

UNIVERSITE DE LILLE
FACULTE DE MEDECINE HENRI WAREMBOURG
Année 2023

THESE POUR LE DIPLOME D'ÉTAT
DE DOCTEUR EN MEDECINE

**Évaluation de la sécurisation des données de santé de la
Messagerie Instantanée Interprofessionnelle Predice PRO :
comparaison entre les médecins généralistes utilisateurs
et non utilisateurs des Hauts-de-France.**

Présentée et soutenue publiquement le 02/02/2023 à 18h00 au
Pôle Recherche

Par SAFIYA GUEFIF

JURY

Président :

Monsieur le Professeur Marc HAZZAN

Asseseurs :

Monsieur le Docteur Nassir MESSAADI

Directeur de thèse :

Madame le Docteur Isabelle BODEIN

Avertissement

La Faculté n'entend donner aucune approbation aux opinions émises dans les thèses : celles-ci sont propres à leurs auteurs.

Remerciements

A mon Président de jury,

Monsieur le Professeur Marc HAZZAN

*Doyen de la faculté de médecine Henri Warembourg et Professeur des Universités
Faculté de Médecine Henri Warembourg,
Université de Lille*

*Praticien Hospitalier
Chef de service de Néphrologie, Dialyse et Transplantation,
CHU de Lille, Hôpital Claude Huriez*

Vous me faites un immense honneur de juger mon travail et de présider le jury de cette thèse. Veuillez trouver ici la marque de ma gratitude et de ma profonde reconnaissance.

A mon Juge,

Monsieur le Docteur Nassir MESSAADI

*Maître de conférence des Universités
Coordonnateur du DES de Médecine Générale,
Faculté de Médecine Henri Warembourg,
Université de Lille*

*Praticien libéral
Cabinet de Médecine Générale à Lille*

Vous me faites l'honneur de juger ce travail et je vous en remercie. L'internat de médecine générale fait partie des plus belles années de ma vie, notamment grâce à votre contribution en tant que coordonnateur, soyez assuré de mon profond respect.

A ma directrice de Thèse,

Madame le Docteur Isabelle BODEIN

*Maître de stage des Universités,
Faculté de Médecine Henri Warembourg,
Université de Lille*

*Praticien Libéral,
Cabinet de Médecine Générale à Cassel*

Nous avons partagé de précieux moments lors des groupes d'échanges de pratique de médecine générale. J'en ai tiré une profonde leçon de vie, et un exemple de carrière à suivre. Votre sympathie, votre disponibilité et votre professionnalisme m'ont marqué. C'est un honneur d'avoir pu travailler à vos côtés.

Je vous remercie et vous prie de croire en l'assurance de tous mes respects.

Je tiens également à exprimer ma reconnaissance :

A Monsieur le Professeur Emmanuel CHAZARD,

PU-PH de Biostatistique et Informatique Médicale

À l'Université de Lille et au CHU de Lille,

Pour les supports d'aide à la préparation d'une thèse de médecine.

A Monsieur le Docteur Luc DUSSART et le Docteur Florent LEFRANC,

Maîtres de Stage Universitaire de la faculté de médecine de Lille,

Pour ce qu'ils m'ont apporté durant mon stage de phase socle du DES de Médecine générale. Un stage qui m'a émerveillé et m'a confirmé dès les premières semaines que j'avais fait le bon choix de spécialité.

A mes parents,

Papa, Maman je vous aime de tout mon cœur, aucun mot n'est assez fort pour décrire la reconnaissance que j'ai pour vous. J'ai eu la meilleure des enfances grâce à vous, je suis fière de l'éducation que vous nous avez octroyé ainsi que tous vos sacrifices. Je tiens ma ténacité et mon sens de l'effort de mon père qui a travaillé toute sa vie pour notre bien-être et notre éducation, qui a toujours été présent pour nous et sur qui je pourrais toujours compter. Je tiens ma bienveillance et mon sacrifice pour les autres de ma mère, qui s'est sacrifié toute sa vie pour notre bien-être, qui tire son bonheur de celui des autres, j'espère devenir une mère aussi parfaite que toi qui m'a soutenue dans toutes les épreuves de ma vie, tu souffres quand on souffre, tu es heureuse quand on est heureuse, il n'y a pas plus miséricordieux qu'une mère et un père, et notamment une mère et un père comme vous. Vous méritez les plus beaux jardins et les plus beaux habits du paradis, je vous aime. Je porterais avec fierté ce titre de Docteur GUEFIF en rendant honneur à ma famille et au nom de mon père.

A Anas, mon époux,

A celui pour qui j'ai le plus de respect et d'admiration, le meilleur des anesth-réa. Tu es le plus attentionnée des maris, tu lis en moi comme dans un livre ouvert, tu me connais mieux que moi-même. Rien pour moi n'est plus important sur terre que ton amour et ton soutien. Lorsque je ferme les yeux je te vois et lorsque j'ouvre les yeux je veux te voir, tu me manques à chaque instant, chaque battement de mon cœur te réclame. Je t'aimerais toute ma vie Anas, je t'aimerais en mourant et même après.

A ma sœur Sanah, et mes frères Ibrahim et Jounaid,

*Je suis fière d'être votre sœur, nous avons eu la meilleure enfance ensemble. **Sanah** qui a toujours été mon exemple de femme, ton mari Karim et toi avaient toujours été là pour moi durant ses difficiles années en tant qu'étudiante en médecine, rien n'est plus important pour moi que d'avoir une sœur aussi courageuse et aimante, rien n'est plus important de voir la fierté dans tes yeux, tu resteras un pilier essentiel à mon bien-être. **Ibrahim** ta bienveillance, ta force et ton courage me rendent fier de toi, ta bienveillance envers les gens est un exemple à suivre. **Jounaid**, ta résilience et ton courage force le respect, ta persévérance et ta bonté me rendent également fière de toi. Vous méritez tous les trois le meilleur, je serai toujours là pour vous. A travers les sourires et les larmes, on ne se séparera jamais.*

A toute ma famille et notamment,

*Mes tantes **Rachida et Farida**, à mon oncle bien aimé **Ahmed**, mes autres mamans et mon deuxième papa, vous êtes un exemple de courage, vous rassemblez la famille et veillez à son bien-être. **A mes autres oncles et tantes AbdAllah, Hassen, Nadia et leurs enfants**, pour qui j'ai le plus profond respect, votre vie est une source inépuisable de valeurs qui resteront ancrées en moi pour toujours. **Au reste de ma famille que j'aime et qui pourront toujours compter sur moi.***

A mes cousins et cousines Maymana, Imane, Idayette, Wissem, Ismaël, et leurs enfants Zakarya et Souleymane,

Nous avons vécu une des plus belles enfances, une enfance merveilleuse, des souvenirs à n'en plus finir. Je serais toujours là pour vous, je vous aime. Vous avez contribué à mon éducation et la construction de mes valeurs, et vous y contribuez à chaque instant.

A ma belle-famille, mes beaux-parents, mes beaux-frères et belles-sœurs Kadija et Hanane, à leurs enfants Mariam et Ilyes,

Je n'aurais pu rêver meilleure belle famille, je vous aime autant que mes parents, que mes frères et sœurs. Je suis fière de faire partie intégrante de votre famille. J'espère être à la hauteur de l'amour et du soutien que vous me portez, et de toute la bienveillance dont vous faites preuve à mon égard.

A ma plus ancienne et précieuse amie Chahrazad avec qui j'ai eu l'honneur de passer les obstacles de la première année de médecine, du concours de l'internat et avec qui j'ai réalisé ma thèse, nous allons clôturer nos études en passant notre soutenance ensemble, qui je l'espère sera l'un des plus beaux souvenirs de notre vie. Tu es l'une des personnes les plus courageuse et vaillante que je connaisse, et je suis fière de notre amitié ainsi que de celle de nos maris. A notre trio ECN 2020 avec **Malak, le redoublement de ma cinquième année aura été l'une des épreuves les plus bénéfiques me permettant de passer ce concours en compagnie de bienveillance, d'entraide et beaucoup de rigolade.**

A mon groupe de sœurs, mon groupe d'assise : tout d'abord ma **Scherazade qui est l'une des plus belles rencontres de ma vie, **Millicent, Adjila, Yasmina et ses filles Soundousse, Naysam, Assia et Nayla, Hafida, Fatema, Louisa, Khadija** et toutes les sœurs que j'ai pu rencontrer : vous êtes des trésors, qui me poussent vers le bien. Bien plus qu'une équipe, une famille, aux **Professeurs** ayant profondément modifiés mon existence, pour qui j'ai le plus grand respect et pour qui j'invoquerai toute ma vie.**

A toutes les personnes rencontrées durant l'internat et l'externat, camarades et médecins :

Merci à tous pour vos enseignements, votre bienveillance, votre professionnalisme. Chaque stage réalisé a été une source précieuse d'apprentissage, j'espère avoir eu un rôle dans le flambeau que l'on se passe de main en main grâce au compagnonnage, avec force et honneur, et pour le bien de nos patients.

Sigles

ARS	Agence Régionale de Santé
ADELI	Répertoire national d'identification des professionnels de santé
ANS	Agence du Numérique en Santé (ex-ASIP)
ASIP	Agence des Systèmes d'Information Partagé de Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ApCV	Application Carte Vitale
AWS	<i>Amazon Web Service</i>
BE	<i>Benefits Evaluation</i>
CNIL	Commission Nationale de l'Informatique et des Libertés
CISS	Collectif Inter-associatif Sur la Santé
CPS	Carte de Professionnel de Santé
DGOS	Direction Générale de l'Offre de Soins
DNS	<i>Domain Name System</i>
DPO	Délégué à la Protection des Données
DMP	Dossier Médical Partagé
eCPS	Carte de Professionnel de Santé électronique
eHealth	Santé numérique, (synonyme e-Santé)
e-SS	Score e-Santé Sécurité
FSN	Fournisseur de Service Numérique
GHT	Groupements Hospitaliers de Territoire
GDPR	<i>General Data Protection Regulation (Europe)</i>
iEHR	<i>interoperability of Electronic Health Records</i>
HIPAA	<i>Health Insurance Portability and Accountability Act (Etats-Unis)</i>
HOP'EN	Programme Hôpital Numérique Ouvert sur son Environnement

MSU	Maître de Stage Universitaire
NEHR	<i>National Electronic Health Record (Singapoure)</i>
NIS	<i>Network Information Service (Europe)</i>
NIR	Numéro d'Inscription au Répertoire des personnes physiques (synonyme : numéro de sécurité sociale)
OSE	Opérateur de Service Public ou Privé
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
PGSSIS	Politique Générale de Sécurité des Systèmes d'Information de Santé
PMSI	Programme de Médicalisation des Systèmes d'Information
PSSI	Politique de Sécurité du Système d'Information
PIS	<i>Political Information System</i>
SASPAS	Stage Ambulatoire en Soins Primaires en Autonomie Supervisée
Score e-SS	Score e-Santé Sécurité (e pour numérique)
SIE	Système d'information Essentielle
SUNES	Segur de l'Usage Numérique en Établissement de Santé
SONS	Système Ouvert et Non Sélectif
URPS ML HDF	Union Régionale des Professionnels de Santé Médecins Libéraux Hauts-De-France
ZAR	Zone d'Accompagnement Régional
ZAC	Zone d'Action Complémentaire
ZIP	Zone d'Intervention prioritaire

