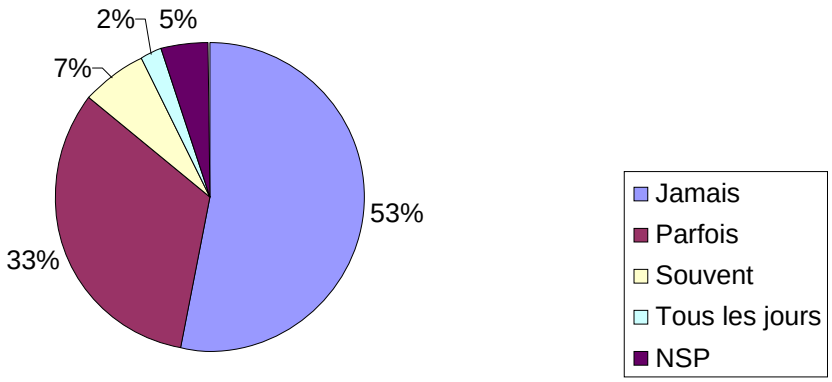


Fig. 35 - Essai de restauration

3.5.3 La protection physique des données patients.

Parmi les médecins interrogés :

- 58% ont placé l'unité centrale de leur ordinateur dans une zone peu exposée aux variations de température.
- 64% ont pris des dispositions pour protéger l'unité centrale du vol.
- 62% ont pris des dispositions pour protéger les sauvegardes du vol.
- 67% conservent des copies de sauvegarde en dehors du cabinet.

	Effectif (na = 1)	Proportion
Oui	85	0.574
Non	55	0.372
NSP	8	0.054

TAB. 36 – Ordinateur dans une zone peu exposée aux variations de température

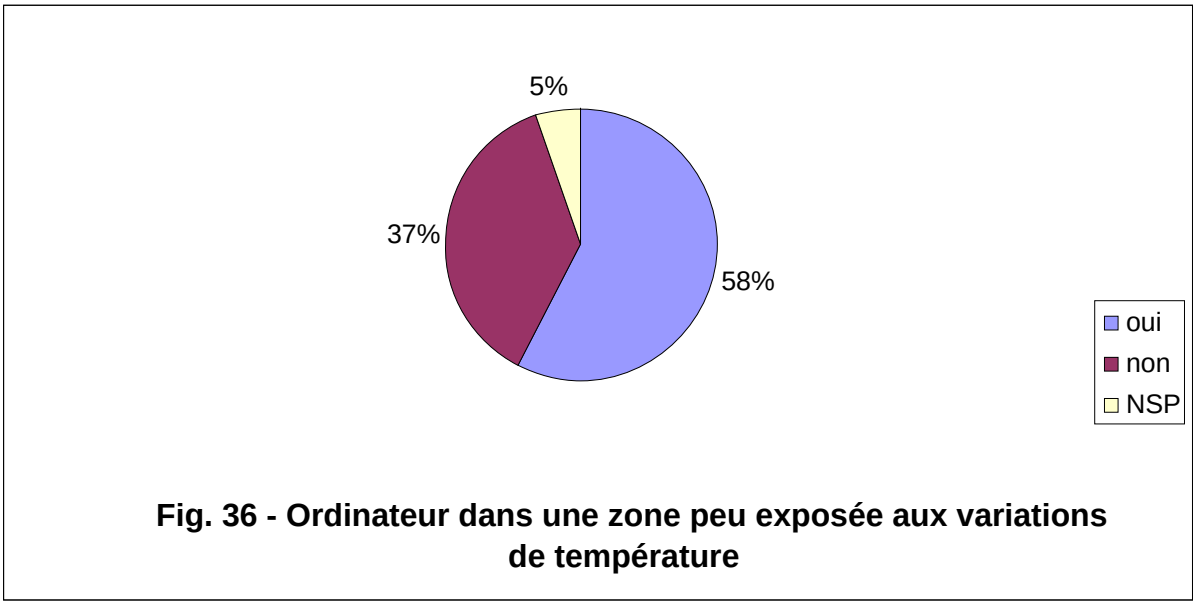


Fig. 36 - Ordinateur dans une zone peu exposée aux variations de température

	Effectif (na = 2)	Proportion
Oui	95	0.646
Non	48	0.327
NSP	4	0.027

TAB. 37 – Protection de l'unité centrale contre le vol

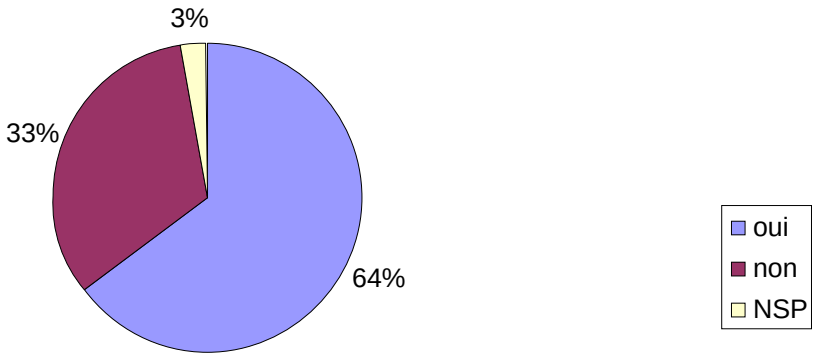


Fig. 37 - Protection de l'unité centrale contre le vol

	Effectif (na = 3)	Proportion
Oui	83	0.619
Non	47	0.351
NSP	4	0.030

TAB. 38 – Protection des sauvegardes contre le vol

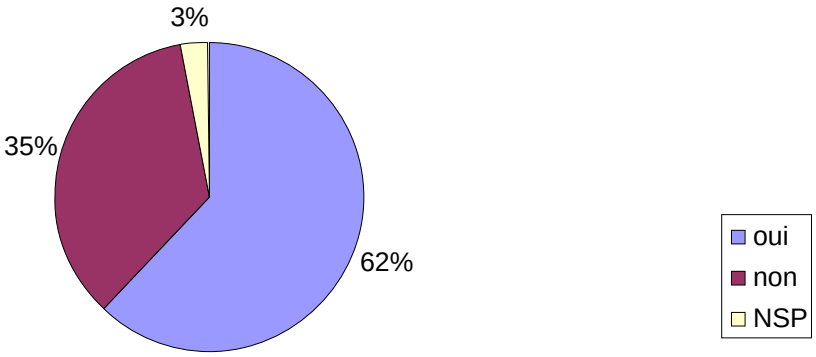


Fig. 38 - Protection des sauvegardes contre le vol

	Effectif (na = 1)	Proportion
Oui	90	0.662
Non	44	0.324
NSP	2	0.015

TAB. 39 – Copie des sauvegardes hors cabinet

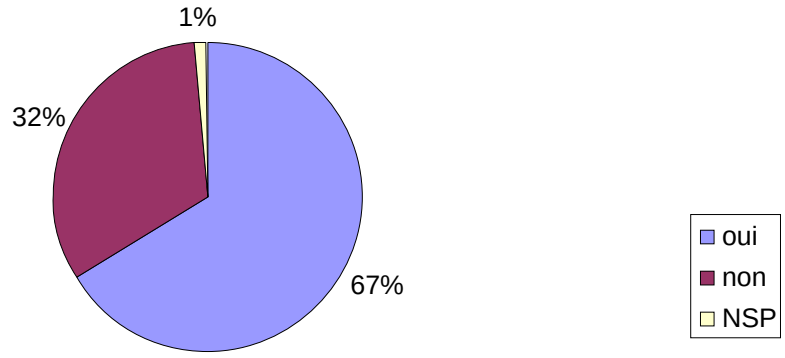


Fig. 39 - Copies de sauvegarde hors cabinet

3.5.4 La protection logicielle de l'ordinateur.

- 78% des médecins ayant répondu au questionnaire utilisent un antivirus. Parmi eux, 80% le mettent à jour régulièrement.
- 40% utilisent un logiciel contre les spywares.
- 51% utilisent un firewall.
- 9% utilisent un logiciel sécurisé d'effacement des données.