Sommaire

Table des matières

AVERTISSEMENT	3
REMERCIEMENTS	4
SIGLES	10
SOMMAIRE	13
INTRODUCTION GENERALE	16
1. LE VIRAGE NUMERIQUE EN SANTE	16
a) À l'international	16
b) En France	17
2. LES DANGERS DU NUMERIQUE	18
a) Danger externe : la cybercriminalité	18
b) Danger interne : la fuite des données et les obligations des professionnels de santé	19
c) Aspect légal	20
3. ASPECT REGLEMENTAIRE DE LA SECURISATION DES DONNEES	21
a) Les instances européennes et françaises garantissant la sécurisation du partage de données-patient	21
Le GDPR européen et les directives européennes NIS	21
La réglementation française :	21
L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et le Référentiel Général de Sécurité (RGS)	22
Mise en place du Règlement Général de la Protection des Données (RGPD)	23
La Commission Nationale de l'Informatique et des Libertés CNIL	23
b) Les grands principes de la sécurité des données	23
c) Les notions à comprendre dans le domaine de la sécurité	24
Savoir identifier les individus qui communiquent : l'identitovigilance	24
Comment se connecter à ses applications : l'authentification	24
Comment est définie la communauté professionnelle et qu'est-ce que l'Interopérabilité ?	25
Savoir protéger les données des patients à travers l'hébergement, le chiffrement et le cloisonnement des accès aux données	26
Désigner un responsable des données qui déclare les incidents : le délégué à la protection des personnes (DPO)	28
Recueillir le consentement du patient	29
L'interdiction de la vente de données	30
4. CREATION DE SERVICES SOCLES	30
a) Messagerie électronique sécurisée MSSANTÉ :	30
b) MON ESPACE SANTÉ : est un dossier médical partagé, espace d'interopérabilité entre les professionnels de santé, permettant de renforcer le lien ville-hôpital	31
c) L'agenda électronique sécurisé	31
d) Les logiciels de prescription électronique	31
e) Logiciel-métier pour les dossiers-patient	32
f) Service de téléconsultation sécurisé	32
g) Dispositif de télé médecine	32
h) Messagerie instantanée sécurisée	33
5. LES DIFFERENTS MOYENS DE COMMUNICATION EN SANTE DANS LA LITTERATURE	33
6. OBJET DE L'ETUDE : PREDICE PRO	35
Déroulement du projet Predice PRO	35
Présentation du service	35
Description du niveau de sécurité du système	36
INTRODUCTION	37
MATERIEL ET METHODES	38
1. TYPE D'ETUDE, OBJECTIFS ET CRITERES DE JUGEMENT	38

a) Critère principal d'intérêt : le Score e-Santé Sécurité.....	38
b) Critères de jugement.....	39
Le critère de jugement principal.....	39
Les critères de jugement secondaires.....	39
d) Population.....	39
Méthode de recrutement.....	39
Critères d'inclusion.....	40
Critères de non-inclusion.....	41
1. RECUEIL DE DONNEES.....	41
a) Données recueillies.....	41
b) Modalités du recueil.....	41
2. ANALYSE DE DONNEES : NOM DES VARIABLES.....	42
a) Variables d'intérêts.....	42
b) Critères d'exposition.....	43
3. ANALYSE STATISTIQUE : LES METHODES UTILISEES.....	43
a) Analyse bivariée et comparaison de moyenne.....	43
Comparaison de moyenne.....	43
Analyse bivariée.....	44
Analyses multivariées.....	44
4. SIGNIFICATIVITE.....	45
5. CADRE REGLEMENTAIRE.....	45
RESULTATS.....	46
1. DIAGRAMME DE FLUX.....	46
2. DESCRIPTION DES PATIENTS A L'INCLUSION.....	47
3. OBJECTIF PRINCIPAL : SCORE E-SANTE SECURITE DES UTILISATEURS DE PREDICE PRO ET DES NON-UTILISATEURS	49
4. PREMIER OBJECTIF SECONDAIRE : SCORE E-SANTE SECURITE DES MOYENS DE COMMUNICATION SECURISES ET NON-	50
SECURISES.....	50
5. DEUXIEME OBJECTIF SECONDAIRE : SCORE E-SANTE SECURITE DES MOYENS DE COMMUNICATION SECURISES.....	51
6. TROISIEME OBJECTIF SECONDAIRE : ANALYSE BIVARIEE ET MULTIVARIEE : FACTEURS PREDICTIFS DU MOYEN DE	52
COMMUNICATION SECURISEE OU NON.....	52
DISCUSSION.....	55
1. ANALYSE DES RESULTATS.....	55
a) Critère de jugement principal.....	55
b) Critères de jugement secondaires.....	55
c) Données de la littérature.....	56
2. DISCUSSION DE LA METHODE ET SIGNIFICATIVITE CLINIQUE.....	58
a) Points forts de l'étude.....	58
b) Points faibles de la méthode.....	59
Biais de sélection :.....	59
Biais de déclaration :.....	59
Faible taux de réponse :.....	60
c) Conflit d'intérêt :.....	60
3. PERSPECTIVES.....	60
a) Vers l'application des autres propositions de l'Ordre des médecins (2).....	60
b) Vers la standardisation des règles que doivent suivre les éditeurs.....	61
c) Vers le consentement des patients au travers des échanges entre professionnels sur les	62
messageries instantanées.....	62
d) Vers la programmation de nouvelles fonctionnalités sur Predice PRO.....	62
e) Vers la formation des médecins dans le Numérique en Santé :.....	63
f) Vers l'incitation financière pour les médecins généralistes.....	63
g) Vers l'acceptation des contraintes de sécurité.....	64
CONCLUSION.....	65
REFERENCES.....	66
ANNEXES.....	69

Introduction générale

1. Le Virage Numérique en Santé

a) À l'international

La transformation numérique du système de soin est une innovation internationale. La démocratisation du service Internet depuis les années 90 a été rapidement mise à profit par les systèmes de santé. Différents comités de professionnels de santé témoignent de cet intérêt nouveau qui a été mis à leur service.

En Ecosse, *Bouamrane et al*, ont effectué une étude qualitative avec entretien semi structuré de médecins généralistes concernant les perspectives de la télémédecine : la majorité considère que le système électronique fait partie intégrante et est un élément essentiel de leur travail durant la consultation, qu'il a un rôle clef dans la continuité des soins, et l'accessibilité aux informations de santé (7, 25).

A Singapour, dans son étude transversale, *Qin Yong* a interrogé des médecins généralistes utilisant le NEHR qui est un système sécurisé de collecte de données-patient entre plusieurs professionnels. La majorité de ses médecins en tiraient un bénéfice dans leur pratique (8).

Aux Etats-Unis, la qualité et l'efficacité de la e-santé semblent indispensables dans la pratique des jeunes médecins, mais un besoin émerge : sa standardisation (10).

Au Canada et aux Pays-Bas, une revue de la littérature nous informe que l'intégration des technologies de e-santé dans le secteur médical permet d'innover et d'améliorer le soin dans sa globalité. Cela requiert l'implémentation dans le secteur de la santé de nouveaux outils et concepts (26).

En Nouvelle-Zélande, une étude cross-over recueille l'avis de 400 patients, la majorité étant en faveur du développement de la e-santé. Ils soulèvent la nécessaire limitation de cette innovation par les besoins de confidentialité et norme de sécurité. Leur principale préoccupation était l'émergence de possibles agressions externes (27).

b) En France

Lors du SEGUR de la santé, l'Agence nationale de la santé a annoncé un budget de 6 milliards d'euros, dont un tiers concerne le **SEBUR du Numérique en Santé** : il s'agit d'un engagement collectif afin d'accélérer le virage numérique (11).

L'objectif est le financement et la promotion de l'informatisation des professionnels. L'échange de 250 millions de documents médicaux est prévu d'ici 2023.

Le gouvernement et son financement, l'inscription dans l'économie mondiale, le regard de la société, sont des facteurs permettant une standardisation des pratiques médicales. Leur influence directe permet une organisation saine des différents outils de e-santé (Annexe 1).

Pour répondre à ces problématiques, le ministère de la santé a su mettre en place différents programmes :

- Les Groupements Hospitaliers de Territoire (**GHT**) qui sont un mode de coordination entre établissements de santé, avec en premier lieu, **SUN-ES**, qui est le prolongement du programme **HOP'EN** permettant les échanges de données-patient entre établissements (11).
- **MonEspaceSanté** (nouveau Dossier Médical Partagé) grâce à un budget de 210 millions d'euros. Il est initié pour chaque patient par les établissements hospitaliers.
- Le référencement **SONS** (Système Ouvert et Non Sélectif) qui permet le financement des industriels impliqués. En effet ce sont des éditeurs de solutions logicielles qui vont permettre le partage de données-patient tout en respectant les exigences de l'Agence Nationale de la Santé.

Dans son livre blanc, le **Conseil National de l'Ordre des Médecins** préconise que la déontologie médicale s'applique au vecteur d'information qu'est Internet. On voit donc que l'expansion rapide de cet outil a fait naître une réponse de la part des instances médicales.

Concernant l'activité libérale, le maintien de la sécurité des données dans la coopération entre professionnels de santé doit être couvert, tout en soutenant les médecins généralistes dans l'informatisation de leur exercice, notamment d'un point de vue financier (2).

Ainsi, l'*Avenant 9 à la convention médicale* a été signé entre l'**Assurance Maladie** et les représentants des **médecins libéraux**. Il permet le financement de ces logiciels, conditionné par l'alimentation de *MonEspaceSanté*, notamment dans le volet « synthèse médicale », par l'utilisation d'une messagerie de santé sécurisée, et par l'usage de la prescription dématérialisée (*l'Arrêté L1111-15 du Code de Santé Publique*).

2. Les dangers du numérique

a) Danger externe : la cybercriminalité

Le coût de la cybercriminalité est estimé dans le monde à plus de 575 billions de dollars en 2021, il s'agit d'un nouveau fléau international (9).

Selon l'ANSSI, le nombre de cyber-attaques a été multiplié par 4 en 2020. Cela peut s'expliquer d'une part par l'augmentation des signalements, mais également par le contexte de crise sanitaire.

Le site du gouvernement *cybermalveillance.gouv.fr* a vu ses demandes d'assistance technique augmenter considérablement. Plusieurs professionnels se sont vus pirater leur compte avec demande de rançon, après de multiples tentatives d'hameçonnage. Dans ce cadre, les faux supports techniques, l'usurpation d'identité, et les violations de données sont les motifs les plus fréquents de demande d'assistance.

Durant l'été 2022, un hôpital d'Ile-de-France a été la cible de hackers exigeant une rançon de 10 millions d'euros après avoir vu son système informatique totalement paralysé.

Dans un communiqué de presse, l'hôpital de l'Essonne précise

Tous les logiciels métiers de l'hôpital, les systèmes de stockage et le système d'information ayant trait aux admissions de la patientèle étaient inaccessibles.

Ces attaques obligent les établissements de santé à devoir recourir au dossier médical papier, voire poussent à la nécessité d'adresser leurs patients à d'autres hôpitaux, désorganisant ainsi toute la prise en charge médicale. Cela est source d'erreurs et de perte de chance pour les patients.

Les établissements de santé sont évidemment une cible privilégiée des pirates au vu des problématiques engendrées et de leurs nécessités à assurer un service continu, ainsi, les "rançongiciel" peuvent avoir des conséquences lourdes sur la coordination des soins.

Au-delà de ces risques extérieurs, des problématiques internes voient aussi le jour.

b) Danger interne : la fuite des données et les obligations des professionnels de santé

Deux praticiens ont été sanctionnés d'une amende de 6.000 euros après avoir partagé des comptes-rendus d'imagerie de leur patient dans l'espace Web. Cela constitue une violation concernant le traitement des données personnelles.

Légifrance a rendu sa la délibération *SAN 2020-014 du 7 décembre 2020* : une erreur de paramétrage a permis le libre accès à un serveur informatique d'images médicales avec présence de l'identification des patients (nom, prénom, date de naissance et de consultation). L'aspect technique caractérisant cet accès non protégé est spécifié dans les deux délibérations de la CNIL (34).

Malgré l'absence de volonté des médecins libéraux de laisser un libre accès en ligne de ces images, la violation n'était que la conséquence d'un raccord de leurs **disque dur externe** à leurs box Internet.

Une absence de paramétrage de l'accès au réseau Internet, ainsi qu'une **absence de données cryptées** a permis un manque de protection des données-patients.

Dans ce rapport Légifrance a été spécifié :

De même, le Guide pratique pour les médecins, publié par la CNIL en concertation avec le Conseil national de l'ordre des médecins, invite les médecins à limiter le plus possible la connexion d'appareils non professionnels sur le réseau au sein duquel sont traitées les données des

patients, ainsi qu'à recourir à des moyens d'authentification forte pour accéder à ce réseau.

Une vigilance particulière doit être mise en place afin d'éviter la violation des données médicales. La nécessité d'une **assurance** en responsabilité civile concernant les actes de télémédecine est également à la charge du praticien.

Il est probablement préférable pour les médecins généralistes d'effectuer un **contrat de sous-traitance**, qui est à étudier attentivement afin de vérifier le respect des obligations CNIL et du RGPD. Il en vient de sa responsabilité, sous peine de sanction comme nous venons de le voir (36, 37).

c) Aspect légal

Dans l'article 226-17 du code pénal

*L'absence de **déploiement de mesures de sécurités techniques** ou la négligence sont sanctionnées, en tant qu'atteinte à la vie privée de 5 ans d'emprisonnement et 300 000 euros d'amende.*

Dans l'article 226-22 du code pénal

*L'atteinte à la **confidentialité des données**, à une personne non autorisée est punie de 5 ans de prison et 300 000 euros d'amende, en cas de divulgation par imprudence ou négligence cela est puni de 3 ans de prison et 100 000 euros d'amende.*

Selon les règles préconisées par le Conseil d'Etat,

*Concernant l'**échange de données entre professionnels**, la garantie de la confidentialité des informations médicales est assurée en soumettant les systèmes de conservation sur support informatique et de transmission par voie électronique. Les mesures à respecter sont définies par le décret après avis de la CNIL.*

Dans l'article L1110-4 CSP :

*Le fait de **tenter d'obtenir la communication de ces données** en violation de cette disposition est puni d'un an d'emprisonnement et 15 000 euros d'amende.*

Le médecin est donc un acteur de la sécurité des données-patient. Il se doit d'analyser les risques internes et externes, de les prévoir et enfin de réguler son activité sur un modèle prédéfini par le Règlement Général de la Protection des Données (RGPD).

3. Aspect Réglementaire de la sécurisation des données

La sécurisation des moyens d'échanges interprofessionnels apparaît essentielle afin de ne pas méconnaître une faille au secret médical dans l'espace Web.

De la sécurisation des données médicales hospitalières s'ensuit la sécurisation des données médicales libérales notamment à travers les logiciels patients, les messageries électroniques ainsi que les messageries instantanées (1).

Plusieurs instances permettent d'ériger un cadre légal à cette sécurisation.

a) Les instances européennes et françaises garantissant la sécurisation du partage de données-patient

Le GDPR européen et les directives européennes NIS

La défense du droit à la vie privée est régie par trois institutions primordiales : le Parlement Européen, le Conseil de l'Europe, et la Commission Européenne.

La directive *Network and Information Security (NIS)* a été mise en place le 6 juillet 2016 par le Parlement Européen et le Conseil de l'Union Européenne.

Les 4 thématiques de la directive NIS sont la Gouvernance, la Protection, la Défense, et la Résilience.

Plusieurs supports ont été alors rédigés pour les professionnels de santé européens notamment un guide concernant l'identité digitale : les *Digital Identity Guidelines* (24), ainsi qu'un référentiel de sécurité : le *GDPR (General Data Protection Regulation)*.

La Cybersécurité devient un intérêt national, et concerne les opérateurs de service public ou privé.

La réglementation française :

L'ANS, anciennement *Agence des systèmes d'informations partagées de santé* (ASIP-Santé), est une agence gouvernementale française chargée de la santé numérique.

Le GIP Sant&Numérique Hauts-de-France s'est vu confier **par l'ARS** le programme régional de développement de la e-Santé. Cette transformation numérique du champ sanitaire est un enjeu national. L'ARS veille à la répartition équitable de l'offre de soin sur tout le territoire des Hauts-de-France (HDF).

L'Union régionale des professionnels de santé médecins libéraux des Hauts-de-France (**URPS-ML-HDF**) permet d'organiser l'exercice libéral au niveau régional afin d'accompagner les médecins généralistes dans leur transformation digitale.

A travers sa Politique Générale de Sécurité en Santé (**PGSSIS**), l'ANS permet la rédaction de chartes permettant l'analyse des risques résiduels concernant l'accès aux données, et l'identification des systèmes d'information.

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et le Référentiel Général de Sécurité (RGS)

L'ANSSI constitue une cellule de crise qui peut être saisie lors de cyberattaques. Elle recueille les signalements d'incident afin de pouvoir les limiter dans l'avenir.

Elle effectue des contrôles de prestataire de service afin de vérifier le respect des obligations notamment la sécurité des réseaux et des systèmes d'information, en cas de manquement la sanction est une amende pouvant s'élever à 125 000 euros.

Le RGS est le cadre réglementaire permettant les échanges entre professionnels de santé. Il permet notamment d'assurer la confiance des citoyens.

Le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 :

Permet la création d'un référentiel général de sécurité relatif aux échanges électroniques entre les usagers et les autorités administratives. Dans le cadre du développement des téléservices et des échanges électroniques entre l'administration et les usagers, les autorités administratives doivent garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de ces services.

Mise en place du Règlement Général de la Protection des Données (RGPD)

Plusieurs principes sont essentiels et caractérisent le devoir du médecin : la transparence, le consentement explicite du patient, l'analyse des risques et impacts, la notification en cas de violation des données.

L'article 5 du RGPD, préconise que le partage de données doit :

- Être licite loyal et transparent,*
- Avoir une finalité déterminée explicite et légitime,*
- Avoir des données adéquates pertinentes et limitées,*
- Respecter la minimisation des données,*
- Respecter l'exactitude des données et leur mise à jour,*
- Définir une durée de conservation,*
- Protéger les données par les moyens énoncés dans le guide pratique de la CNIL.*

La Commission Nationale de l'Informatique et des Libertés CNIL

C'est une commission qui traite des réclamations ou violation du règlement RGPD, elle est chargée de veiller au respect des règles qui sont annoncées dans ce règlement. Elle permet ainsi l'application de *l'article 25-II de la loi informatique et liberté (14)*.

b) Les grands principes de la sécurité des données

Il existe quatre principes de base des systèmes d'informations : la disponibilité, la traçabilité, la confidentialité, et enfin l'intégrité. Ce sont les **critères DICP** qui permettent la classification de l'informatisation concernant les échanges de données :

-Disponibilité : implique un accès rapide et permanent, avec une accessibilité sans faille aux données. Pour cela, une mise à jour des hébergeurs de données médicales est nécessaire. Cela implique aussi un fonctionnement en zone blanche (en l'absence de réseau) c'est-à-dire à l'aide d'un mode asynchrone.

-Traçabilité : permet de tracer l'identité de l'accédant, permettant la continuité du suivi en toute conformité.

-Intégrité : Les données doivent être exactes et complètes, avec une confiance en l'authenticité du système.

-Confidentialité : Seules les personnes autorisées peuvent avoir accès au système, en évitant tout accès indésirable.

Tout cela permet d'éviter les risques de vol de données, d'intrusion, de négligence, de cybercriminalité, de sabotage, d'erreurs de paramétrage...

De ses grands principes, les autorités ont déduit de multiples notions, qui sont indispensables à appréhender.

c) Les notions à comprendre dans le domaine de la sécurité

Savoir identifier les individus qui communiquent : l'identitovigilance

L'identité doit pouvoir être certaine sans risque d'erreur médicale. Cela est possible grâce à l'INR ou **NIR** : Numéro d'Inscription au Répertoire des personnes physiques. Il correspond au numéro de sécurité sociale.

L'identification des professionnels de santé a lieu via la **carte CPS ou e-CPS** (carte dématérialisée), le **numéro RPPS ou ADELI** (pour les autres professionnels de santé)

L'Article L. 1111-8-1 CSP à travers le Décret n° 2017-412 du 27 mars 2017 préconise l'utilisation du NIR pour l'identification des dossiers patients notamment en médecine générale à travers les logiciels patients. Il s'agit d'un identifiant national de sécurité.

Comment se connecter à ses applications : l'authentification

Il est nécessaire d'utiliser un mot de passe fort utilisant chiffres, lettres majuscules et minuscules, caractères spéciaux, avec 12 caractères minimum.

La **caractéristique OTP** (*One Time Password*) est aussi indispensable : c'est une authentification à double facteur c'est-à-dire qu'une réception d'un code SMS ou email permet de valider l'identifiant et le mot de passe utile à la connexion.

L'authentification devient très forte si elle est effectuée via **une carte CPS ou eCPS**. La eCPS est une version dématérialisée de la carte CPS, elle n'est pas encore développée dans le secteur de la e-santé car des difficultés d'utilisation émergent. Les codes de validation de cette carte sont habituellement envoyés par voie postale (courrier recommandé).

Selon la CNIL, la nécessité d'un **verrouillage automatique** en cas de non-utilisation au bout de 30 minutes est recommandé.

Elle recommande également l'installation de **pare-feu**, la **sécurisation du réseau** internet, la mise en place d'**antivirus** et leurs mises à jour régulières.

Concernant **l'outil informatique** en tant que tel, l'utilisation d'un appareil professionnel est recommandée afin de séparer l'activité de soin de la vie personnelle et ainsi éviter les erreurs. Leur accès doit être sécurisé également (par un code ou un schéma d'ouverture du téléphone par exemple).

L'accès au logiciel de santé via le téléphone ou l'ordinateur professionnel doit aussi être sécurisé : c'est la sécurisation du **double accès**.

Des précautions doivent être prises lors de la consultation du logiciel ou de la messagerie : il doit avoir lieu en l'absence d'individus n'appartenant pas au cercle de soin. Il ne faut pas non plus les laisser ouverts sans surveillance.

La **robustesse** de l'authentification et de la connexion permet donc de limiter les potentielles intrusions.

Comment est définie la communauté professionnelle et qu'est-ce que l'Interopérabilité ?

L'Article L. 1434-12 rédige la définition de la **communauté professionnelle territoriale de santé** :

La communauté professionnelle territoriale de santé est composée de professionnels de santé regroupés, le cas échéant, sous la forme d'une ou

*de plusieurs équipes de soins primaires, d'acteurs assurant **des soins de premier ou de deuxième recours**, [...] et d'acteurs **médico-sociaux et sociaux** ainsi que de services de prévention et de **santé au travail**, concourant à la réalisation des objectifs du projet régional de santé.*

L'INTEROPERABILITE :

L'interopérabilité correspond au partage de données-patients entre différents systèmes informatiques médicaux (28).

Par exemple, le logiciel-métier du médecin généraliste est capable d'interagir avec le logiciel Apycript afin d'intégrer des bilans biologiques au dossier médical d'un patient : un accès direct aux résultats évite donc une autre connexion à un autre logiciel à l'aide d'autres identifiants.

Cela permet d'améliorer l'ergonomie, en permettant aux professionnels de santé de ne pas se connecter à plusieurs logiciels différents. La consultation de dossier-patient devient alors plus fluide, permettant un gain de temps.

Savoir protéger les données des patients à travers l'hébergement, le chiffrement et le cloisonnement des accès aux données

LES DONNÉES PATIENTS :

Elles correspondent à son identification (nom, prénom, date naissance...), aux informations de vie personnelle, à son type de couverture sociale, et aux informations relatives à sa santé (soins, traitements, résultats d'imagerie...)

La CNIL recommande :

*La limitation des informations réunies dans ce dossier,
L'utilisation des données dans le cadre du suivi du patient,
La mise à jour des traitements du patient,
La suppression des dossiers au-delà de la durée de conservation (20 ans),
La mise en place des mesures de sécurité,
L'information du patient afin de lui assurer le respect de ses droits.*

Le **dossier papier** est théoriquement régi par ces mêmes règles mais elles deviennent difficilement applicables, augmentant ainsi le risque d'erreur.

L'HÉBERGEMENT DES DONNÉES :

Il se fait via l'*article L1111-8 du code de santé publique* : La préservation des données doit se faire via un hébergeur de données avec une **certification HDS** (Hébergeur de Données de Santé) si le support est informatique. Les transferts de données hors Union Européenne ne doivent pas être autorisés, les données doivent donc être hébergées au minimum au sein de l'union européenne.

Pour cela, la majorité des médecins ont recours aux **prestataires tiers**, qui doivent pouvoir garantir un niveau de sécurité convenable, le médecin doit cependant vérifier les caractéristiques du contrat avec son sous-traitant. (21).

Selon la CNIL :

*Il est préférable d'utiliser un prestataire qui comporte un hébergeur agréé et certifié. Il se doivent d'effectuer un stockage des dossiers dans un serveur à distance, celui-ci doit être un hébergeur agréé ou certifié pour l'hébergement, le stockage, selon la loi L1111-8 du CSP. Il convient d'être attentif au contrat d'assistance qui doit comporter une **clause de confidentialité** rappelant au fournisseur ses obligations*

A noter que l'utilisation de **clé USB** ou **disque dur externe** aux outils informatiques est déconseillée.

La CNIL recommande :

Dans le cas où cette solution était choisie pour les médecins généralistes, il faut effectuer régulièrement des sauvegardes sur des supports amovibles et les conserver dans un lieu différent du cabinet.

De plus, si le disque dur externe est utilisé, il est nécessaire d'effectuer un chiffrement des données (cryptage) dans sa totalité, fichier par fichier, avec un logiciel qui soit adapté.

LE CHIFFREMENT DES DONNÉES :

C'est le fait de crypter les données, afin qu'elles soient difficiles à déchiffrer en l'absence de logiciel adapté. En cas de fuite de données, ou d'hameçonnage réussi, les données deviennent ainsi incompréhensibles.