	Effectif (na = 2)	Proportion
Oui	115	0.782
Non	29	0.197
NSP	3	0.020

TAB. 40 – Antivirus

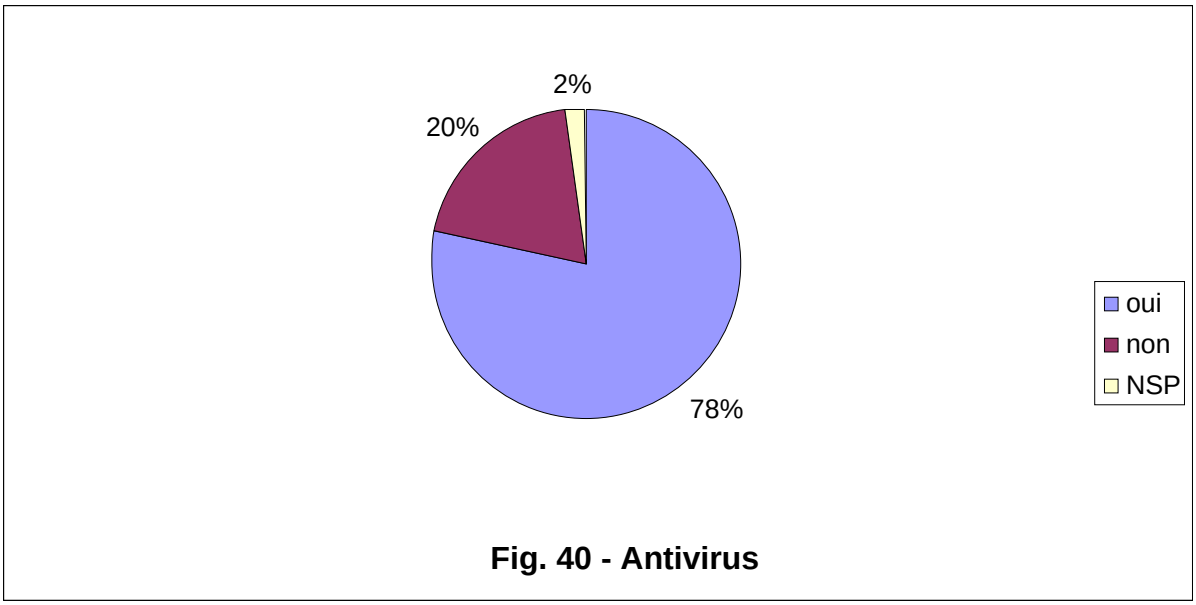


Fig. 40 - Antivirus

	Effectif (na = 2)	Proportion
Oui	90	0.796
Non	16	0.142
NSP	7	0.062

TAB. 41 – Mise à jour régulière de l'antivirus

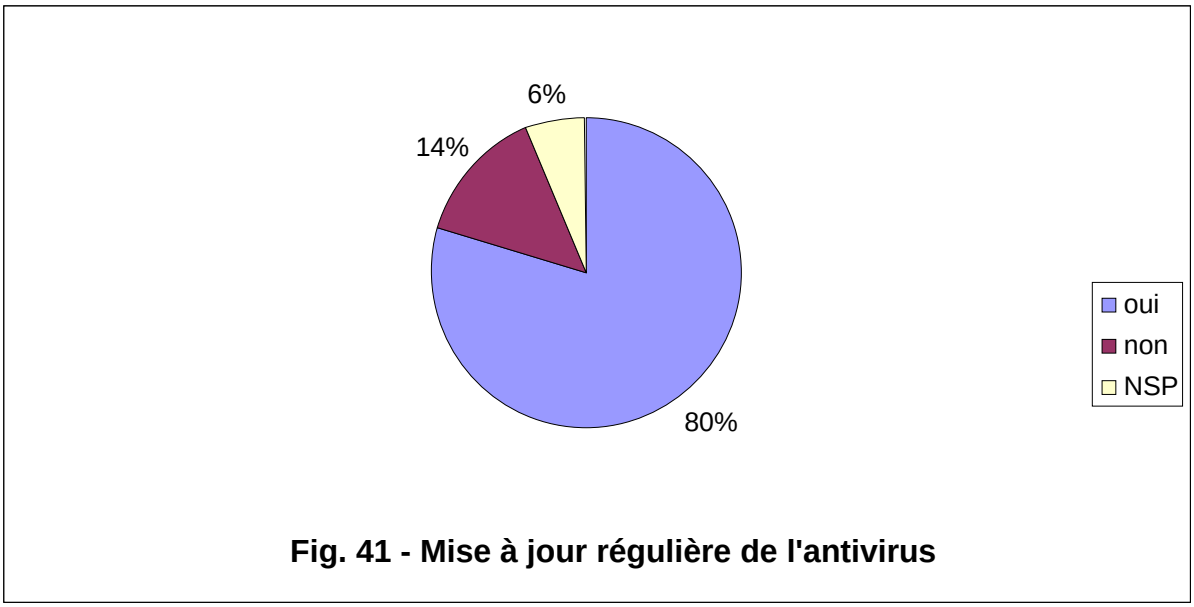


Fig. 41 - Mise à jour régulière de l'antivirus

	Effectif (na = 8)	Proportion
Oui	56	0.397
Non	48	0.340
NSP	37	0.262

TAB. 42 – Logiciel contre les spywares

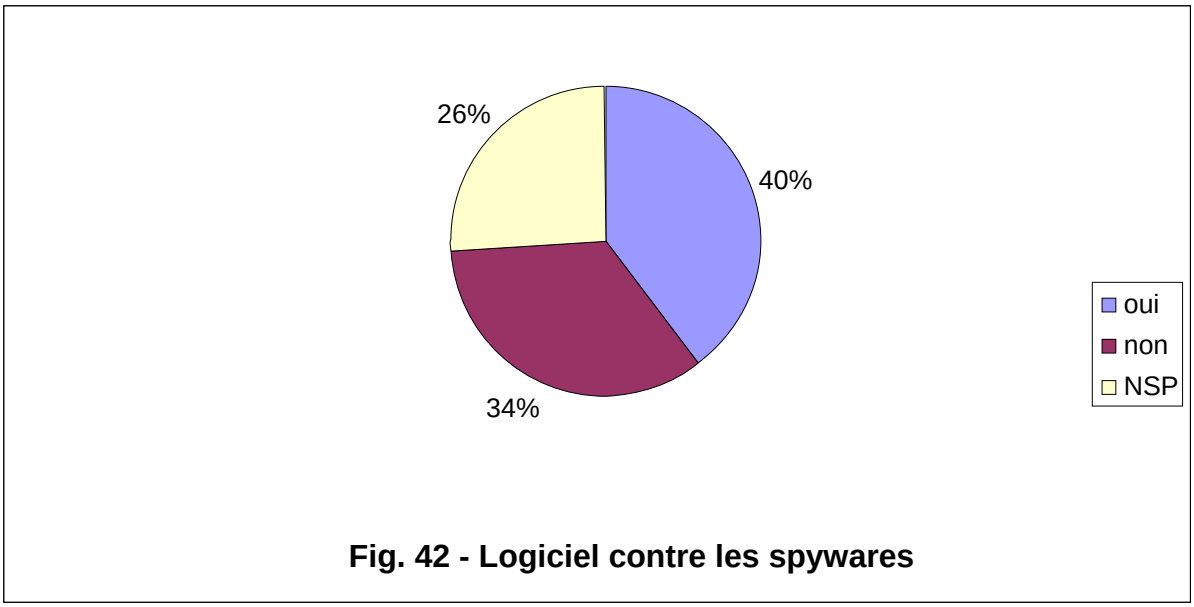


Fig. 42 - Logiciel contre les spywares

	Effectif (na = 8)	Proportion
Oui	73	0.518
Non	39	0.277
NSP	29	0.206

TAB. 43 – Firewall

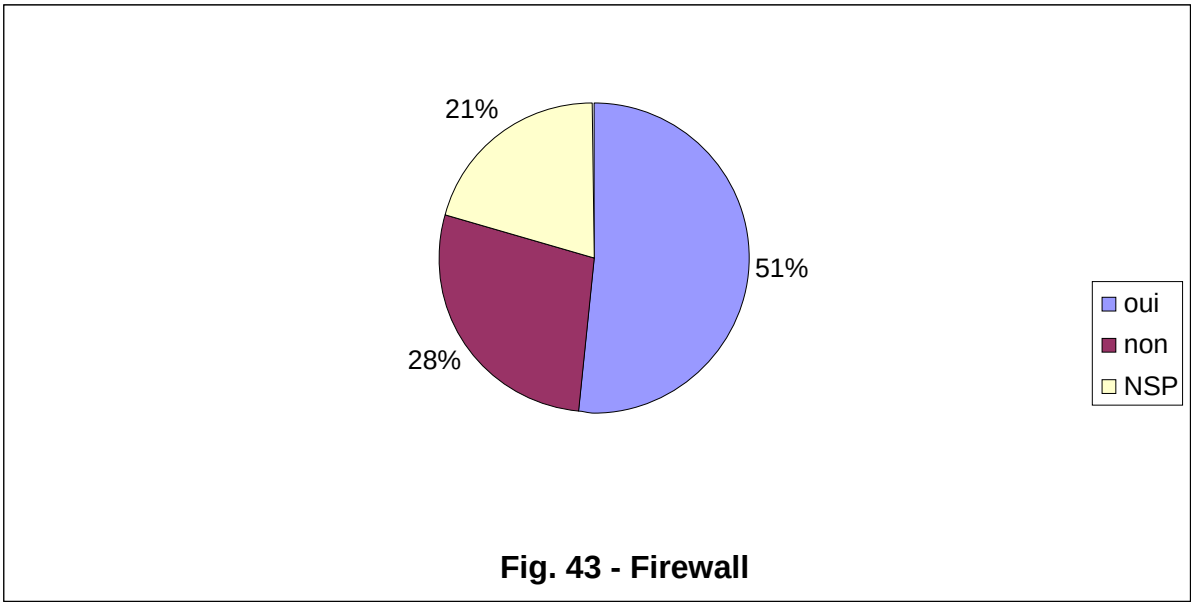


Fig. 43 - Firewall

	Effectif (na = 12)	Proportion
Oui	13	0.095
Non	74	0.540
NSP	50	0.365

TAB. 44 – Effacement sécurisé des données

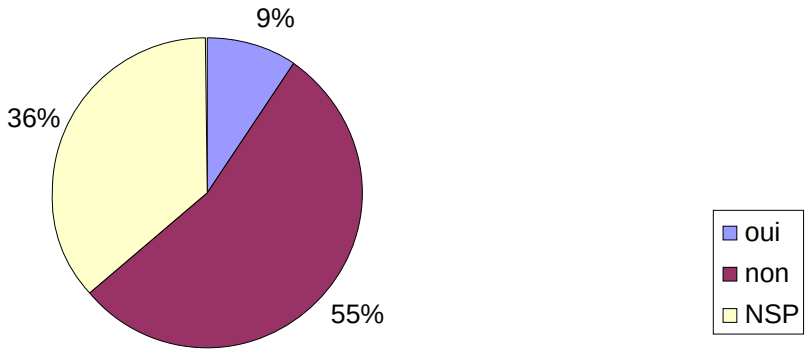


Fig. 44 - Effacement sécurisé des données

3.5.5 L'assistance informatique.

67% des médecins ont souscrit une garantie lors de l'achat de leur matériel informatique. Celle-ci propose une solution de remplacement dans 77% des cas.

	Effectif (na = 3)	Proportion
Oui	98	0.671
Non	42	0.288
NSP	6	0.041

TAB. 45 – Garantie

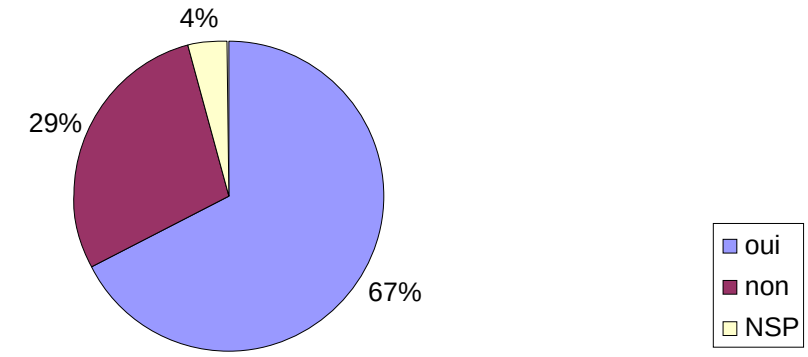


Fig. 45 - Garantie

	Effectif (na = 4)	Proportion
Oui	72	0.766
Non	22	0.234

TAB. 46 – Solutions de rechange en cas de défaillance

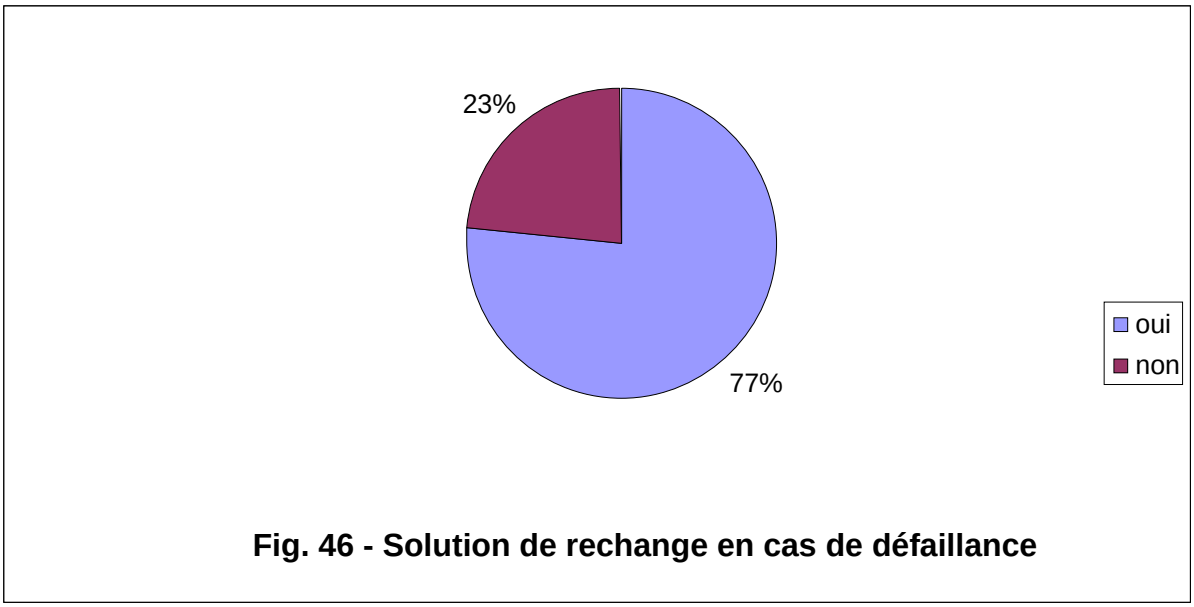


Fig. 46 - Solution de rechange en cas de défaillance

Les médecins interrogés ont fait appel à une assistance téléphonique :

- Pour le matériel dans 52% des cas
- Pour le logiciel dans 78% des cas

	Effectif (na = 6)	Proportion
Oui	74	0.517
Non	69	0.483

TAB. 47 – Assistance téléphonique pour le matériel

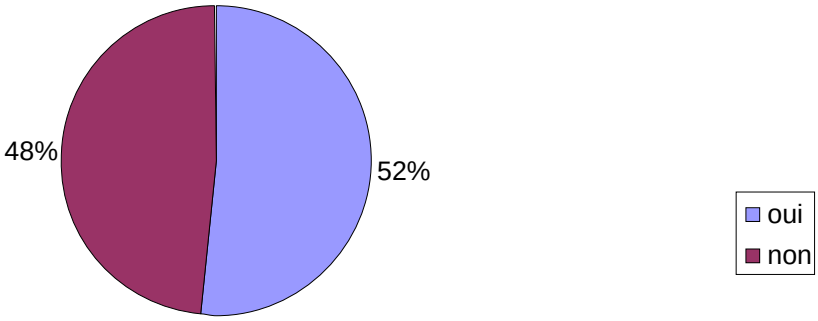


Fig. 47 - Assistance téléphonique pour le matériel

	Effectif (na = 6)	Proportion
Oui	112	0.783
Non	31	0.217

TAB. 48 – Assistance téléphonique pour le logiciel de gestion de données patient

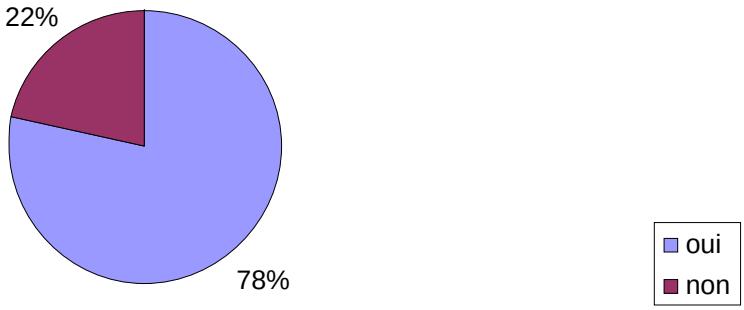


Fig. 48 - Assistance téléphonique pour le logiciel de gestion des données patient

87% ont été satisfaits par les réponses fournies. 55% des médecins ayant répondu au questionnaire ont fait appel à un technicien au cabinet. Parmi ces médecins, 94% ont été satisfaits de ce service.