LE CLOISONNEMENT DES ACCES AUX DONNEES :

Il est nécessaire de définir différents **niveaux d'accès** aux données sur mesure pour chaque patient.

Il convient de définir un **référént** désigné par le patient qui est souvent le médecin généraliste, puis un **cercle de confiance restreint** contenant différents professionnels, et un **cercle de soin plus large** dont les membres ne peuvent accéder qu'aux informations nécessaires à l'exercice du soin.

Toutes les données ne sont pas indispensables à partager, certaines informations peuvent être bloquées ou restreintes pour certains professionnels.

Exemple 1 : Les allergies du patient doivent être connues par toutes les personnes appartenant au cercle de soin, mais les difficultés relationnelles intra-familiale du patient sont des informations inutiles pour certains professionnels de santé.

Exemple 2 : il est déconseillé qu'un médecin généraliste Lillois puisse communiquer avec un cardiologue de Marseille concernant un patient à Brest : l'annuaire patient doit être cloisonné par région.

Selon l'Article L1110-4 du CSP (version du 28 janvier 2016 modifié par la loi numéro 2016-41 du 26 janvier 2016 article 96) :

*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, excepté dans les cas de dérogation prévus par la loi.*

*Un professionnel peut échanger avec un ou plusieurs professionnels identifiés, des informations relatives à une même personne prise en charge et que ces informations soient **strictement nécessaires à la coordination ou à la continuité des soins**, à la **prévention** ou à son suivi **médico-social** et social. [...]*

Lorsqu'ils font partie de la même équipe de soins au sens de l'article L1110-12, ils peuvent partager des informations strictement nécessaires à la coordination ou à la continuité des soins.

*En cas de personne ne faisant pas partie de la même équipe de soins, il est nécessaire de recueillir le consentement préalable de la personne concernée. [...]La personne doit être informée de **son droit d'exercer une opposition** à l'échange et au partage d'information.*

Désigner un responsable des données qui déclare les incidents : le délégué à la protection des personnes (DPO)

Le **DPO** est le garant de la sécurité de l'information.

Il n'est pas obligatoire de désigner un DPO lorsque l'exercice est individuel. Pour les réseaux de professionnels et les maisons de santé (et toutes situations où les dossiers sont partagés entre plusieurs professionnels), cette désignation devient

obligatoire. Il faut donc désigner un DPO en interne, ou une personne extérieure (cabinet d'avocat, consultants).

Si un médecin le souhaite, la CNIL a rédigé un document afin de décrire les différentes étapes afin de devenir DPO (22).

Ce dernier doit tenir un **registre des activités**. La CNIL en a décrit un modèle à titre d'exemple (23). Ce registre centralisé et mis à jour est une vue d'ensemble sur l'activité effectuée, notamment la notification du partage de données personnelles. Il identifie notamment les sous-traitants, quelles données sont communiquées, le destinataire, la façon dont cela est réalisé (de façon sécurisée ou non). Ce registre est conservé en interne, et n'est pas obligatoirement transmis à la CNIL.

Le DPO se doit de **déclarer les incidents** inhérents à la confidentialité auprès de la CNIL. Cela permet de hiérarchiser les risques et d'éviter de potentielles erreurs.

Recueillir le consentement du patient

Le consentement pour la conservation des données ne doit pas être confondu avec le consentement au partage de ces dernières. En effet, il n'est pas nécessaire de recueillir le consentement des patients pour la conservation des données nécessaires au diagnostic ou à la prise en charge sanitaire ou sociale (21).

En revanche, **le partage des données** de santé est encadré par l'article L1110-4 du Code de Santé Publique :

*Ce partage est réservé aux professionnels de santé mais **le patient a le droit d'exercer une opposition** à l'échange et au partage d'information le concernant.*

Le personnel et les autres collaborateurs du médecin généraliste (secrétariat...) et les étudiants en médecine sont tenus au secret médical également, il convient de leur rappeler leurs obligations et de le spécifier dans les termes du contrat.

L'interdiction de la vente de données

La vente de données personnelles est une technique commerciale utilisée en permanence sur internet. La **vente de données** médicales est interdite en France et est passible de lourdes sanctions.

La *loi informatique et liberté* affirme que :

La collecte des données personnelles de santé à titre onéreux est interdite (y compris avec l'accord de la personne), sous peine de sanctions après application de l'article 226-21 du code pénal de 300 000 euros d'amende et 5 ans d'emprisonnement.

Les échanges interprofessionnels doivent nécessairement passer par des **services socles** utiles aux médecins généralistes dans leur exercice quotidien.

4. Création de services socles

a) Messagerie électronique sécurisée **MSSANTÉ** :

Il s'agit de messageries électroniques type « email crypté » entre professionnels de santé nommées **MSSanté**.

Exemple : Cette messagerie permet aux laboratoires d'envoyer des résultats biologiques aux médecins généralistes, ou encore aux médecins généralistes d'envoyer des ordonnances cryptées aux pharmaciens afin de faciliter la livraison de traitement aux personnes âgées à domicile.

Cette Messagerie MSSanté (12) :

*protège la responsabilité des professionnels habilités à échanger des données de santé. Utiliser une messagerie sécurisée préserve les données du patient dans le respect du secret médical, cadre posé par la CNIL et le code de la santé publique. L'ANS a mis en place **une liste blanche des opérateurs** autorisés à échanger des données dans l'espace de confiance MSSanté. Les référentiels reposent sur les standards de l'internet et de la messagerie afin d'aider les industriels, les établissements et les institutions à développer conformément leurs offres.*

b) MON ESPACE SANTÉ : est un dossier médical partagé, espace d'interopérabilité entre les professionnels de santé, permettant de renforcer le lien ville-hôpital

Il s'agit d'un **carnet de santé numérique** : il permet une interopérabilité entre médecins généralistes et les autres professionnels de santé. C'est un dossier de synthèse permettant l'accès au dossier médical de patient sur **tout le territoire national** dans un but d'optimisation des prises en charge.

C'est un dossier partagé, **éthique et sécurisé**, mis en place par l'Assurance Maladie et contenant les données-patients essentielles de manière synthétisée.

Cet espace numérique de santé permet donc le partage d'information médicale par différents corps de métiers (médecins généralistes, médecins urgentistes et hospitaliers, infirmiers, kinésithérapeutes...).

MON ESPACE SANTÉ dispose aussi d'une application mobile afin de stocker et partager des données de santé, un agenda de santé, et un catalogue de services référencés par l'Etat. Il permet le partage de documents (comptes rendus médicaux, résultats de laboratoires, dernières ordonnances...). Les patients peuvent limiter les informations aux professionnels de santé de leur choix. En cas d'urgence vitale, un bris de glace a été mis en place.

Depuis son lancement en janvier 2022, déjà 6.4 millions d'utilisateurs disposent d'un profil, et plus de 7 millions de documents ont été ajoutés.

c) L'agenda électronique sécurisé

Ce moyen permet de préserver la confidentialité des prises de rendez-vous.

Exemple : Doctolib, Maia etc

d) Les logiciels de prescription électronique

Des logiciels d'aide à la prescription électronique (e-prescription) ont été mis en place pour les médecins généralistes : la présence de code-barre et QR-code sécurisé

permet d'éviter les tentatives de fraudes, de faciliter les échanges entre professionnels de santé et d'améliorer la coordination des soins.

e) Logiciel-métier pour les dossiers-patient

L'offre dans ce domaine est variée. Ces logiciels-métier répondent à un cahier des charges complexe. Ils permettent, entre autres, de sauvegarder les dossiers médicaux, et permettent une bonne tenue du dossier patient.

Exemple : *Hellodoc, Weda, Crossway...*

f) Service de téléconsultation sécurisé

Ils permettent l'échange vidéo et audio avec les patients, le partage de documents et d'ordonnance pour certaines indications restreintes, avec un système de facturation sécurisé.

g) Dispositif de télémédecine

Ils sont en pleine expansion. Il s'agit de **plateformes** de report de données médicales pour les patients souffrant de maladie chronique :

Exemple : MyDiabby où le patient diabétique reporte au quotidien ses glycémies sur une application mobile. L'endocrinologue ou le médecin généraliste a un accès professionnel à cette plateforme, il peut contacter son patient et lui indiquer quelle modification thérapeutique effectuer afin d'équilibrer sa maladie.

Mais également d'autres outils de télémédecine :

Exemple : Outil de **téléexpertise** de dermatologie à distance, avec utilisation de technologies sophistiquées permettant des photographies de haute qualité de lésions cutanées potentiellement cancéreuses. Cela permettrait le bénéfice d'expertise aux plus grands nombres et en tous lieux.

h) Messagerie instantanée sécurisée

Il s'agit de messagerie entre professionnels de santé, notamment dans le secteur libéral, permettant l'échange de messages en quelques secondes via leurs smartphones. C'est un outil efficace permettant le partage d'information urgente concernant un patient avec un gain de temps, tout en respectant les règles de sécurité expliquées ci-dessus (chapitre 5.4.3), et qui sera détaillé ci-après à travers l'outil Predice PRO dans le cadre de cette étude (Annexes 4,5,6).

5. Les différents moyens de communication en santé dans la littérature

De nombreuses applications sont utilisées au quotidien dans le système de soin. Cela permet le partage d'informations aussi bien entre médecins généralistes et patients, qu'entre professionnels de santé.

Des échanges textos ou par messages vocaux enregistrés via ces applications sont parfois utilisés entre médecins et paramédicaux afin de communiquer des données de santé, ils sont **moins intrusifs et chronophages** qu'une conversation téléphonique.

Cependant, l'éventail de messageries est large, des applications incontournables dominent le marché international.

Parmi elles, l'utilisation de certaines applications cryptées telles que Whatsapp ou **Messenger**. Leur utilisation n'est pas interdite dans le secteur de la santé aux Etats-Unis par la HIPAA (5). En France elles sont aussi massivement utilisées.

Giordano V, Koch H et al, pensent que les messageries instantanées (telle que **Whatsapp**) sont un moyen de communication entre équipes médicales rapide et efficace. Une revue de la littérature au travers de 10 études internationales conclut à un moyen de communication innovant (4).

Mars et Scott, effectue une revue de la littérature afin de déterminer la satisfaction des utilisateurs de Whatsapp. Elle contenait 32 études réalisées notamment dans des pays pauvres avec faible budget alloué à la santé (comme le

Brésil, l'Inde, et les Philippines) et concernait 17 disciplines (la médecine générale n'en faisait pas partie). Whatsapp y est décrit comme **simple** d'utilisation, **peu cher** et efficace pour communiquer entre professionnels de santé. Il notifie que peu d'attention était octroyée à la confidentialité, au consentement des patients et à la sécurisation des données (6).

Drolet et al, en 2017, effectuent une enquête transversale : 63% des chirurgiens (appartenant à la Société Américaine de Chirurgie de la Main) rapportent que les **Messages Textos** ne correspondent pas au standard de sécurité de la HIPAA. 37% d'entre eux rapportent **ne pas les utiliser** pour communiquer en intra-hospitalier, notamment les **plus jeunes médecins** interrogés. (5)

Dans leur revue de la littérature aux États-Unis, *Sashikumar Ganapathy et al.* examinent le rôle des applications telles que WhatsApp, **Facetime**, **Messenger**, **Viber** dans la télémédecine. Ils concluent qu'afin de sauvegarder les données patients et leur confidentialité, les applications mobiles ne devraient servir **qu'à une fonction de santé** (3).

En effet, cette idée est majoritaire en Europe. La sauvegarde de la confidentialité des données patients est un enjeu majeur de société. Différents moyens de communication sont inacceptables notamment les diverses applications mobiles utilisées dans notre vie quotidienne. Le secteur médical est régi par des obligations notamment le secret médical. Il existe un **encadrement strict** de cette nouvelle pratique que constitue la e-santé.

En somme, nous voyons bien l'hétérogénéité des moyens de communication utilisés, et la nécessité de pouvoir différencier un moyen de communication qui soit sécurisé ou non.

A ce titre, La Commission Nationale de l'Informatique et Liberté (CNIL), a initié un guide de bonne pratique concernant les échanges de données-patient (20). Selon elle, les messagerie-chat, SMS, MMS ou autres messageries standards sur internet **ne sont pas recommandées** car n'ont aucune garantie de confidentialité.

De même, la **communication téléphonique** ne permet pas de garantir l'identité des personnes communiquant, aucune identification ni intermédiaire sécurisé (comme une carte professionnelle) ne sont garantis.

Exemple : Quand le médecin traitant est contacté par des professionnels de santé hospitaliers, pour la plupart, il n'y a aucune possibilité d'identification stricte. Le caractère frauduleux des appels ne peut être écarté.

6. Objet de l'étude : Predice PRO

L'Agence régionale de santé (ARS) des Hauts-de-France lance le projet PREDICE (Annexe 4) qui comprend **une messagerie instantanée interprofessionnelles prénommée Predice PRO**.

Déroulement du projet Predice PRO

La première étape est la mise en œuvre du projet (entre juin et septembre 2021), puis l'expérimentation à partir d'août à septembre 2021 auprès de 4 CPTS des Hauts-de-France. La généralisation dans tous les Hauts de France a eu lieu lors du premier trimestre de l'année 2022 à travers l'application mobile.

Les **objectifs** de cette expérimentation étaient de :

- Remonter les incidents techniques,
- L'anticipation et l'analyse des risques inhérents au projet,
- Et enfin de remonter les besoins d'évolution de l'outil.

Les référents de ce projet font partie de **l'ARS** et de **l'URPS**.

Présentation du service

Il s'agit d'une messagerie instantanée interprofessionnelle. Nous en avons étudié la première version utilisée par les professionnels de santé durant l'année 2021-2022.

Elle permet la création de conversation entre deux ou plusieurs professionnels de santé avec :

- L'envoi et la réception instantanés de messages directement depuis un smartphone à type de texte, documents, photographies (application reliée à l'appareil photo du téléphone) ;
- La réception de notifications : être averti et pouvoir ouvrir directement des discussions ou des documents ;

- L'existence d'un **annuaire** santé sécurisé regroupant divers professionnels de santé des Hauts-de-France ;
- La possibilité de définir le **cercle de soin du patient**, et de paramétrer des conversations afin de discuter avec les professionnels de santé autour du dossier-patient, de modifier, voire de supprimer les accès de certains professionnels ;
- Le **consentement oral** est un prérequis avant d'échanger, il est conseillé de l'indiquer dans le dossier patient ;
- Une **plateforme d'assistance technique** en cas de problème est disponible, par téléphone et par email.

Description du niveau de sécurité du système

- **Haut niveau d'identification patient** : à travers les nom, prénom, date de naissance, lieu d'habitation et commune de naissance.
- **Haut Niveau d'identification du professionnel** : nom, prénom, profession, lieu d'exercice, carte CPS, numéro RPPS ou numéro ADELI. Il s'appuie sur le répertoire opérationnel des ressources (ROR) et AMELI pour la création des comptes.
- **Robustesse de l'Authentification** qui est à double facteur (après confirmation par code SMS/email) avec mot de passe fort, et nécessité de changement régulier de mot de passe (semestriel).
- Présence d'un **verrouillage automatique** de l'application après inactivité de quelques minutes et déverrouillage possible par code pin ou capteur biométrique.
- Présence de **différents niveaux d'accès** aux documents avec une confidentialité dite normale, restreinte, ou privée.
- L'éditeur sous-traitant est **Maincare Solution**, il dispose d'une politique interne de protection des données éditée par son DPO.
- L'hébergement des données est **agréé HDS**, dont le partenaire hébergeur est **Cheops Technology**. Ils permettent la sécurisation des infrastructures hébergeurs dans des emplacements géographiques de deux Datas Center au titre de la certification ISO27001. Celle-ci garantit un contrôle d'intégrité, de cloisonnement, de chiffrement, d'archivage et de sécurisation des données patients.

INTRODUCTION

L'expansion des différents acteurs du monde médical a permis l'émergence de réseaux de santé réunis au travers d'un Dossier-Patient, permettant de centraliser les données essentielles à sa prise en charge.

Tout processus de soin implique un suivi rigoureux et une traçabilité pour chaque praticien dans un souci d'efficacité, de sécurité, et d'information.

L'informatisation des différents systèmes de santé a ainsi permis de voir apparaître la proposition de nouvelles solutions concernant la création et la mise à jour des dossiers médicaux et paramédicaux : le Dossier Médical Partagé (DMP) devenu Mon Espace Santé en 2022. Ce réseau de soins doit s'articuler parfois rapidement, sans omission, afin de permettre une coordination des soins centrée sur le patient.

Des inquiétudes inhérentes aux partages de données-patient peuvent se distinguer telles que : la confidentialité des données, l'oubli, l'erreur d'identification patient ou d'identification du professionnel de santé à l'intérieur même du réseau de soin. La vigilance de la part des praticiens se doit donc d'être accrue.

Il existe des problématiques internes aux acteurs impliqués mais l'on déplore également de potentielles agressions externes telles que les cyberattaques. Autant de défis qui sont la conséquence de l'émergence du numérique en santé.

Ainsi, lorsque les professionnels de santé veulent communiquer rapidement concernant leur patient, plusieurs moyens s'offrent à eux. L'introduction générale nous a permis de mettre en évidence les carences de la littérature concernant la sécurisation des données de e-santé.

Concernant les échanges entre médecins généralistes et autres professionnels de santé, quelques solutions éthiques mises en place par l'ARS et l'URPS des Hauts-de-France voient le jour, notamment la messagerie sécurisée **Predice PRO**.

L'objectif principal de ce travail est **l'évaluation de la sécurisation des données par l'utilisation de la messagerie instantanée interprofessionnelle Predice PRO**.

MATERIEL ET METHODES

1. Type d'étude, objectifs et critères de jugement

Il s'agit d'une étude observationnelle, transversale, quantitative, et réalisée de manière prospective.

Cette étude est multicentrique, menée dans les Hauts-de-France avec des médecins interrogés entre juin et septembre 2022.

a) Critère principal d'intérêt : le Score e-Santé Sécurité

La méthode retenue pour l'architecture des questionnaires est basée sur « l'Évaluation des Bénéfices » (*Benefits Evaluation BE*) mise au point par *Canada Health Infoway* (15). Il s'agit d'un marqueur du succès d'un système de e-santé et il est basée sur le modèle *Information System Succes Model* de *DeLone and MacLean*. Il a été conçu après revue de la littérature et l'évaluation de plusieurs systèmes électroniques en santé (*Health Information Systems HIS*).

Dans leur *Handbook of e-Health* (18), *Lau and Kuziemsky* ont élaboré un guide d'évaluation en e-santé. Ce guide comprend trois composantes : la qualité du système, la qualité de l'information et la qualité des services : cela permet d'estimer le degré de satisfaction, et le bénéfice en termes d'accès, de sécurité et de productivité d'un système d'information.

Nous nous sommes également basées sur le **Guide CNIL** et les règles de sécurité du **RGPD** afin d'élaborer notre propre score.

Il s'agit donc d'un score d'évaluation d'un outil numérique en santé : **le Score e-Santé** qui se divise en 2 sous-scores:

- Le **Score e-Santé Satisfaction** nommé **Score globale d'évaluation**, qui fera l'objet d'une autre thèse collaborative réalisée par Chahrazad Kheder.
- Le **Score e-Santé Sécurité** qui est l'objet de ce travail.

Le critère principal d'intérêt de ce travail concerne donc le Score e-Santé Sécurité (e-SS).

b) Critères de jugement

Le critère de jugement principal

Comparaison du Score e-Santé Sécurité, estimé par les médecins généralistes des Hauts-de-France, entre utilisateurs de Predice PRO et non-utilisateurs.

Le but est d'évaluer la sécurisation des données-patient en comparant le score de Predice PRO à celui des autres moyens de communication interprofessionnelle.

Cette étude de la sécurisation des échanges de données-patient nous permettra d'évaluer l'éventuel **bénéfice apporté par Predice PRO**.

L'hypothèse principale est l'augmentation du Score e-Santé Sécurité de Predice PRO en comparaison aux autres moyens de communication communément utilisés.

Les critères de jugement secondaires

- La comparaison du Score e-Santé Sécurité entre les moyens de communication **sécurisée** (en dehors de Predice Pro) et les moyens de communication **non sécurisés**.
- La comparaison du Score e-Santé Sécurité entre **Predice PRO** et les autres moyens de communication **sécurisés**.
- Établir les facteurs prédictifs parmi les **caractéristiques des médecins généralistes** du type de moyen de communication utilisé (**sécurisé ou non**).

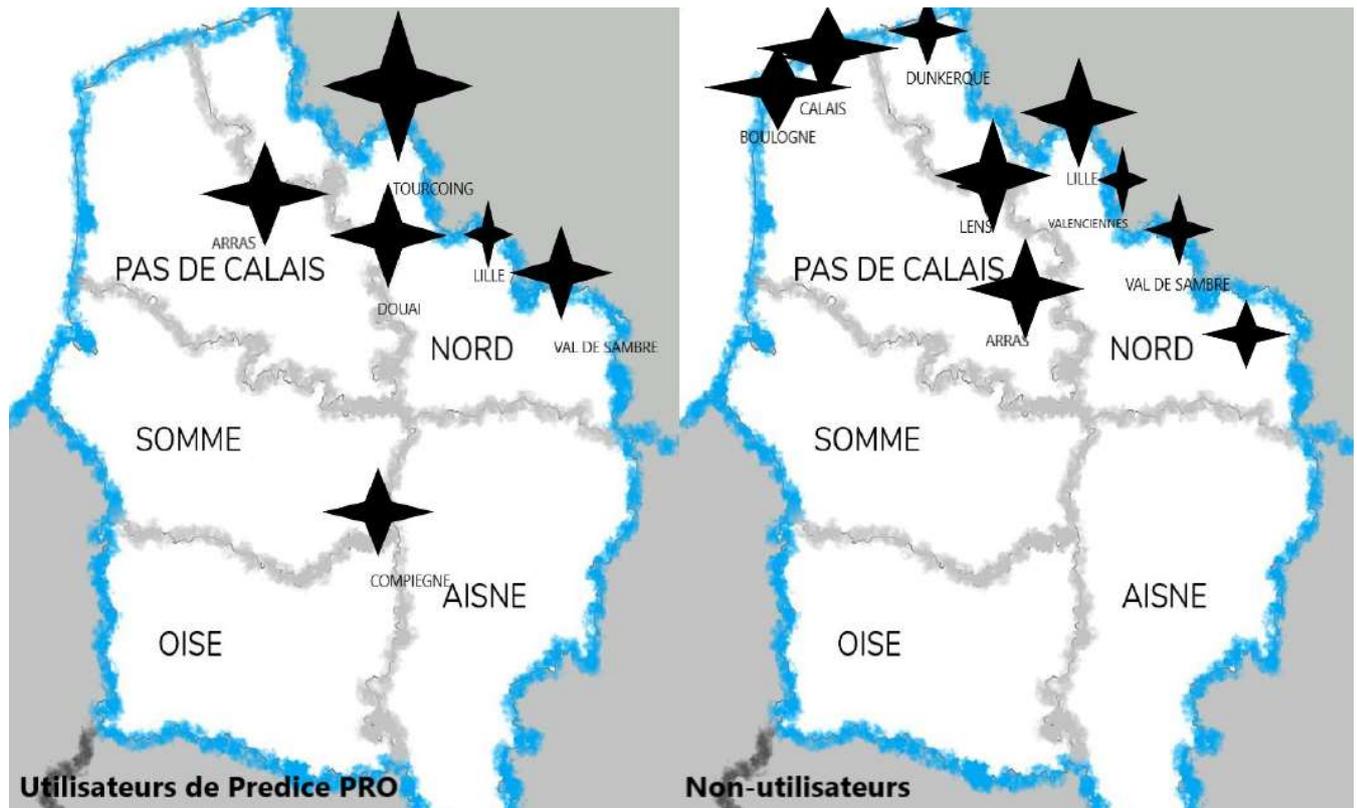
d) Population

Méthode de recrutement

Le recrutement des patients a eu lieu en deux temps :

- Par l'envoi d'emails sur la boîte mail universitaire de la faculté de médecine de Lille aux différents maîtres de stage universitaire ;

- Ainsi qu'aux utilisateurs de Predice PRO par envoi d'emails aux professionnels de santé, via l'URPS aux quatre CPTS prenant part à l'expérimentation (CPTS Val-de-Sambre, CPTS Tourcoing-Mouvoux-Neuville, CPTS Grand Douai, CPTS de Compiègne mais également des professionnels de Lille et d'Arras). Deux relances par courriel puis par téléphone ont été réalisés auprès des coordinateurs des CPTS.



Carte. Localisation de la population de l'étude : utilisateurs de Predice PRO et non-utilisateurs des Hauts-de-France.