	Effectif (na = 2)	Proportion
Oui	101	0.871
Non	14	0.121
Variable	1	0.009

TAB. 49 – Satisfaction

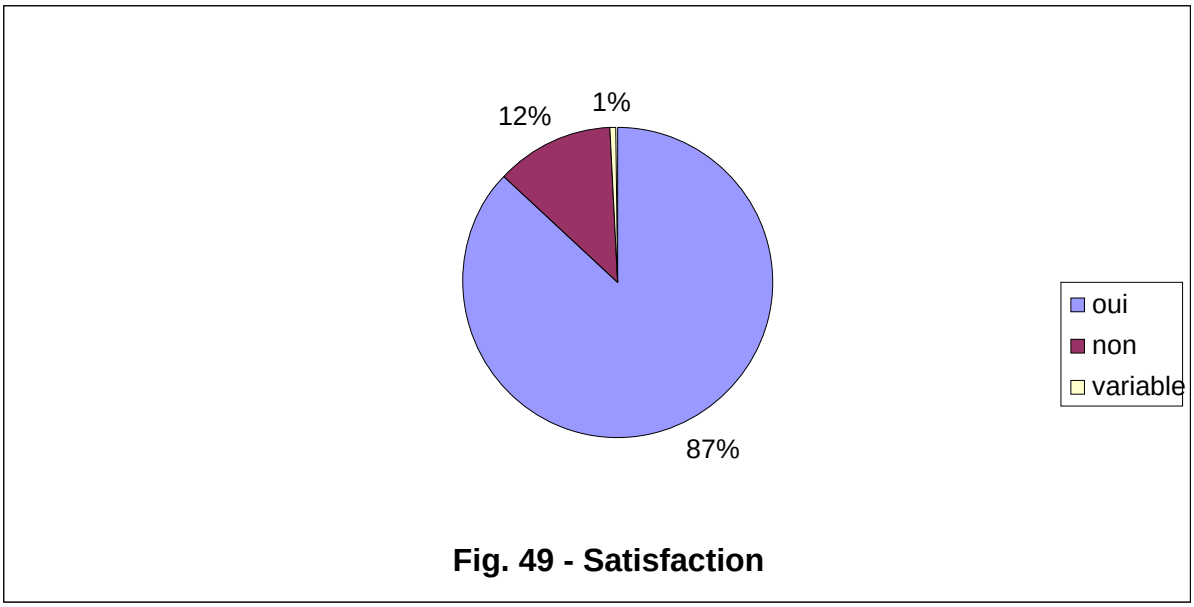


Fig. 49 - Satisfaction

	Effectif (na = 10)	Proportion
Oui	77	0.554
Non	62	0.446

TAB. 50 – Technicien sur place

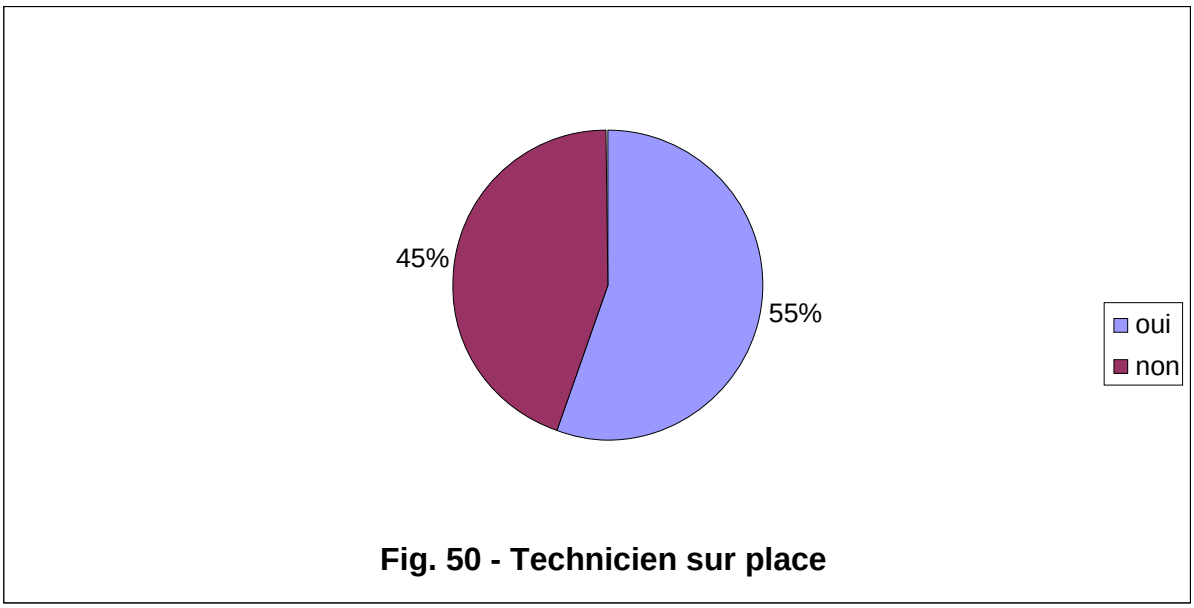


Fig. 50 - Technicien sur place

	Effectif (na = 0)	Proportion
Oui	72	0.935
Non	5	0.065

TAB. 51 – Problème résolu

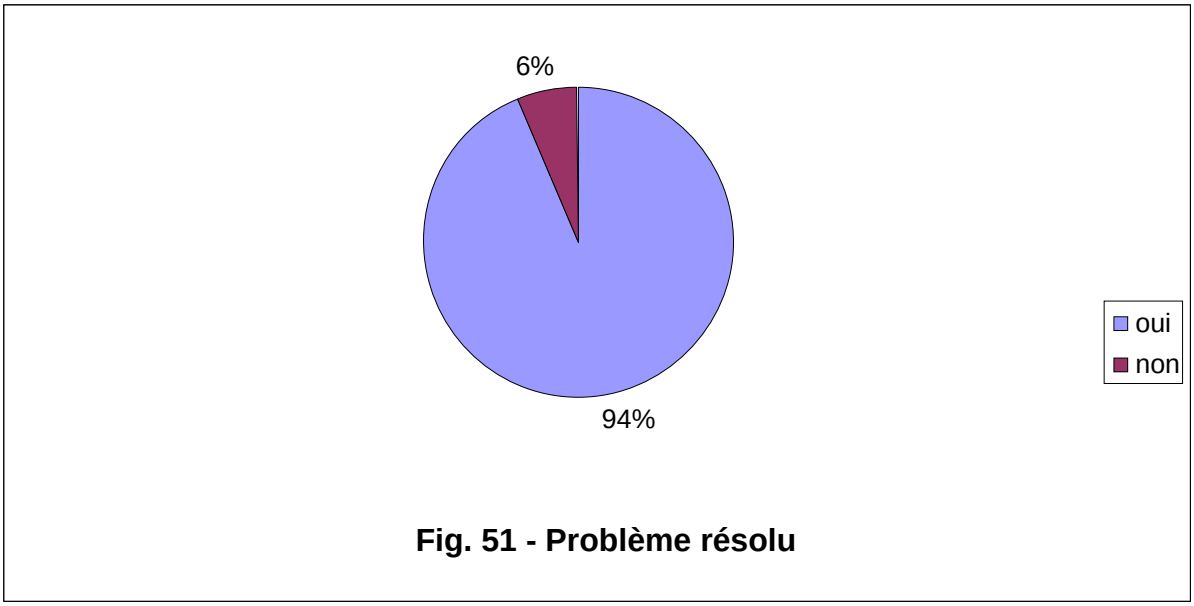


Fig. 51 - Problème résolu

3.6. L'expérience des médecins interrogés.

3.6.1 Perte de données patients informatisées.

31% des médecins interrogés ont perdu des données patients informatisées. Pour 51% d'entre eux la perte de données n'est survenue qu'une fois. Et dans 48% des cas la perte de données est comprise entre 1 et 8 jours.

	Effectif (na = 2)	Proportion
Oui	45	0.306
Non	100	0.680
NSP	2	0.014

TAB. 52 – Perte de données patient informatisées

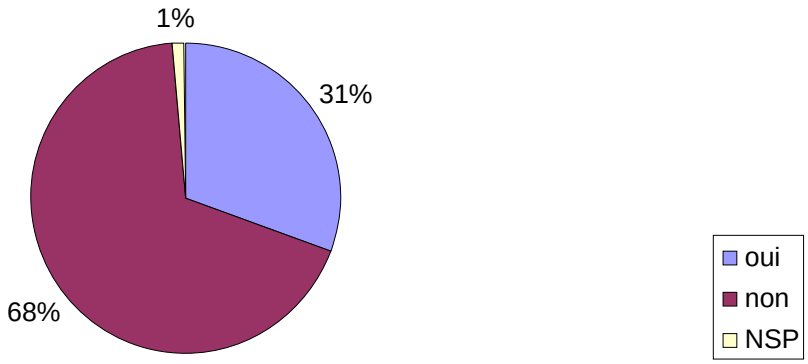


Fig. 52 - Perte de données patient informatisées

J'ai eu plusieurs difficultés pour formuler cette question. Tout d'abord comment quantifier une perte de données ? Pour simplifier, j'ai décidé de la formuler en jours en donnant un exemple. Je considère que si la dernière sauvegarde remonte à 15 jours, la perte de données est estimée à 15 jours. Ensuite je souhaitais rechercher une amélioration entre la première perte de données et la dernière. Mais trop peu de médecins ont répondu à la deuxième partie de la question (soit 11 sur les 45 ayant perdu des données patients) j'ai donc décidé de ne pas exploiter ces réponses.

	Moyenne	Mediane	Ecart-type	Min	Max	NA
Nombre d'épisodes de perte de données	2.282	1	2.384	1	10	6

TAB. 53 – Nombre d'épisodes de perte de données

	Effectif (na = 6)	Proportion
1	20	0.513
2	9	0.231
3	7	0.179
10	3	0.077

TAB. 54 – Nombre d'épisodes de perte de données

	Moyenne	Mediane	Ecart-type	Min	Max
Quantité de données perdues la première fois (en jours)	23.130	3	86.199	0	500

TAB. 55 – Quantité de données perdues la première fois (en jours)

	Effectif (na = 6)	Proportion
0	1	0.030
0.3	1	0.030
1	10	0.303
2	3	0.091
3	2	0.061
7	4	0.121
8	1	0.030
10	4	0.121
15	1	0.030
30	5	0.152
500	1	0.030

TAB. 56 – Quantité de données perdues la première fois (en jours)

	Moyenne	Mediane	Ecart-type	Min	Max
Quantité de données perdues la dernière fois (en jours)	91.889	3	240.017	1	730

TAB. 57 – Quantité de données perdues (première fois)

	Effectif (na = 10)	Proportion
-27	1	0.111
-15	1	0.111
-8	1	0.111
-7	1	0.111
0	1	0.111
2	1	0.111
3	1	0.111
30	1	0.111
715	1	0.111

TAB 58 – Différence de quantité de données perdues

3.6.2 L'accès non autorisé aux données patients.

Un tiers a pu avoir accès à des données patients à l'insu du médecin dans 4% des cas.

	Effectif (na = 2)	Proportion
Oui	4	0.027
Non	139	0.946
NSP	4	0.027

TAB 59 – Par mot de passe

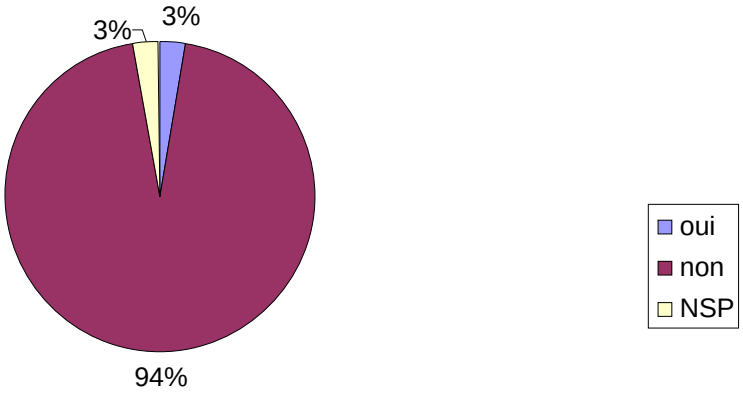


Fig. 53 - Par mot de passe

	Effectif (na = 9)	Proportion
Oui	3	0.021
Non	131	0.936
NSP	6	0.043

TAB 60 – Par un autre moyen

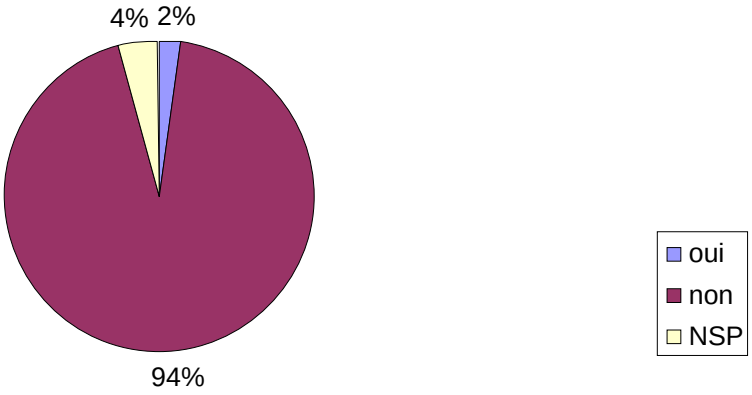


Fig. 54 - Par un autre moyen

	Effectif (na = 9)	Proportion
Oui	6	0.043
Non	128	0.914
NSP	6	0.043

TAB 61 – Quelque soit le moyen

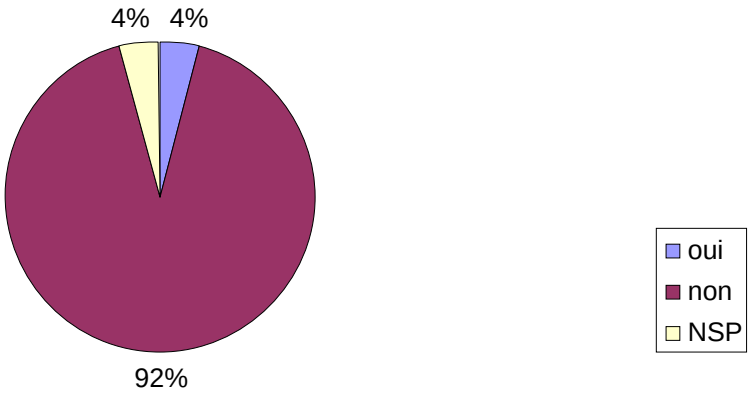


Fig. 55 - Quelque soit le moyen

3.6.3 La perte de données d'origine criminelle.

7% des médecins se sont fait volé le disque dur de leur ordinateur.

	Effectif (na = 0)	Proportion
Oui	11	0.074
Non	138	0.926

TAB 62 – Vol de disque dur

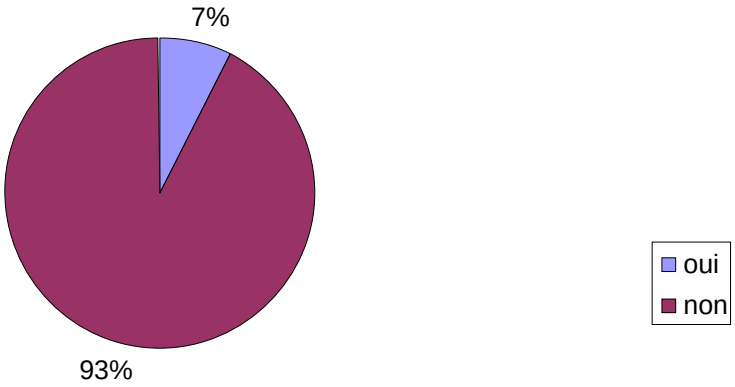


Fig. 56 - Vol de disque dur

1% (soit 2 médecins) ont subi une destruction criminelle de celui-ci.

	Effectif (na = 4)	Proportion
Oui	2	0.014
Non	139	0.959
NSP	4	0.028

TAB 63 – Destruction de disque dur

Seul un des 149 médecins interrogés a subi une destruction du support de ses sauvegardes d'origine criminelle. Il s'agit en fait d'un des deux médecins cités précédemment qui lors d'un incendie criminel a perdu à la fois son ordinateur et ses sauvegardes.

	Effectif (na = 1)	Proportion
Oui	1	0.007
Non	134	0.985
NSP	1	0.007

TAB 64 – Destruction de support de sauvegarde

24% des médecins ayant répondu au questionnaire ont déjà été victimes d'un virus informatique.

	Effectif (na = 2)	Proportion
Oui	36	0.245
Non	108	0.735
NSP	3	0.020

TAB 63 – Infection par un virus

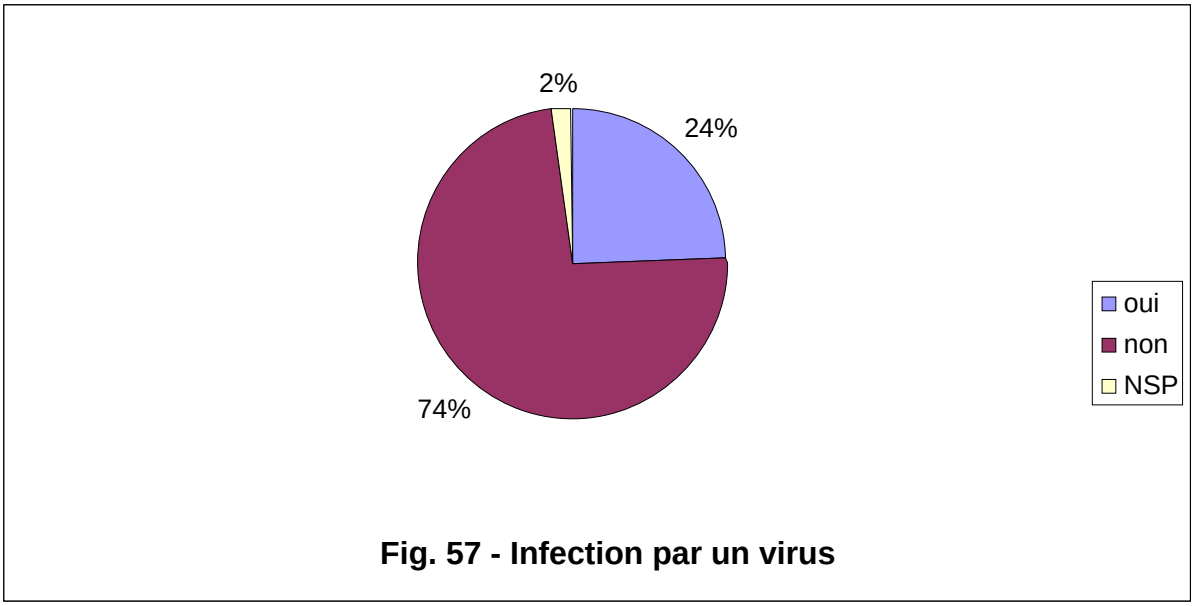


Fig. 57 - Infection par un virus

3.6.4 La perte de données d'origine accidentelle.

16% des médecins interrogés ont subi une destruction accidentelle du disque dur. Et 14% ont déjà perdu des sauvegardes contenant des données patients informatisées.

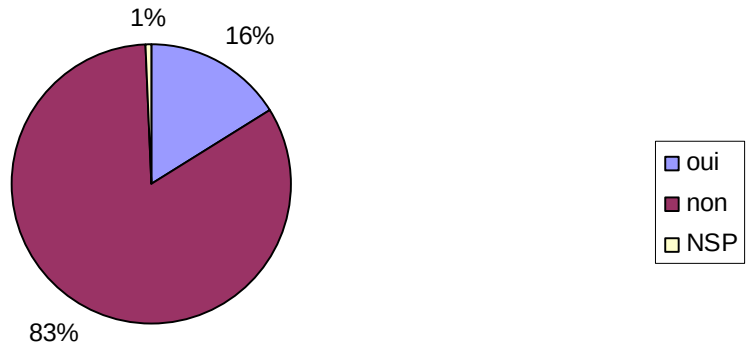


Fig. 58 - Destruction accidentelle du disque dur

	Effectif (na = 1)	Proportion
Oui	24	0.162
Non	123	0.831
NSP	1	0.007

Tab 66 – Destruction accidentelle du disque dur

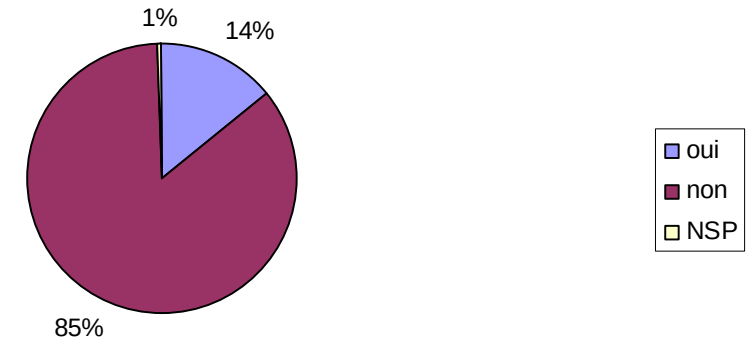


Fig. 59 – Perte de sauvegardes contenant des données patient informatisées

	Effectif (na = 0)	Proportion
Oui	21	0.141
Non	127	0.852
NSP	1	0.007

TAB 67 – Perte de sauvegardes contenant des données patient informatisées

A titre informatif, les raisons des pertes de sauvegardes sont regroupées dans le tableau 68.

	Effectif (na = 1)	Proportion
autre	4	0.200
autre= mauvaise sauvegarde	1	0.050
autre= sauvegarde incompatible avec nouveau logiciel	1	0.050
autre= vol	1	0.050
destruction du support	4	0.200
effacement de la sauvegarde	3	0.150
les patients des jours non sauvegardes	1	0.050
modification du logiciel	1	0.050
perte de la sauvegarde	3	0.150
P/E sauvegarde et P/E support	1	0.050

TAB 68 – Raisons des pertes des sauvegardes

18% de la totalité des médecins interrogés ont été au moins une fois dans l'impossibilité de restaurer des données sauvegardées.

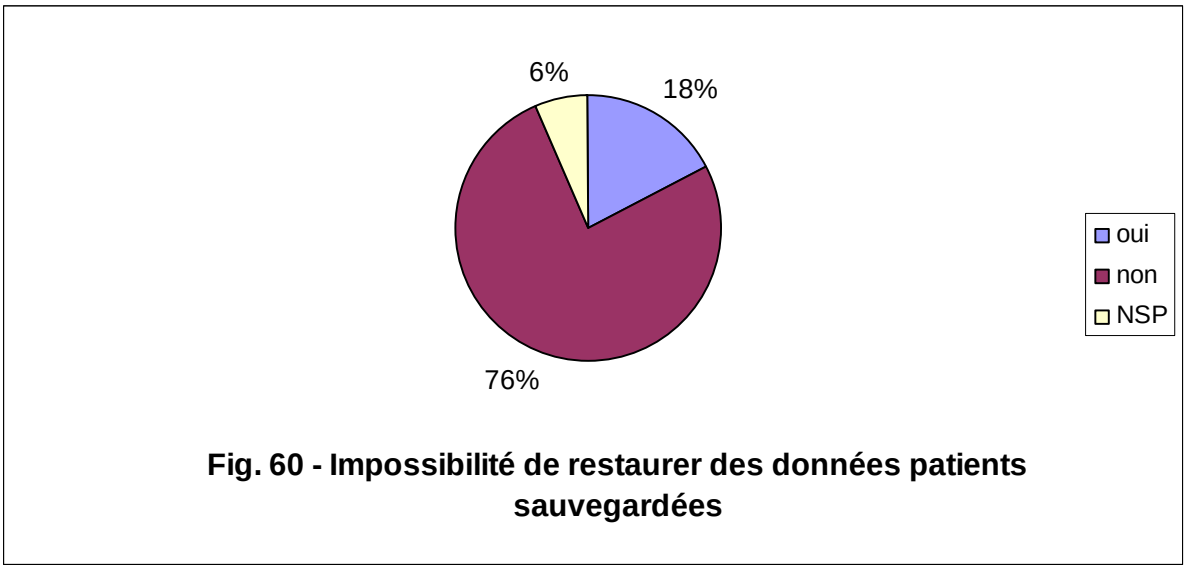


Fig. 60 - Impossibilité de restaurer des données patients sauvegardées

	Effectif (na = 24)	Proportion
Oui	22	0.176
Non	95	0.760
NSP	8	0.064

TAB 69 – Impossibilité de restaurer des données patient sauvegardées

3.6.5 Le ressenti des médecins interrogés.

- 30% des médecins ont eu des réticences avant de s'informatiser.
- 63% ont confiance dans la protection de leurs données informatisées (11% de non répondants).
- 62% pensent que leur système informatique est compatible avec le respect du secret médical (22% de non répondants).