Critères d'inclusion

Concernant toute la population :

- Être professionnel de santé libéral installé et en exercice dans les Hauts-de-France durant le recueil de données ;
- Être médecin généraliste avec une activité libérale, ou mixte libérale/hospitalière, être interne de médecine générale remplaçant, ou être médecin généraliste remplaçant.

Concernant les utilisateurs de Predice PRO :

- Inclusion également de paramédicaux (infirmiers libéraux notamment) ;
- Nous avons interrogé les utilisateurs ayant participé à l'expérimentation à partir d'août 2021 et appartenant aux 4 CPTS citées ci-dessus. Nous les avons interrogés en août 2022 après l'utilisation de Predice PRO pendant une année.

Critères de non-inclusion

Internes d'autres spécialités, interne de médecine générale non-remplaçant ou SASPAS, Médecin généraliste avec une activité salariée hospitalière stricte sans activité libérale.

1. Recueil de données

a) Données recueillies

Les caractéristiques sociodémographiques des médecins généralistes interrogés étaient : le genre, l'âge, la modalité d'exercice, le type d'activité, l'aisance informatique, les outils informatiques utilisés dans leur pratique quotidienne, la fréquence des échanges interprofessionnels, les caractéristiques de leur patientèle, les motifs de consultation, le type de pratique, la fréquence des échanges interprofessionnels, le type de professionnel avec qui le médecin communique, les motifs d'utilisation d'un moyen de communication interprofessionnel, et enfin l'objet des échanges.

b) Modalités du recueil

L'enquête a été réalisée à l'aide d'un sondage en ligne via le logiciel *Sphinx Declic*, envoyée par email à un échantillon représentatif de paramédicaux et médecins généralistes utilisateurs de la plateforme, ainsi qu'à différents médecins généralistes MSU et internes de dernière année de médecine générale de la faculté de médecine de Lille.

Le questionnaire était anonyme et mis à disposition pendant quatre mois (de juin à septembre 2022), douze mois après la lancée de Predice PRO (entre août 2021 à août 2022).

2. Analyse de données : nom des variables

a) Variables d'intérêts

Les variables d'intérêt recueillies comportaient :

- Les caractères sociodémographiques des professionnels de santé ;
- Le Score e-Santé Sécurité estimé par les professionnels de santé.

Ce score est composé de 20 items, et est compris **entre 20 et 80 points**. Ces items concernent les modalités de verrouillage de l'outil de communication, l'authentification, l'identification, l'hébergement des données, le niveau d'accessibilité, de confidentialité et de restriction d'accès aux données, la possibilité de droit d'opposition et de consentement des patients, et enfin la revente de données personnelles (voir chapitre 5.3.3).

Le design de l'étude est quantitatif et implique l'utilisation de statistiques descriptives via une **échelle de LIKERT** au travers de variables qualitatives multivaluées.

Les différentes réponses estimées par les professionnels de santé concernant le Score e-Santé Sécurité comportait les mentions : « parfaitement d'accord », « modérément d'accord », « modérément en désaccord », « totalement en désaccord », auxquelles respectivement un score de 1, 2, 3, 4 était attribué.

La valeur médiane était attribuée à la mention « non applicable ». Cette médiane était calculée pour chaque item.

b) Critères d'exposition

Concernant les variables définissant les groupes, le caractère sécurisé ou non du moyen de communication a été établie après revue de la littérature (chapitre 5.5 de l'introduction générale) :

- **Moyens de communication non-sécurisés** : la conversation téléphonique, WhatsApp, SMS/MMS, email personnel, Telegram, Messenger, Courrier Postal, Skype ;
- **Moyens de communication sécurisés** : Predice PRO, email professionnel, Healphi, la Parole, Idomed, les réunions interprofessionnelles, Messagerie MSSanté, DoctolibTeam.

3. Analyse statistique : les méthodes utilisées

a) Analyse bivariée et comparaison de moyenne

Comparaison de moyenne

Les variables quantitatives sont exprimées en moyenne et écart type, ainsi qu'en médiane, premier et troisième quartile (Q1, Q3).

Les variables qualitatives sont exprimées sous la forme d'un effectif total.

Les variables quantitatives ont été analysées via une **comparaison de moyenne** des Score e-Santé Sécurité entre deux échantillons indépendants :

- Les utilisateurs de Predice PRO et les non-utilisateurs ;
- Les moyens de communication sécurisés (en dehors de Predice PRO) et les moyens non sécurisés ;
- Les utilisateurs de Predice PRO et les autres moyens de communication sécurisés.

Après application d'un **test de Shapiro-Wilk**, les variables récoltées ne suivaient pas une loi de distribution normale. On procédait donc à un test de **Mann-Whitney** pour l'analyse des variables quantitatives, et par un **test du Khi²** pour les variables qualitatives.

Analyse bivariée

L'indépendance entre deux variables qualitatives était testée à l'aide d'un test du Khi².

Les relations de chacune des covariables et la variable binaire (moyen de communication sécurisé ou non) sont modélisées et testées à l'aide d'une analyse bivariée. Les résultats sont exprimés en termes d'Odds-ratio assorti d'un intervalle de confiance.

Concernant l'attribution du Score e-Santé Sécurité, il était attribué un score médian pour chaque item à la mention « non-applicable ».

Analyses multivariées

Une régression logistique a été effectuée afin d'évaluer les facteurs prédictifs du type de moyen de communication utilisé (**sécurisé ou non**).

Les relations entre les **covariables** candidates et une **variable binaire** (moyen de communication sécurisé ou non) étaient modélisées et testées à l'aide d'une **régression logistique**. Les résultats étaient exprimés en termes de coefficient assorti d'un intervalle de confiance à 95%.

En effet, nous avons cherché à prédire la variable binaire (sécurisé ou non) à l'aide d'une combinaison de plusieurs variables prévisionnelles. Ces covariables participaient de façon additive à l'équation de régression et la pondération de chaque variable était évaluée par son **coefficient de régression**.

Les covariables disponibles sont toutes incluses dans l'**analyse multivariée** et ce quel que soit leur degré de significativité dans les analyses univariées. Seul le modèle final est présenté.

Les différentes analyses ont été effectuées avec le **logiciel XLSTAT 2021.3.1**.

4. Significativité

Les tests statistiques étaient bilatéraux. Les p-values étaient considérées comme significatives au seuil de 5%. Les intervalles de confiance étaient calculés à 95%.

5. Cadre réglementaire

Cette étude a été initialement pilotée par l'URPS des Hauts-de-France durant l'année 2021, puis poursuivie à titre personnel au moment du recueil des données.

L'analyse statistique a été indépendante de l'URPS et effectuée par un ingénieur spécialisé en statistique.

L'étude a été déclarée auprès de la CNIL par le délégué à la protection des données de l'Université de Lille en janvier 2022.

RESULTATS

1. Diagramme de flux

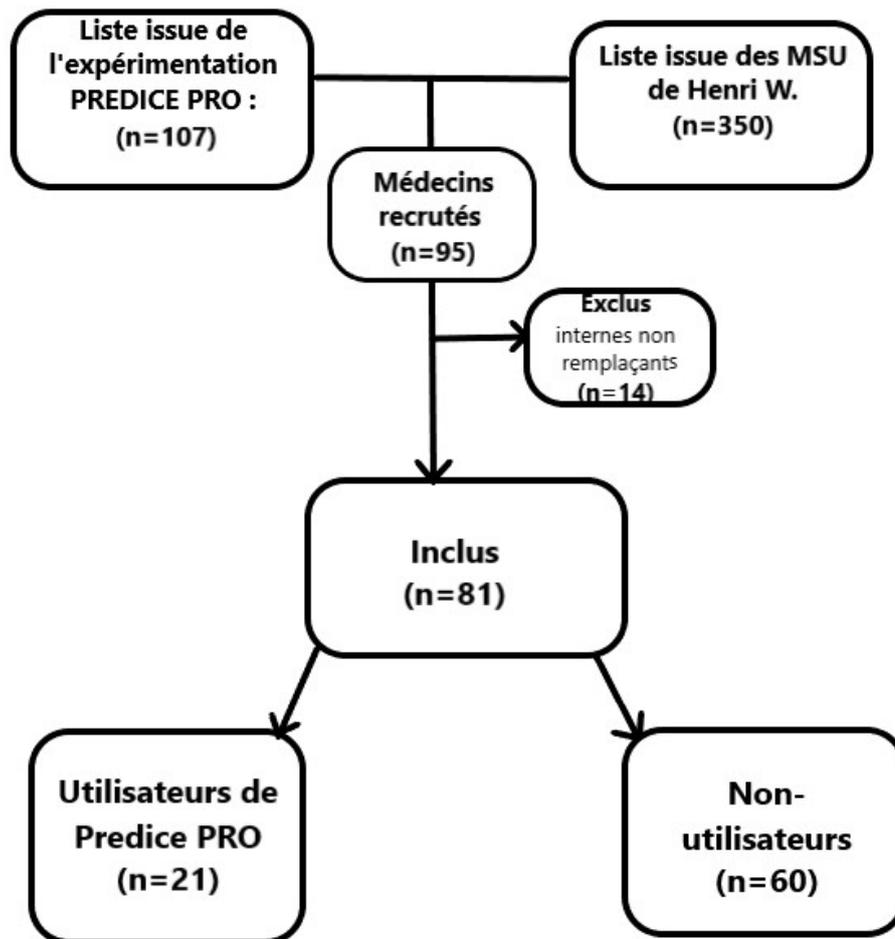


Figure 1. Flow-chart du recrutement des médecins généralistes utilisateurs et non-utilisateurs de Predice PRO.

2. Description des patients à l'inclusion

Caractéristique Démographique		UTILISATEUR	NON-UTILISATEUR
Population		<i>Prédice Pro</i> 21	<i>Total Non-utilisateurs</i> 60
			<i>Conversation tel</i> 19
			<i>WhatsApp</i> 9
			<i>SMS/MMS</i> 7
			<i>Email perso</i> 2
			<i>Télégram</i> 2
			<i>Messenger</i> 2
			<i>Courrier postal</i> 1
			<i>Skype</i> 1
			<i>DoctolibTeam</i> 6
			<i>MSSante</i> 6
			<i>Reunion interprof</i> 1
			<i>Idomed</i> 1
			<i>Parole</i> 1
			<i>Healphi</i> 1
			<i>Email pro</i> 1
Genre			
	<i>Masculin</i>	8	35
	<i>Féminin</i>	13	25
Age		41,09 (moyenne) ecart type: 8,39 médiane=41	41,71 (moyenne) ecart type : 11,55 médiane = 37
Modalité d'exercice			
	<i>ZIP</i>	2	2
	<i>ZAC</i>	1	6
	<i>ZAR</i>	0	2
	<i>Urbaine</i>	10	33
	<i>Rural et Semi-rural</i>	11	30
Type d'activité			
	<i>Libéral</i>	20	52
	<i>Salarié</i>	0	3
	<i>Mixte</i>	1	5
Aisance informatique			
	<i>Mauvaise</i>	0	1
	<i>Passable</i>	2	8
	<i>Moyenne</i>	8	10
	<i>Bonne</i>	5	32
	<i>Excellente</i>	6	9
Outils informatiques			
	<i>Téléphone professionnel</i>	15	35
	<i>Ordinateur de bureau</i>	9	44
	<i>Téléphone personnel</i>	8	43
	<i>Tablette</i>	7	7
	<i>Ordinateur portable</i>	3	16
	<i>Bracelet connecté</i>	0	6
Type de pratique			
	<i>Nombre de consultation</i>		
	-30	15	39
	+30	6	21
	<i>Durée d'une consultation</i>		
	5-15 min	9	8
	15-20 min	12	43
	20-30 min		9
	<i>Nombre de téléconsultation</i>		
	0	9	34
	+1	11	25
	<i>Nombre de visite à domicile</i>		
	0	1	9
	+1	20	51

Fréquence des échanges interprof		
< Hebdomadaire	8	18
> ou = Hebdomadaire	13	42
Caractéristique des patients		
Pourcentage de Patients > 75 ans polyathologique	12	19
AUTRES :	47	136
Femme	2	6
Homme	2	1
Equivalent H/F	11	29
Sénior > 65 ans	16	19
Adulte 30-65 ans	11	47
Adulte jeunes 18-30 ans	3	10
Enfants 0-18 ans	2	23
Patient âgé dépendant en EHPAD		1
Motif de consultation		
Survi	6	14
Aigu	5	8
Les deux de manière équivalente	12	38
Communication entre type de professionnel		
IDE libéral	15	50
Med G	16	21
Pharmacien	8	41
Kinésithérapeute	4	8
Auxiliaire de vie	5	3
Med libéral d'autre spé	3	27
Médecin Hospitalier	3	26
Sage femme	2	3
IDE hospitalier	1	3
Biologiste	0	10
Interne (med G et autre spé)	0	19
AUTRES = secrétaire, gestionnaire de tutelle, coordinateur MS, orthophoniste, podologue	0	4
Motif d'utilisation		
Urgent	2	20
Non urgent	11	11
les 2 de manière équivalente	7	29
Objets des échanges		
Discussion autour d'une pec	14	45
Discussion autour d'un patient	13	34
Discussion autour organisation CPTS	10	8
Education interprofessionnel	5	7
Demande d'avis d'un autre confrère de même spécialité	4	8
MAJ reco et pratique professionnelle	3	3
Demande d'avis spécialisé	2	36
Récupération d'info médicale avec milieu hospitalier	2	10
Demande RCP	1	2
Pas de réponse	1	0

Tableau 1. Caractéristiques démographiques des utilisateurs de Predice PRO et des non-utilisateurs (effectifs).