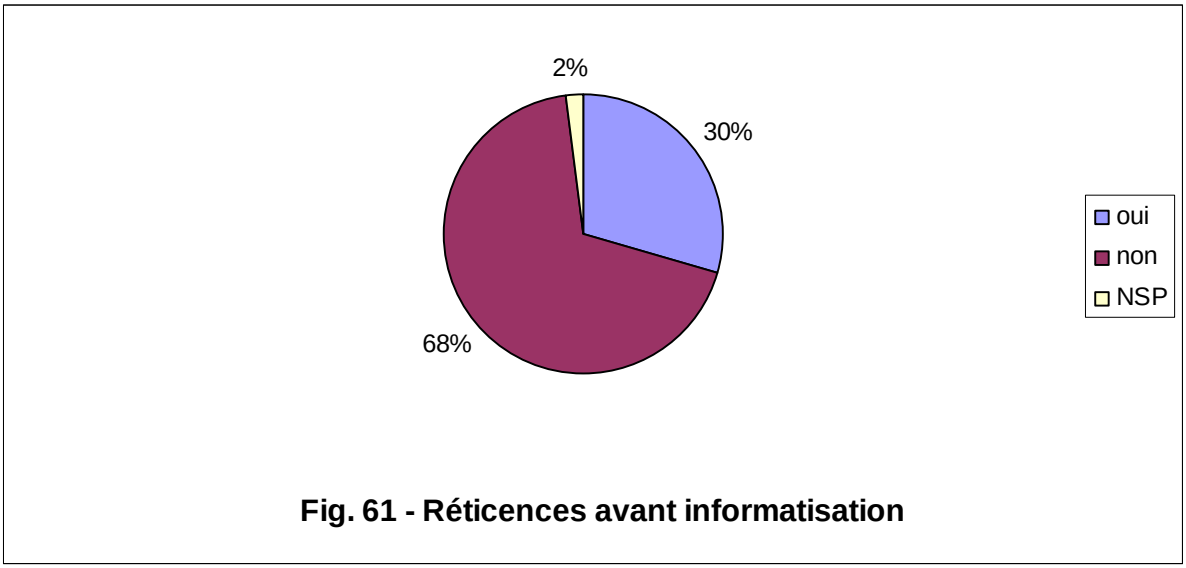


Fig. 61 - Réticences avant informatisation

	Effectif (na = 0)	Proportion
Oui	44	0.295
Non	102	0.685
NSP	3	0.020

TAB 70 – Réticences liées à la protection de vos données patient informatisées

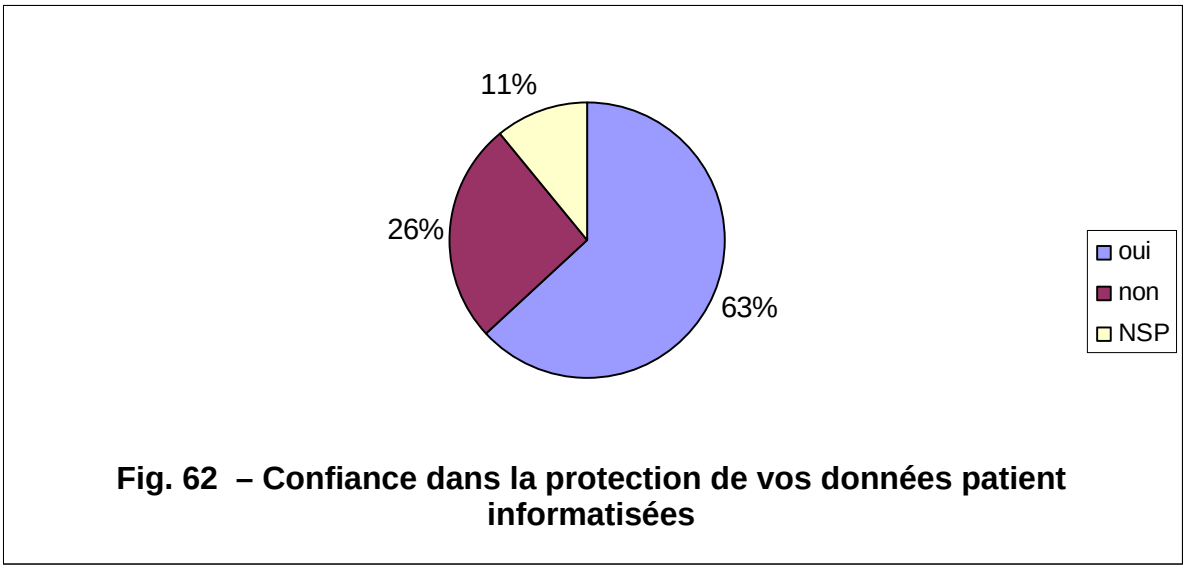


Fig. 62 – Confiance dans la protection de vos données patient informatisées

	Effectif (na = 0)	Proportion
Oui	94	0.631
Non	39	0.262
NSP	16	0.107

TAB 71 – Confiance dans la protection de vos données patient informatisées

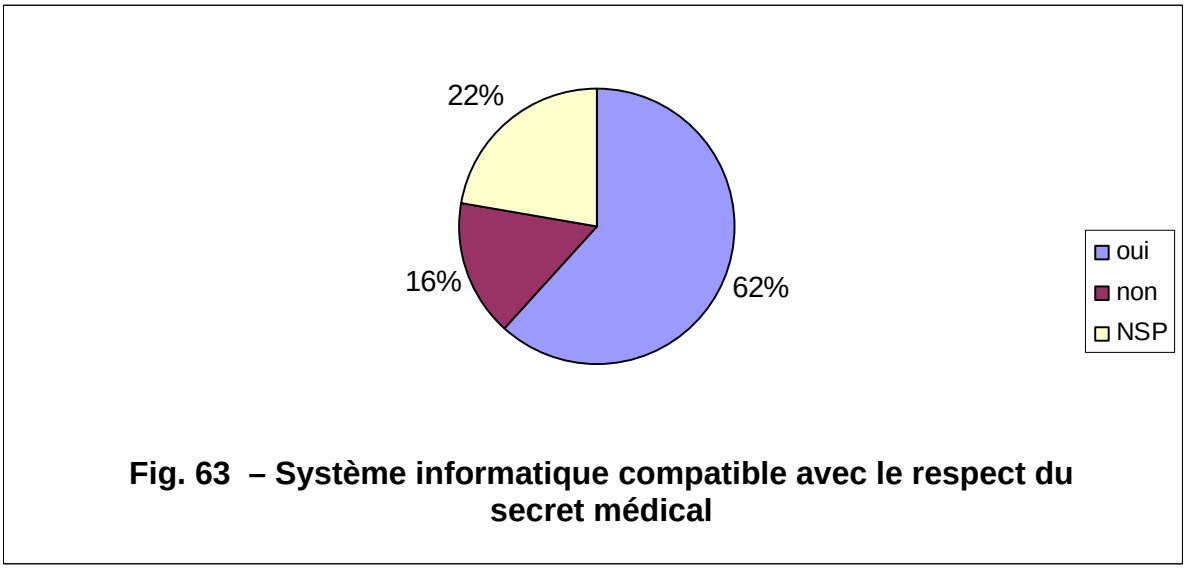


Fig. 63 – Système informatique compatible avec le respect du secret médical

	Effectif (na = 0)	Proportion
Oui	92	0.617
Non	24	0.161
NSP	33	0.221

TAB 72 – Système informatique compatible avec le respect du secret médical

4. DISCUSSION.

4.1. Démographie et matériel informatique des médecins interrogés.

4.1.1 Démographie.

Cette partie a pour intérêt de cerner la population des médecins interrogés. Celle-ci semble comparable à celle d'autres études portant sur l'informatique au cabinet du généraliste (4) (7) (9). Pour rappel, on constate une prédominance de médecins hommes. L'âge médian des médecins interrogés est de 51 ans.

4.1.2 Matériel utilisé.

Le matériel le plus fréquemment retrouvé au cabinet des médecins généralistes interrogés comprend un ordinateur fixe de type PC (Personal Computer).

Ce matériel est récent. Il a été renouvelé moins de deux ans auparavant pour 51% des médecins de l'étude. Cette impression se confirme en regardant les périphériques utilisés par les médecins au cabinet. Bien sûr, beaucoup possèdent une imprimante et un scanner, mais on constate qu'ils utilisent aussi des clefs USB et des graveurs DVD.

Une grande majorité des médecins interrogés ont une connexion internet dédiée à un usage professionnel et parmi eux 64% ont une connexion ADSL.

Les médecins interrogés ont donc tendance à s'équiper en matériel récent et le renouvèlent pour s'adapter à l'évolution des technologies informatiques.

4.1.3 Utilisation du matériel informatique.

Les deux principales utilisations de l'informatique au cabinet restent la télétransmission et le logiciel médical. La quasi-totalité des médecins interrogés télétransmettent les feuilles de soins et utilisent un logiciel de gestion des données concernant les patients.

Les médecins généralistes interrogés diversifient l'usage de leur ordinateur : courriel professionnel, ressources électroniques diverses (comme le dictionnaire

VIDAL par exemple), gestion de la comptabilité libérale ou aide mémoire informatique dans le cadre du suivi des patients.

Je constate que l'utilisation de l'outil informatique est diversifiée et prend une part importante dans la pratique des médecins généralistes libéraux.

4.1.4 La conservation de dossiers sur support papier.

Les médecins interrogés font donc plus que de la simple télétransmission de feuilles de soins électroniques. Pourtant beaucoup conservent des dossiers papier au cabinet (63%). Ils regroupent le plus souvent l'archivage des courriers et des examens complémentaires ainsi que les dossiers précédant l'informatisation du cabinet.

4.2. Protection des données patients informatisées.

4.2.1 Le mot de passe.

L'utilisation et l'élaboration d'un mot de passe sont des étapes primordiales dans la protection des données informatiques. Les médecins de l'étude utilisent à 66% un mot de passe pour accéder à leur ordinateur et à 79% pour leur logiciel de données patients.

Plusieurs critères permettent de définir un bon mot de passe. Dans le « jargon informatique », un mot de passe de qualité est un mot de passe fort. D'après la note d'information du CERTA concernant les mots de passe: *« Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules. »* (19)

Quelques règles simples pour choisir son mot de passe (20):

- *Avoir des mots de passe de 10 caractères minimum.*

- *Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).*
- *Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance…).*
- *Le même mot de passe ne doit pas être utilisé pour des accès différents.*
- *Changer de mot de passe régulièrement.*
- *En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.*
- *Éviter de stocker ses mots de passe dans un fichier ou lieu proche de l'ordinateur si celui-ci est accessible par d'autres personnes.*
- *Si possible, limiter le nombre de tentatives d'accès.*

Si l'on se rapporte aux données de l'étude, la majorité des médecins interrogés ne respectent pas les règles nécessaires à l'élaboration d'un mot de passe fort.

Pour rappel :

- 81% ne changent jamais leur(s) mot(s) de passe.
- 69% n'utilisent pas de mots de passe de plus de 8 caractères.
- 44% n'utilisent pas de caractères alphanumériques.
- 40% utilisent le même mot de passe pour toutes les applications.
- 21% utilisent des données personnelles pour élaborer leur(s) mot(s) de passe.
- 6% notent leur(s) mot(s) de passe pour pouvoir s'en rappeler.

Si l'on se rapporte aux données concernant les 114 médecins utilisant un mot de passe pour leur logiciel de gestion des données patients, on obtient les pourcentages suivants:

- 96% ne changent jamais leur mot de passe.
- 81% n'utilisent pas plus de 8 caractères.
- 54% n'utilisent pas de caractères alphanumériques.
- 45% utilisent le même mot de passe pour toutes les applications.
- 26% utilisent des données personnelles.

- 8% notent leur mot de passe pour pouvoir s'en rappeler.

Je n'ai pas pris en compte deux recommandations de la note du CERTA (celles concernant les logiciels retenant les mots de passe et ceux qui limitent le nombre d'accès). J'ai pu constater que celles-ci ne sont pas incluses par défaut dans les systèmes d'exploitation ou les logiciels médicaux les plus utilisés.

J'ai par contre souhaité inclure une autre mesure. Les systèmes d'exploitation informatique permettent de masquer les informations avec un écran de veille lorsque l'ordinateur n'est pas utilisé pendant un certain temps. Il est possible de paramétrer l'ordinateur pour que celui-ci demande un mot de passe qui désactive l'écran de veille. Une mesure très simple et qui me semble efficace contre les yeux indiscrets.

73% des médecins interrogés utilisent un écran de veille et seuls 19% parmi eux utilisent un mot de passe pour le désactiver.

En fonction des sources, le nombre de caractères minimum conseillé pour l'élaboration d'un mot de passe varie entre 8 et 10 caractères. Lors de mon étude, j'ai choisi un mot de passe d'au moins 8 caractères car c'est la recommandation qui est le plus souvent citée.

Si je sélectionne tous les médecins inclus dans la base de données de mon étude en fonction des recommandations du CERTA, seuls 2 médecins sur les 149 répondent aux critères sélectionnés (soit 1%)!

Les médecins libéraux interrogés sont donc sensibles à la nécessité d'utiliser un mot de passe pour protéger leurs données. Par contre, ils sont très peu informés sur les règles d'élaboration et de gestion des mots de passe.

4.2.2 La sauvegarde.

En cas de perte de données, la sauvegarde est essentielle à la restauration des données concernant les patients. Mais pour qu'elle assure son rôle, il faut respecter certaines règles dans son élaboration et sa mise à jour (20):

- Essayer les logiciels de récupération (restauration) et de sauvegarde.
- Sauver régulièrement les données
- Éloigner de l'ordinateur le support des sauvegardes de ses données.
- Vérifier la lisibilité des sauvegardes.

4.2.2.1 La fréquence des sauvegardes.

Pour qu'une sauvegarde soit utile, elle doit être mise régulièrement à jour, l'objectif étant de minimiser la perte de données en cas d'événement indésirable. Certains logiciels permettent d'automatiser les sauvegardes. Il est ainsi possible de programmer la fréquence et l'heure de sauvegarde pour que celles-ci s'effectuent en tache de fond. C'est un moyen sûr d'avoir des sauvegardes avec les dernières données disponibles sur le système.

Je suis resté imprécis dans les réponses possibles à la question : Faites-vous des sauvegardes régulières des données concernant vos patients ? Les médecins avaient le choix entre plusieurs réponses « tous les jours, souvent, parfois, jamais et je ne sais pas ». Avant de lancer mon étude, j'ai testé mon questionnaire avec une quinzaine de médecins «cobayes ». J'ai pu en conclure que ce paramètre est difficile à mémoriser avec exactitude et donc source d'erreur.

Le paramètre qui me semble important à retenir est que 44% des médecins ayant répondu au questionnaire font des sauvegardes

journalières. Au total, près de 85% des médecins de l'étude font régulièrement des sauvegardes. Et seulement 1% n'en fait jamais.

Une fois de plus, les médecins interrogés sont sensibilisés à l'importance de la sauvegarde mais aussi à l'intérêt de la tenir à jour pour qu'elle soit utile.

4.2.2.2 Le support de la sauvegarde.

Une fois que la sauvegarde est faite et à jour sur le disque dur, il est préférable de la dupliquer et de la délocaliser (ou de la sauvegarder directement sur un support externe comme un disque dur par exemple) et de faire une ou plusieurs copies de sauvegarde. En effet, il faut prévoir toute les éventualités et parmi elles une destruction du disque dur de l'ordinateur. Cela aussi, les médecins interrogés pour l'étude l'ont compris puisque 96% effectuent des copies de sauvegarde sur un support différent.

Plusieurs solutions sont possibles quant au choix de cette copie de sauvegarde. Dans la figure 33, j'ai regroupé les réponses des 138 médecins de l'étude faisant des copies de sauvegarde. Les réponses sont classées du support le plus ancien au plus moderne. En débutant l'étude je m'attendais à voir le CD-ROM et le DVD-ROM s'imposer comme mode de sauvegarde principal. Mais je constate une forte réactivité sur le type de support utilisé et sur la modernité du matériel utilisé par les généralistes interrogés. En effet les supports sur clefs USB et disque dur externe sont majoritairement utilisés. La disquette et la disquette ZIP tendent à disparaître. Par contre, je constate l'apparition d'un type de sauvegarde entièrement délocalisé et dématérialisé sur serveur internet. Il faut cependant rappeler que ce type de sauvegarde nécessite des hébergeurs spécialisés ayant les accréditations pour conserver des

données médicales. La catégorie « autre » comprend surtout des médecins possédant un autre ordinateur en particulier à leur domicile sur lequel ils conservent des copies de sauvegarde. Il est intéressant de noter que 25% des généralistes interrogés utilisent au moins deux types de support pour leurs sauvegardes.

4.2.2.3 La validité de la sauvegarde.

Une fois la sauvegarde effectuée régulièrement et dupliquée sur des supports différents, il reste un paramètre à prendre en compte. Il est en effet nécessaire de vérifier la validité (ou lisibilité) de cette sauvegarde. Il faut s'exercer à restaurer les données sauvegardées pour avoir la certitude de pouvoir le faire en cas de perte de données. Il est en effet fréquent en informatique de ne pas pouvoir utiliser une sauvegarde pour diverses raisons (changement de version du logiciel, sauvegarde corrompue, par exemple). Cet exercice est donc indispensable pour assurer la sécurité des données sauvegardées. Or, même si 85% des généralistes interrogés font régulièrement des sauvegardes de leurs données, 53% n'en ont jamais testé la validité. Il existe donc une faille simple à corriger, en vérifiant, régulièrement, que l'on est capable d'effectuer le processus de restauration des données sauvegardées. Mais il faut reconnaître que cela alourdit la tache administrative du médecin généraliste. Tester une restauration de données a un coup en temps et en mise en œuvre de moyens.

4.2.3 La protection physique.

Pour compléter ma vision sur la sécurité des données patients, j'ai souhaité interroger les médecins de l'étude sur la protection physique de leurs données.

Un des facteurs qui influencent classiquement la conservation des données informatiques est la variation de la température. 57% des généralistes interrogés ont pensé à ce facteur au moment de l'installation de leur matériel informatique.

64% des généralistes de l'étude protègent leur unité centrale du vol (dans un local fermé à clef par exemple). Volontairement, je n'ai pas approfondi les différents types de protection car aucune n'est fiable à 100%. Je retiens qu'une faible majorité des médecins interrogés ont pensé à l'éventualité d'un vol de matériel.

Seul 57% d'entre eux protègent leurs supports de sauvegardes. Cette mesure peut être discutée quand on sait que certains logiciels de gestion des données patients cryptent leurs sauvegardes et qu'il n'est possible de les utiliser qu'avec le logiciel en question.

Pour assurer la protection des données (en cas d'incendie ou de dégât des eaux par exemple), il est préférable de conserver des copies de sauvegarde en dehors du cabinet médical (en cas d'incendie par exemple). 65% des généralistes interrogés le font.

Il existe donc, dans ce domaine de la protection physique des données informatiques, des mesures simples à réaliser par le médecin généraliste, pour améliorer ces résultats.

4.2.4 La protection logicielle.

Pour assurer la sécurité des données informatiques il est nécessaire de s'équiper de certains logiciels. Les antivirus sont les logiciels les plus utilisés par les généralistes interrogés mais il en existe une multitude. En fait il existe une parade à chaque type d'intrusion. J'en ai sélectionné certains en fonction du type d'utilisation et des risques possibles, tout en restant réaliste. Il s'agit d'un cabinet médical, pas du Pentagone !

Dans l'introduction de ma thèse j'ai limité mon sujet à la protection des données concernant les patients. J'ai exclus de mon sujet la protection des échanges d'informations notamment par le biais d'Internet. Pourtant même sans échange, une connexion au Web reste une porte d'entrée pour un éventuel risque entraînant une destruction des données. C'est pourquoi j'ai décidé d'inclure ces questions, bien qu'elles soient à la limite de mon champ d'étude.

4.2.4.1 L'antivirus.

78% des médecins de l'étude utilisent un antivirus. Parmi ces médecins 80% font des mises à jour régulières de leur logiciel anti-virus. Les médecins interrogés sont donc conscients de l'importance d'avoir un antivirus mis à jour régulièrement pour protéger leur système informatique. Et compte tenu des résultats de l'étude que je développerais plus tard, cette protection est fondamentale.

4.2.4.2 Les autres logiciels.

- 50% utilisent un firewall.
- 38% utilisent un logiciel contre les spywares.
- 9% utilisent un logiciel sécurisé d'effacement des données.

Je constate d'emblée une moindre utilisation de ce type de logiciels. Pourtant avec l'augmentation de la mise en réseau des ordinateurs et le développement de l'Internet à haut débit ces logiciels acquièrent une importance considérable en sécurité informatique.

Je remarque dans les figures 42 et 43 que le taux de non réponse et de réponse par « je ne sais pas » est élevé. Ce qui me laisse supposer que beaucoup de médecins interrogés ne connaissent pas ce type de logiciels et leur utilisation.

4.2.5 L’assistance informatique.

Avant de commencer cette étude, je pensais que le médecin généraliste, en dehors d’une poignée de passionnés est un néophyte en informatique. Cette hypothèse comme j’ai pu le constater par la suite n’est plus tout à fait exacte.

Le but de cette partie du questionnaire est de chercher à savoir si les médecins interrogés ont cherché à déléguer certaines taches de maintenance du matériel et du logiciel de gestion des données patients. Même si ces questions ne concernent pas directement la conservation et la protection des données informatiques, elles interviennent dans la tenue des dossiers patients. En effet, sans ordinateur le médecin ne peut pas mettre à jour ses données informatiques. Ce qui sous entend, si cette éventualité n’est pas prévue, un retour temporaire au dossier papier et une perte de temps par la suite pour mettre les données informatisées à jour. D’autre part, il existe un risque d’erreur et perte d’information lors de la mise à jour des dossiers patients à posteriori.

67% des 149 généralistes de l’étude ont souscrits une assistance pour leur matériel informatique et pour 77% d’entre eux celle-ci propose une solution de rechange en cas de défaillance du système informatique. Seul 52% des médecins interrogés ont eu recours à une assistance téléphonique pour un problème matériel. Par contre 78% ont fait appel à une « hotline » pour le logiciel de gestion des dossiers patients.

Dans un deuxième temps, j’ai cherché à savoir si les médecins ayant eu recours à des informaticiens professionnels ont été satisfait des réponses fournies. Pour ces questions j’ai volontairement décidé de ne pas séparer les problèmes matériels et logiciels. 87% des médecins ayant eu recours à une assistance téléphonique ont été satisfait par les réponses fournies. 55% de la totalité des

médecins interrogés ont eu recours à un technicien sur place. Et pour 93% de ces médecins, l'informaticien a résolu leur problème.

Il paraît donc préférable pour les médecins n'ayant pas de connaissance en informatique de déléguer les taches et de ne pas hésiter à avoir recours à des professionnels pour résoudre certains problèmes. Pourtant en tant que médecin généraliste, si je désire confier toute la logistique liée a l'informatique de mon cabinet à un tiers, il faut pouvoir vérifier en posant certaines questions que certaines taches seront effectuées avant de signer le contrat de maintenance.

4.3. Expérience et ressenti des médecins de l'étude.

Cette partie de la discussion permet de confronter les hypothèses à la réalité du terrain. Dans quelle mesure les médecins généralistes sont-ils confrontés à des problèmes de sécurité informatique et de perte de données patients ?