PEC=prise en charge, info=information, RCP=réunion de concertation pluridisciplinaire, Med G=médecin généraliste, conversation tel=conversation téléphonique, email perso=email personnel, email pro=email professionnel, réunion interprof= réunion interprofessionnelle, IDE=infirmer diplômé d'état.

3. Objectif principal : Score e-Santé Sécurité des utilisateurs de Predice PRO et des non-utilisateurs

Comparaison du SCORE e-SS entre les utilisateurs de Predice PRO et les non-utilisateurs

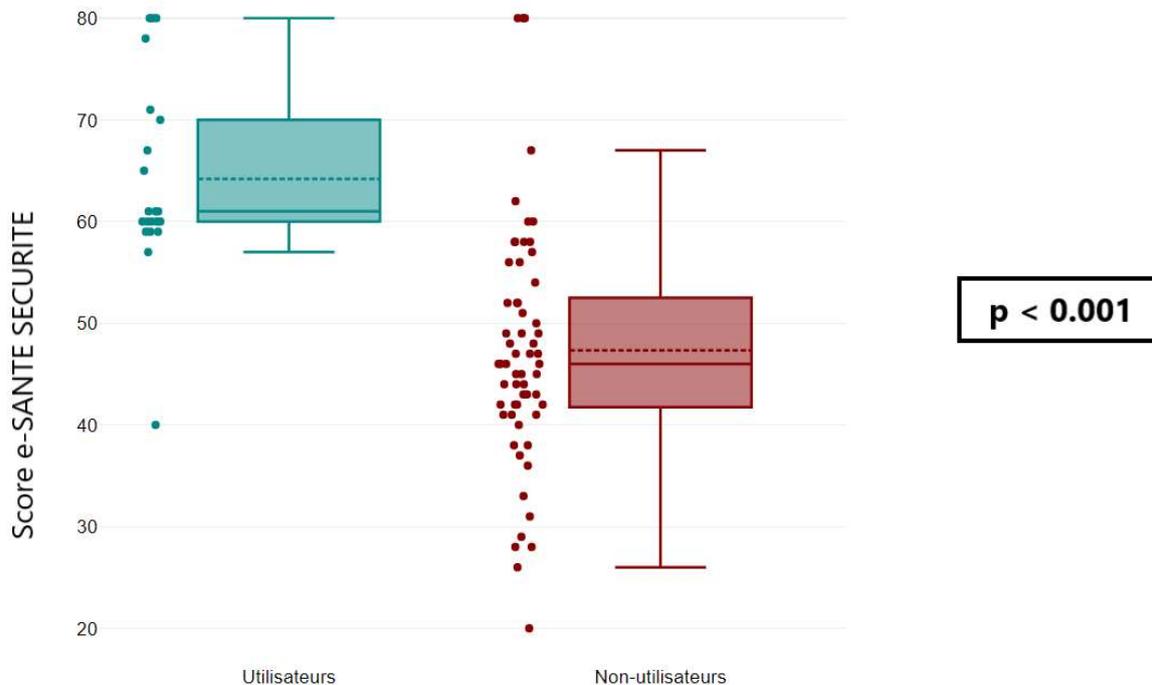


Figure 2. Box-Plot : Score e-Santé Sécurité (entre 20 et 80) estimés par les Médecins Généralistes. Médiane, Moyenne (pointillés), Quartiles et Bornes.

Dans le groupe utilisateurs, le Score e-Santé Sécurité moyen était de **63,9** (+/- 10,5 points), alors qu'il était réduit à **47,3** (+/- 12 points) dans le groupe non-utilisateurs.

On notait donc une augmentation significative de **16,6** points ($p < 0.001$) au profit du groupe utilisateurs de Predice PRO.

4. Premier objectif secondaire : Score e-Santé Sécurité des moyens de communication sécurisés et non-sécurisés

Comparaison du SCORE e-SS entre les moyens sécurisés et non-sécurisés

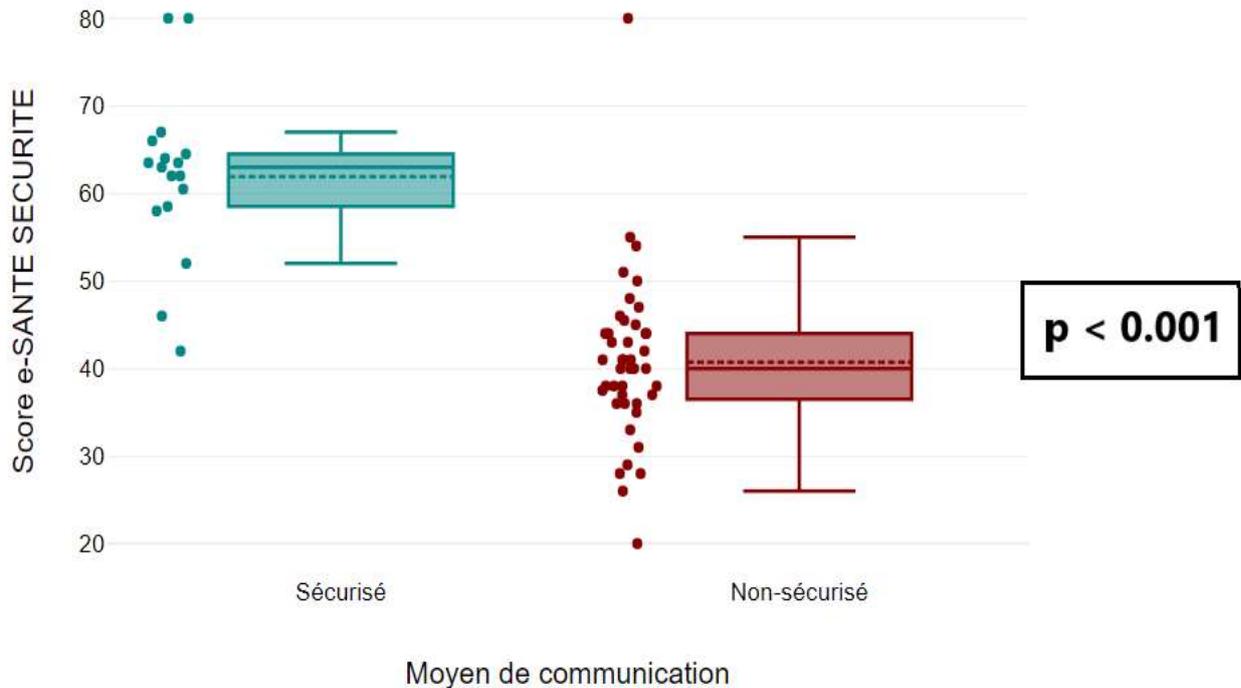


Figure 3. Box-Plot : Score e-Santé Sécurité (entre 20 et 80) estimés par les Médecins Généralistes. Médiane, Moyenne (pointillés), Quartiles et Bornes.

Dans le groupe moyen de communication sécurisé, le Score e-Santé Sécurité moyen était de **61,9** (+/- 9,7 points) alors qu'il était réduit à **40,7** (+/- 9,5 points) dans le groupe moyen de communication non-sécurisé.

On notait une augmentation significative de **21,2** points ($p < 0.001$) au profit du groupe moyen de communication sécurisé.

5. Deuxième objectif secondaire : Score e-Santé Sécurité des moyens de communication sécurisés

Comparaison du SCORE e-SS entre PREDICE PRO et les autres moyens sécurisés

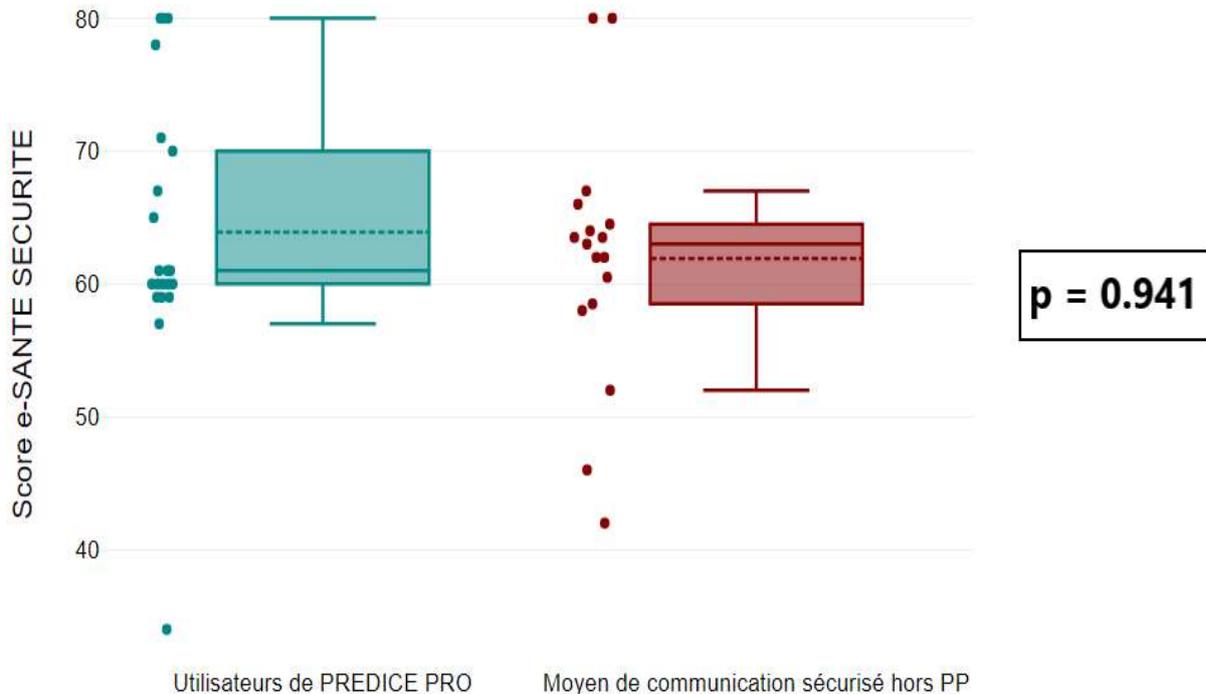


Figure 4. Box-Plot : Score e-Santé Sécurité (entre 20 et 80) estimés par les Médecins Généralistes. Médiane, Moyenne (pointillés), Quartiles et Bornes.

Dans le groupe utilisateurs de Predice PRO, le score e-Santé Sécurité moyen était de **63,9** (+/- 10,5 points) contre **61,9** (+/- 9,7 points) dans le groupe moyen de communication sécurisé (en dehors de Predice PRO).

On ne notait pas de différence significative entre les deux scores, les deux groupes étaient comparables ($p=0.941$).

6. Troisième objectif secondaire : Analyse bivariée et multivariée : facteurs prédictifs du moyen de communication sécurisé ou non.