4.3.1 Perte de données patients informatisées.

C'est une question fondamentale de l'étude. Elle reflète le manque d'efficacité de la protection des données par les médecins généralistes interrogés.

Près d'un tiers (31%) des médecins ayant répondu au questionnaire ont déjà perdu des données médicales informatisées. Dans la majorité des cas (55%) cet événement n'est survenu qu'une fois. Mais il peut s'agir de la perte des données recueillies sur une journée (15%) aussi bien que la perte de la totalité des données patients du cabinet (13%).

J'ai souhaité savoir si les médecins n'ayant pas perdu de données avaient tendance à mieux protéger celles-ci. J'ai donc extrait les données concernant la protection des données du questionnaire (partie II) pour faire cette comparaison. Les résultats sont regroupés dans le tableau 73 et la figure 64.

pertedonnees.f	n	mean	sd	se	lower95ci	upper95ci
Oui	44.00	9.98	2.91	0.44	9.09	10.86
Non	95.00	10.12	2.80	0.29	9.55	10.69
NSP	2.00	8.00	5.66	4.00	-42.82	58.82
NA	2.00	6.50	0.71	0.50	0.15	12.85

TAB 73 – Degré de protection selon la perte de données

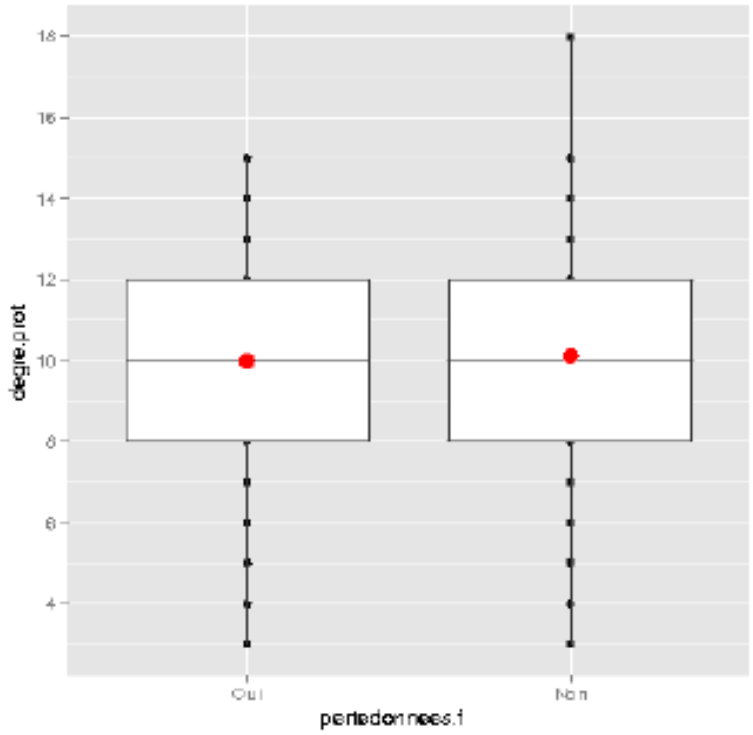


FIG 64 – Degré de protection selon la perte de données

D'après ces tableaux, je peux conclure qu'il n'y a pas de différence de protection significative entre les médecins ayant ou non perdu des données informatisées. Mais actuellement, la protection de ces mêmes médecins n'est pas assez efficace pour limiter les pertes de données médicales informatisées.

Il y a donc, tant que l'on n'utilisera pas un autre moyen de conservation des données concernant les patient en médecine libérale un intérêt réel à changer les habitudes et à adopter une ligne de conduite minimale permettant la protection de celles-ci.

4.3.2 Accès non autorisé aux données patients.

Cette partie de l'étude pose un problème dont plusieurs médecins interrogés m'ont fait la remarque. Je suis conscient d'un biais: si quelqu'un accède à vos

données avec votre mot de passe, vous n'avez aucun moyen de le savoir. Mais j'ai gardé cette question pour avoir une vue d'ensemble sur le sujet.

Seulement 3% des médecins interrogés ont connaissance d'un tiers ayant eu accès à leurs données patients avec leur mot de passe et 3% par un autre moyen. 1 médecin a répondu oui à ces deux questions. Donc, 5 médecins sur les 149 interrogés ont confirmé l'accès par un tiers non autorisé à leurs données patients informatisées. J'aurais aimé comparer ces chiffres avec ceux de médecins ayant des dossiers papiers, mais en pratique je n'ai pas de trouver une réponse à cette question.

L'accès non autorisé aux données informatisées concernant les patients dans les cabinets de médecine générale semble donc être un problème mineur.

4.3.3 La perte de données d'origine criminelle.

Ces questions permettent de compléter mon étude sur la sécurité des données en médecine de ville.

La perte de données d'origine criminelle est dominée par les vols de matériel informatique au cabinet du médecin généraliste. En effet, 7% des médecins ayant répondu au questionnaire ont subit un vol de matériel. La destruction criminelle du disque dur ou du support des sauvegardes est donc à prendre en compte.

J'ai souhaité inclure dans cette partie de l'étude une question sur les virus informatiques. Une des causes indirectes de la perte de données est liée à ces virus. Et il est intéressant de noter que 24% des médecins de l'étude ont été au moins une fois victime d'un virus informatique (figure 57). Ce qui représente un risque important à prendre en compte pour la protection des données.

Les échanges de données par internet ne font pas partir du champ de mon étude. Mais je considère la connexion au réseau comme une menace pour la sécurité des données patients informatisées.

« *Si vous disposez d'une connexion à Internet, sachez qu'il existe des risques d'intrusion dans votre système informatique pouvant conduire à l'implantation de virus ou d'autres programmes susceptibles d'altération vos données ou de récupérer à votre insu, certaines informations ».* Fiche thématique CNIL édition 2003.

Il faut noter la présence d'un biais dans cette partie de l'étude. En effet, 29% des médecins ayant un antivirus ont été victime d'une attaque virale, contre 7% de ceux n'ayant pas de protection antivirus.

On peut émettre plusieurs hypothèses. Soit, les médecins n'ayant pas d'antivirus ont été infectés à leur insu. Soit, les médecins ayant été victime d'un virus informatique se sont équipés d'un logiciel antivirus par la suite.

La question telle qu'elle est posée ne me permet pas de conclure. Mais le fait important à retenir est qu'au moins un quart des médecins interrogés (et probablement plus) a été victime d'une attaque virale.

4.3.4 La perte de données d'origine accidentelle.

16% des généralistes de l'étude ont subi une destruction accidentelle du disque dur contenant les données concernant leurs patients. Et 14% ont déjà perdu des sauvegardes contenant des dossiers patients.

La défaillance matérielle ou liée à l'utilisateur est donc plus souvent en cause que l'origine criminelle.

Il est intéressant de souligner que 15% des médecins interrogés ont déjà été dans l'impossibilité de restaurer des données sauvegardées. Il semble donc logique de contrôler la validité des sauvegardes effectuées. Pourtant parmi ces 15%, 40% ne contrôlent jamais leurs sauvegardes et 45% le font occasionnellement. Aucun des médecins effectuant cette vérification plus régulièrement ont été dans l'impossibilité de restaurer leurs données.

4.3.5 Le ressenti des médecins interrogés.

Ces questions me permettent de sonder les généralistes ayant répondu au questionnaire pour connaître leur degré de confiance dans l'utilisation faite de l'informatique au cours de leur exercice.

Seulement 30% déclarent avoir eu des réticences lors de l'informatisation de leur cabinet médical. Et 63% ont confiance dans la protection de leurs données patients informatisées. Parallèlement, 62% des médecins interrogés pensent que leur système informatique est compatible avec le respect du secret médical. Je remarque un pourcentage élevé de non répondant à cette question (22%).

Les médecins interrogés ne semblent donc (pour une majorité) pas conscients des risques encourus.

J'ai voulu comparer la confiance des médecins avec la survenue de pertes de données informatisées mais la puissance du test effectué est insuffisante. Les résultats sont regroupés dans les tableaux 74 et 75.

	Confiance	Confiance (%)	Pas de confiance	Pas de confiance (%)	na
Pas de perte	66.00	0.73	24.00	0.27	2.00
Perte	26.00	0.65	14.00	0.35	

TAB 74 – Confiance et perte de données

	X-squared	df	p-value
grego$pertedonnees.f and grego$confiance.f	0.5704	1	0.4501

TAB 75– Confiance et perte de données - Test

4.4. Analyse critique.

Dans le cadre de ma thèse, j'ai réalisé une étude transversale, c'est-à-dire une description à un instant T d'une population donnée, à savoir un groupe de médecins généralistes libéraux installés dans le département du Val d'Oise ayant choisi de répondre à mon questionnaire.

Je me suis donc exposé aux différents biais de sélection liés à ce type d'étude.

Tout d'abord, la population interrogée n'est pas représentative de la population générale des omnipraticiens libéraux. Etant originaire du Val d'Oise et pour des raisons pratiques, j'ai choisi ce département pour mon étude.

Avant d'envoyer un questionnaire, j'ai joint par téléphone le médecin généraliste ou son secrétariat pour cibler les médecins tenant des dossiers médicaux informatisés. Ceci dans le but d'optimiser le taux de réponse au questionnaire. La population interrogée n'est donc pas randomisée.

Par ailleurs, le médecin interrogé en répondant au questionnaire induit plusieurs biais. Je suppose qu'il est intéressé par l'informatique en générale. Ou encore, il a été directement victime d'un problème informatique et cette question en particulier le concerne. Il peut tout simplement m'avoir trouvé sympathique lors du court entretien téléphonique précédant l'envoi du questionnaire.

Il a donc choisi de répondre et de renvoyer ce questionnaire pour une raison qui lui est propre et qui induit une sélection.

Il existe par ailleurs un biais de mesure. Dans ce type de questionnaire, les réponses du médecin interrogé peuvent être orientées. Il peut fournir des informations erronées ou influencées par ce qu'il suppose être la bonne réponse ou la réponse que je souhaite.

Concernant le nombre de réponses, j'ai décidé d'arrêter l'étude après avoir reçu environ 150 questionnaires. D'une part, pour des raisons pratiques il m'était difficile d'envoyer plus de 300 questionnaires. D'autre part, comme je l'ai précisé précédemment il s'agit de la description d'une population à un instant donné. Je n'avais donc pas de test à effectuer dans un premier temps. Par la suite ce choix a révélé ses limites. J'ai souhaité savoir si les médecins qui protègent plus leur ordinateur perdent moins de données. Je n'ai pas trouvé de différence. Admettons qu'elle existe, je pense que la nature transversale de l'étude et probablement le nombre trop faible de médecins interrogés ne permettrait pas de la mettre en évidence. J'ai voulu comparer la confiance des médecins avec la survenue de pertes de données informatisées. Mais la puissance du test n'était pas suffisante. J'ai ensuite isolé chaque variable à la recherche d'un facteur

protecteur pour les données informatisées. Là encore la puissance de mes tests s'est révélée insuffisante. A titre informatif, les données concernant cette dernière question sont regroupées dans le tableau 76.

Pourtant et malgré ces failles je pense avoir atteint mon objectif dans la mesure où cette étude m'a permis de faire un état des lieux relatif à la protection des données informatisées concernant les patients, au cabinet du médecin généraliste.

TAB 76– Impact des « reflexes de protection informatiques » sur la perte de données.

	N	Oui $N = 45$	Non $N = 101$	Test Statistic
mdpordi.f : Non	146	36% (16)	34% (33)	$\chi^2_1 = 0.05,\ P = 0.826$
mdplogiciel.f : Non	145	20% (9)	21% (21)	$\chi^2_1 = 0.02,\ P = 0.895$
alphanum.f : Non	118	63% (24)	50% (39)	$\chi^2_1 = 1.78,\ P = 0.182$
carac8.f : Oui	119	11% (4)	18% (14)	$\chi^2_1 = 1.02,\ P = 0.312$
Non		89% (34)	82% (65)	
NSP		0% (0)	0% (0)	
freqmodif.f : Jamais	127	95% (39)	96% (80)	$\chi^2_3 = 2.52,\ P = 0.471$
Chaque mois		0% (0)	1% (1)	
Tous les 3 mois		2% (1)	2% (2)	
Tous les 6 mois		2% (1)	0% (0)	
mememdp.f : Oui	120	49% (19)	50% (39)	$\chi^2_1 = 0.02,\ P = 0.896$
Non		51% (20)	50% (39)	
NSP		0% (0)	0% (0)	
mdpdonperso.f : Oui	123	23% (9)	28% (23)	$\chi^2_1 = 0.34,\ P = 0.562$
Non		77% (30)	72% (59)	
NSP		0% (0)	0% (0)	
postit.f : Oui	124	18% (7)	2% (2)	$\chi^2_1 = 9.23,\ P = 0.002$
Non		82% (32)	98% (80)	
NSP		0% (0)	0% (0)	
ordiveille.f : Oui	144	79% (34)	74% (72)	$\chi^2_1 = 0.38,\ P = 0.538$
Non		21% (9)	26% (25)	
NSP		0% (0)	0% (0)	
mdpapresveille.f : Oui	103	19% (6)	19% (13)	$\chi^2_1 = 0,\ P = 0.991$
Non		81% (26)	81% (56)	
NSP		0% (0)	0% (0)	
sauvegardes.f : Jamais	145	0% (0)	2% (2)	$\chi^2_3 = 1.74,\ P = 0.628$
Parfois		16% (7)	10% (10)	
Souvent		41% (18)	42% (41)	
Tous les jours		43% (19)	45% (44)	
NSP		0% (0)	0% (0)	
autresupport.f : Non	142	7% (3)	2% (2)	$\chi^2_1 = 2.01,\ P = 0.156$
essaierestau.f : Jamais	138	46% (19)	62% (58)	$\chi^2_3 = 5.48,\ P = 0.14$
Parfois		46% (19)	28% (26)	
Souvent		7% (3)	7% (7)	
Tous les jours		0% (0)	3% (3)	
NSP		0% (0)	0% (0)	
temp.f : Oui	140	59% (26)	61% (58)	$\chi^2_1 = 0.05,\ P = 0.826$
Non		41% (18)	39% (37)	
NSP		0% (0)	0% (0)	
protecordi.f : Oui	143	62% (28)	68% (67)	$\chi^2_1 = 0.44,\ P = 0.508$
Non		38% (16)	32% (32)	
NSP		0% (0)	0% (0)	
protectsauvegarde.f : Oui	142	59% (24)	61% (60)	$\chi^2_1 = 0.09,\ P = 0.768$
Non		41% (17)	39% (38)	
NSP		0% (0)	0% (0)	
sauvhorsecabinet.f : Oui	145	72% (31)	62% (61)	$\chi^2_1 = 1.44,\ P = 0.23$
Non		28% (12)	38% (38)	
NSP		0% (0)	0% (0)	
antivirus.f : Oui	144	80% (35)	80% (78)	$\chi^2_1 = 0.01,\ P = 0.905$
Non		20% (8)	20% (19)	
NSP		0% (0)	0% (0)	
majreg.f : Oui	113	74% (26)	82% (62)	$\chi^2_1 = 0.84,\ P = 0.36$
Non		26% (9)	18% (14)	
NSP		0% (0)	0% (0)	
esplogiciel.f : Oui	104	53% (17)	55% (39)	$\chi^2_1 = 0.03,\ P = 0.865$
Non		47% (15)	45% (32)	
NSP		0% (0)	0% (0)	
parefeu.f : Oui	112	65% (22)	66% (50)	$\chi^2_1 = 0.01,\ P = 0.912$
Non		35% (12)	34% (26)	
NSP		0% (0)	0% (0)	
effsecurise.f : Oui	87	24% (8)	11% (7)	$\chi^2_1 = 2.26,\ P = 0.132$
Non		76% (19)	89% (55)	
NSP		0% (0)	0% (0)	

5. CONCLUSION.

En 2008, les médecins généralistes utilisent en majorité l'informatique au cabinet et souvent pour gérer les informations concernant leurs patients. L'utilisation qu'ils en font se complète progressivement et pour beaucoup, le médecin généraliste n'est plus le néophyte qu'il était à la fin des années 90.

Les médecins interrogés sont en partie sensibilisés aux risques liés à l'utilisation de cet outil. Ils ont quelques habitudes en matière de protection informatique. Pourtant celles-ci sont insuffisantes pour assurer la sécurité et la pérennité nécessaire aux données médicales.

Alors que l'accès non autorisé aux données concernant les patients semble être un problème marginal, j'ai pu constater une réelle perte de données. Les mesures mise en œuvre pour limiter ces pertes sont incomplètes. J'ai donc élaboré à partir des informations recueillies au cours de ma thèse, une liste courte de mesures simples. Cette liste est non exhaustive mais elle est accessible au médecin libéral pour assurer une protection minimale des données concernant ses patients au cabinet.

Si celui-ci décide de faire appel à un tiers pour la gestion de son outil informatique cette liste peut servir de base à l'élaboration du contrat de maintenance.

Cette liste peut se diviser en plusieurs parties

1. La protection de l'accès aux données.
2. La protection logicielle et physique des données.

La protection de l'accès aux données.

- Ne pas laisser les informations accessibles à des tiers non autorisés en utilisant des mesures simples (un écran de veille en cas de non utilisation prolongée, orientation du moniteur vers le médecin libéral et non vers le patient).
- Protéger l'accès aux données patients par un ou des mot(s) de passe.
- Adopter des règles simples d'élaboration des mots de passe

(Utiliser des mots de passe forts).

a) De 8 caractères ou plus.

b) Alphanumériques.

c) Ne comportant pas de données personnelles.

- Adopter une politique de gestion des mots de passe

a) Utiliser un mot de passe différent pour chaque application.

b) Changer régulièrement les mots de passe.

c) Ne pas noter son mot de passe sur un support accessible à un tiers.

La protection logicielle et physique des données.

- Faire des sauvegardes régulières.
- Faire des copies de sauvegarde sur différents supports.
- Vérifier régulièrement la validité des sauvegardes effectuées.
- Conserver des copies de sauvegarde en dehors du cabinet.
- Utiliser des logiciels de protection (au moins un antivirus) et les mettre à jour régulièrement.
- Protéger son ordinateur contre la détérioration criminelle ou accidentelle.

En commençant ma thèse, une remarque m'a été faite : pourquoi faire une thèse sur la conservation des données informatiques alors que celles-ci seront entièrement dématérialisées grâce au Dossier Médical Personnel ?

Principalement parce que celui-ci rencontre de nombreux obstacles juridiques et techniques. Dans un avenir proche, le Dossier Médical Personnel sera un vecteur de changement dans les habitudes de gestion des données patients par le médecin libéral. Mais en 2009, le médecin généraliste doit toujours tenir une fiche d'observation pour chaque patient.

Le médecin généraliste reste donc le centralisateur des informations concernant ses patients et doit donc mettre en œuvre certaines mesures pour assurer la pérennité de ces données.

Résumé

Cette thèse a pour but de faire un état des lieux de la protection des données informatisées concernant les patients au cabinet du médecin généraliste. Elle est basée sur une étude transversale adressée par questionnaire à 280 médecins du Val d'Oise entre septembre et décembre 2007. 149 médecins ont répondu au questionnaire.

Les médecins interrogés possèdent des connaissances en sécurité informatiques: l'utilisation d'un mot de passe (79%), l'utilisation d'un antivirus (78%) et sa mise à jour (80%), l'élaboration de sauvegardes (99%), la copie des sauvegardes (95%).

Ces connaissance ont leurs limites et beaucoup de mesures ne sont que peu voire pas utilisées pour assurer la sécurité et la pérennité nécessaires aux données médicales : l'utilisation de mots de passe forts (1%), le renouvellement du mot de passe (4%), la vérification de la « lisibilité » des sauvegardes (40%), la conservation de copies de sauvegarde hors du cabinet (67%), l'utilisation d'autres logiciels de protection, la protection contre le vol (64%).

Or, la perte de données et le risque informatique sont réels : 31% des médecins interrogés ont perdu des données et 24% ont été victimes d'un virus informatique. Et malgré ces chiffres 63% ont confiance dans la protection de leur système informatique.

J'ai donc élaboré à partir des informations recueillies au cours de ma thèse, une liste courte de mesures simples permettant de renforcer la protection des données concernant les patients au cabinet du généraliste.

Mots-clefs

Médecine générale, informatisation, dossier médical, sécurité informatique.

Références bibliographiques

- (1) Questions sur l'informatisation des dossiers médicaux le partage et l'hébergement des données. Rapport de la commission nationale permanente adopté lors des assises du conseil national de l'ordre des médecins du 18 juin 2005. Dr Jean-Marie Faroudja (rapporteur) Drs Monique Carton, Maurice Bernard-Catinat, Jacques Lucas, Jean-Francois Rault.
- (2) Informatisation des cabinets de médecine générale dans les Hauts-de-Seine avril-mai 2001 (état actuel et perspectives) thèse pour le doctorat en médecine du Dr Goretzky Boris Alexandrovitch.
- (3) Baromètre des pratiques en médecine libérale. Synthèse des résultats « l'informatisation du cabinet médical ». Janvier 2004. Projet financé par le FAQSV et l'URML-Bretagne.
- (4) L'apport de l'informatique dans la pratique libérale. Etude FORMMEL 2000. Paul Gourgnon, Nathalie Grandfils, Marie-Jo Sourty-Le Guellec, Maria Zimina.
- (5) Le site du service public de la diffusion du droit http://www.legifrance.gouv.fr/ consultation du 20 janvier 2008.
- (6) Le site de l'assurance maladie : www.ameli.fr consultation du 20 décembre 2007.
- (7) Ordre national des médecins. Démographie médicale française. Situation au 1er janvier 2006. juin 2006. Étude N° 39.
- (8) Le site du GIE Sesam-Vitale : www.sesam-vitale.fr/ consultation du 7 décembre 2007.
- (9) Ipsos Santé GIP DMP – le DMP et les médecins – Novembre 2007.
- (10) Guide pratique de sécurité informatique, Auteur: Bruno Favre et Pierre-Alain Goupille, Edition: Dunod, Date de parution : septembre 2005.
- (11) Le dossier médical, Auteur : Olivier Dupuy, Editeur : Les Études hospitalières, Date de parution : 2002.

- (12) Le secret médical face à l'informatisation de la médecine de ville. Mémoire de DESS droit du multimédia et de l'informatique. université panthéon Assas paris II (Isabelle Eray sous la direction de Me Nathalie Mallet-Poudjol).
- (13) Le site du Conseil National de l'Ordre des Médecins http://www.conseil-national.medecin.fr/?url=deonto/rubrique.php consultation du 15 janvier 2008
- (14) Le site de la Commission Nationale de l'Informatique et des Libertés www.cnil.fr consultation du 10 décembre 2007.
- (15) Le site de la Haute Autorité de Santé http://www.has-sante.fr/portail/jcms/j_5/accueil consultation du 15 janvier 2008.
- (16) Le site de l'encyclopédie libre Wikipédia http://en.wikipedia.org/wiki/PEBKAC consultation du 10 décembre 2007
- (17) International Standard ISO/IEC 17799. second edition 2005-06-15. Information technology – security techniques – code of practice for information security management.
- (18) Guide juridique du dossier médical informatisé, Date de parution : juin 2001, Auteur : A Bensoussan, Editeur : Masson.
- (19) Le site du Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques http://www.certa.ssi.gouv.fr/ consultation du 10 janvier 2008 (référence CERTA-2005-inf-001).
- (20) Le site du portail de la sécurité informatique : http://www.securite-informatique.gouv.fr/ consultation du 7 décembre 2007 en particulier l'article http://www.securite-informatique.gouv.fr/gp_article95.html

A titre informatique sont indiqués d'autres sources qui m'ont été utiles dans l'élaboration de ma thèse :

- Le site www.secuser.com sur la sécurité informatique et la protection de la vie privée consultation du 15 décembre 2007.
- Le site du Club de la Sécurité Informatique Français : www.clussif.asso.fr consultation du 10 décembre 2007.

- Le site http://www.securiteinfo.com sur la sécurité informatique et la sécurité des informations consultation du 20 janvier 2008
- Le site du groupement d'intérêt public dossier médical personnel : www.d-m-p.org consultation du 15 décembre 2007.

Vu :

Le Président de Thèse
Faculté Paris 7
le Professeur BERGMANN

Vu :

Le Doyen de la Faculté de
Médecine Paris 7 - Denis Diderot
Monsieur le Professeur
Benoît SCHLEMMER

Vu et Permis d'Imprimer
Pour le Président de l'Université Paris 7 - Denis Diderot
Et par délégation

Le Doyen

Benoît SCHLEMMER