ANALYSE BIVARIEE		OR	IC	p value
Type d'activité	1: libéral 0: autre	1,36	[0,53-3,48]	0,942
Age	1: < 45 0: > 45	0,59	[0,43-1,89]	0,672
Sexe	1: H 0: F	1	[0,41-2,45]	0,996
Type d'interlocuteur	1: > 3 types 0: < 3 types	0,67	[0,26-1,72]	0,400
Zonage	1: urbain 0: (semi)rural	0,66	[0,27-1,62]	0,365
Densité	1: ZIP 0: ZAC/ZAR	0,95	[0,28-3,21]	0,933
Outils de communication	1: >3 types 0: < 3 types	2,37	[0,7-7,09]	0,699
Aisance informatique	1: Excellente 0: autres	4,46	[2,99-20,06]	0,015
Nombre de patients (par jour)	1: > 30 0: < 30	1,36	[0,53-3,48]	0,520
Visite à domicile (par jour)	1: >5 0: <5	3,46	[1,26-9,45]	0,013
Téléconsultation	1: oui 0: non	1,86	[0,76-4,59]	0,173
Patient sénior	1: > 75ans polypatho 0: autres	2,34	[0,93-5,89]	0,068
Motif de consultation	1: suivi 0: autres	1,53	[0,54-4,31]	0,423
Fréquence d'échange interprofessionnel	1: > Hebdomadaire 0: < Hebdomadaire	0,9	[0,26-3,13]	0,868

Tableau 1. Analyse bivariée : Analyse des facteurs prédictifs de l'utilisation d'un moyen de communication sécurisée (via le Score e-Santé Sécurité)

Dans cette analyse bivariée, parmi les quatorze covariables, deux reviennent significatives :

- **L'aisance informatique** : si le professionnel avait une excellente aisance informatique alors il avait 4,5 fois plus de chance d'avoir un moyen de communication sécurisé (p=0.015).
- **Le nombre de visites à domicile** : si le professionnel effectuait plus de 5 visites à domicile par jour, il avait 3,5 fois plus de chance d'avoir un moyen de communication sécurisé (p=0.013).

A noter que dans ces analyses bivariées et multivariées nous avons inclus Predice PRO dans les moyens de communication sécurisés.

ANALYSE MULTIVARIEE		Coefficient	IC	p value
Age	1: < 45 0: > 45	0,26	[-0,89 – 1,41]	0,66
Zonage	1: urbain 0: (semi)rural	- 0,76	[-1,76 – 0,24]	0,14
Densité	1: ZIP 0: ZAC/ZAR	- 0,86	[-2,43 – 0,69]	0,27
Outils de communication	1: >3 types 0: < 3 types	0,87	[-0,34 – 2,07]	0,16
Aisance informatique	1: Excellente 0: autres	1,49	[1,1 – 2,99]	0,05
Nombre de patients (par jour)	1: > 30 0: < 30	0,25	[-1,01 – 1,5]	0,69
Visite à domicile (par jour)	1: >5 0: <5	0,94	[-0,19 – 2,07]	0,10
Téléconsultation	1: oui 0: non	0,33	[-0,68 – 1,35]	0,52
Patient sénior	1: > 75ans polypatho 0: autres	0,52	[-0,67 – 1,71]	0,39
Type de Suivi	1: suivi 0: aigu	0,29	[-1,03 – 1,62]	0,67
Fréquence d'échange interprofessionnel	1: > Hebdomadaire 0: < Hebdomadaire	- 1,14	[-2,34 – 0,07]	0,05
Type d'interlocuteur	1: > 3 types 0: < 3 types	- 0,75	[-1,87 – 0,38]	0,19

Tableau 2. Analyse multivariée : facteurs prédictifs de l'utilisation d'un moyen de communication sécurisée (via le Score e-Santé Sécurité)

L'objectif de cette analyse était de découvrir les facteurs prédictifs du caractère sécurisé ou non du moyen de communication utilisé.

Pour cela, nous avons effectué une combinaison linéaire des covariables afin d'évaluer la pondération de chacune via un coefficient de régression. Ces coefficients nous permettaient de mesurer l'influence et le poids de chaque covariable après les avoir admises dans un modèle de régression logistique.

Parmi les douze covariables, deux d'entre elles exerçaient une influence **significative** :

- La **fréquence des échanges interprofessionnels** (supérieure à hebdomadaire) exerçait une influence **négative** avec un coefficient de -1.14 :

plus les médecins échangeaient (fréquence supérieure à hebdomadaire) et moins le moyen de communication était sécurisé.

- **L'excellente aisance informatique** avait une influence **positive** avec un coefficient positif de 1.49 : plus ils étaient à l'aise informatiquement et plus le moyen de communication était sécurisé.

DISCUSSION

1. Analyse des résultats

a) Critère de jugement principal

Notre étude s'est voulue innovante et portait sur la création d'une messagerie instantanée sécurisée, Predice PRO, premier outil de communication émis par l'URPS et l'ARS, et répondant à un strict cahier des charges.

Nous avons démontré de manière significative la **supériorité de Predice PRO** en termes de sécurisation des données de santé, confirmant ainsi notre hypothèse principale.

b) Critères de jugement secondaires

Nous avons scindé en deux populations les moyens sécurisés par rapport aux moyens non sécurisés à l'aide des données de la littérature. Cette scission a été confirmée à l'aide de notre score e-Santé Sécurité. En effet, les moyens de communication sécurisés avaient un score e-SS supérieur à ceux non sécurisés.

En parallèle, le score e-SS de Predice PRO était comparable aux autres moyens de communication sécurisés confirmant ainsi la pertinence de ce nouvel outil.

Nous avons également mis en évidence, à l'aide d'une régression logistique, un facteur prédictif de l'utilisation d'un moyen de communication sécurisé (résultat commun aux analyses bivariée et multivariée) : **l'aisance informatique**, avec une influence positive démontrée de façon significative.

Un résultat reste intéressant à relever, mais n'était pas significatif au seuil de 5% ($p=0.068$) : une patientèle composée en majorité de patients seniors de plus de 75 ans polypathologiques multipliait par 2.4 la chance d'avoir un moyen de communication sécurisé. On peut alors s'interroger sur le possible lien de causalité entre la coordination des soins que nécessite une patientèle âgée, et un outil efficace et sécurisé de partage de données-patients.

Notre étude ne montrait pas la fréquence des échanges ni le type de suivi en tant que facteur prédictif d'un moyen de communication sécurisé. Nous aurions pu imaginer qu'un suivi de pathologies chroniques, ainsi qu'une fréquence d'échange importante aurait pu influencer favorablement l'utilisation d'un outil sécurisé.

Au contraire, nous avons prouvé que plus les médecins échangeaient, plus ils utilisaient un moyen non-sécurisé, nous pouvons émettre l'hypothèse que ses moyens de communication non-sécurisés permettaient des échanges plus rapides.

Il aurait été intéressant d'interroger les médecins sur le nombre et le type de formation complémentaire réalisés durant leur cursus, notamment l'obtention d'un diplôme inter-universitaire de télé-médecine, à même de sensibiliser sur ces problématiques sécuritaires.

Il aurait été intéressant également de comparer les messageries instantanées entre elles afin de prouver la supériorité d'une par rapport à l'autre.

Enfin, nous avons choisi de ne pas effectuer la régression logistique sur les facteurs prédictifs du choix de Predice PRO, car nous avons conscience qu'il s'agit d'un nouvel outil. Il nous a donc paru plus judicieux que cette étude princeps mette en évidence les facteurs prédictifs de l'utilisation d'un outil sécurisé en premier lieu.

c) Données de la littérature

En 2020, *Qin Yong* effectue une étude transversale (8) où il interroge des médecins généralistes utilisant le NEHR qui est un système sécurisé de collecte de données de santé de patient entre plusieurs professionnels de santé. Une **régression logistique** montrait que les médecins généralistes de plus de 40 ans, pratiquant depuis plus de 15 ans et ayant une aisance informatique faible sont moins favorable à l'utilisation des données NEHR, mais la majorité de ses médecins en tiraient un bénéfice dans leur pratique, cela est **comparable aux résultats de notre étude**.

Dans une méta-analyse (32), *Bassi et al.* ont interrogé des utilisateurs et non-utilisateurs de e-santé, en portant une attention particulière sur la **sécurité** et la **confidentialité** des données-patient. Dans les conclusions de cette étude, il apparaît

indispensable d'être rigoureux sur la sécurité de ces informations, notamment à travers un **encadrement législatif** solide du secteur de l'industrie. Ils rapportent que les utilisateurs de e-santé devraient être formés convenablement afin de trouver un équilibre : vers une pratique centrée patient et la préservation de leur vie privée, tout en permettant une coordination des soins entre professionnels de santé. Selon cette étude, l'urgence dans ce genre de communication est de trouver une façon sécurisée de récupérer le **consentement** du patient.

Il est indispensable d'être attentif aux **conditions d'utilisation** des applications de messagerie instantanée, leur politique de confidentialité et de revente de données y étant en général précisées.

Pour exemple, la maison mère de WhatsApp est l'entreprise FACEBOOK. Ce géant numérique spécialisé dans la **vente de données personnelles** a été condamnée à une amende de près de 5 milliards de dollars par l'autorité fédérale de la régulation des communications en 2019, cela a permis la mise en place d'un comité de protection de la vie privée. Le fait que WhatsApp apparaissant en deuxième position des moyens de communication les plus utilisés dans notre étude, devrait nous alerter sur nos pratiques.

Concernant **l'hébergement des données**, une plainte d'un syndicat professionnel médical français a été déposée auprès du Conseil d'Etat contre Doctolib. Ce dernier avait recours à l'hébergeur américain Amazon Web. Dans cette plainte, il était accusé de risques d'accès aux données personnelles des patients français par les autorités américaines (13). Face à cette plainte, le Conseil d'Etat a maintenu son partenariat de prise de rendez-vous de vaccination pendant l'épidémie SARS COV2 en relevant que les données recueillies dans le cadre des rendez-vous ne comprenaient pas de données de santé sur les motifs médicaux, et que toutes les garanties de sécurité avaient été mise en place par la société Doctolib. Les médecins devraient donc s'interroger sur l'implication des entreprises privées dans le domaine médical.

Avant de choisir son moyen de communication, le médecin généraliste doit être attentif aux obligations des autorités nationales en termes de sécurité, afin de

respecter son devoir de protection envers la vie privée de ses patients. **Le score e-SS pourrait être une aide afin d'effectuer ce choix.**

2. Discussion de la méthode et significativité clinique

a) Points forts de l'étude

Parmi les lignes de force, il s'agit d'une **étude** prospective, multicentrique, réalisée dans les Hauts de France à la fois en milieu rural et urbain. Nous avons donc choisi de prendre en compte les différentes pratiques de la médecine générale.

Dans les modalités de réponse au **questionnaire**, l'avis neutre compris dans la mention "Non Applicable" avait pour attribution un score médian, cela a permis de ne pas sous-estimer les scores attribués aux différents moyens de communication. Malgré cette précaution, nous avons prouvé la supériorité de Predice PRO.

Notre **population** par son faible effectif n'était pas représentative de la population générale, mais certaines de ses caractéristiques étaient semblables aux caractéristiques des médecins des Hauts-de-France. En effet, selon *l'Atlas de la démographie médicale en France* (39), les médecins exerçant dans les Hauts-de-France ont en moyenne autour de 45 ans, et sont en majorité des hommes.

Les **critères d'inclusion** de notre étude ont permis d'extraire une population homogène et comparable. En effet, parmi les caractéristiques de notre population : dans les deux groupes l'âge moyen était autour de 41 ans, les médecins exerçaient de façon équitable en zone urbaine et rural/semi-rural, la grande majorité avait un exercice libéral stricte, ainsi qu'une aisance informatique moyenne à bonne. Ils communiquaient surtout avec des infirmiers libéraux.

Une partie de notre travail a consisté en **l'élaboration d'un Score e-SS**, qui est né de l'alliance entre le *Benefits Evaluation*, qui est un score validé dans la littérature canadienne (33), et les règles RGPD de la législation française. Il faudrait standardiser ce questionnaire à l'aide d'études complémentaires de plus grande ampleur.

La qualité des données utilisées via les **covariables pertinentes** est à souligner, ces covariables ont été choisies de façon précautionneuse dans les analyses statistiques au travers de notre bibliographie.

Enfin, le recueil de données a été effectué **après un recul d'une année d'utilisation de Predice PRO**, permettant un avis objectif basé sur une longue expérience de la messagerie.

b) Points faibles de la méthode

Biais de sélection :

La procédure de recrutement a eu lieu via l'envoi d'email exclusivement aux maîtres de stage universitaire, dont la pratique peut différer des confrères de la spécialité. De plus, ils ont pu être intéressés particulièrement par le sujet, les MSU ayant en général un intérêt particulier pour les thèses de doctorat.

Biais de déclaration :

Concernant le questionnaire, le score e-SS était estimé par les médecins généralistes, leurs réponses étaient donc subjectives. Pour exemple, les professionnels de santé y avaient répondu à l'aune de leur connaissance sur les règles du RGPD, et des conditions d'utilisation de leur outil de communication (lieu d'hébergement des données, notion de vente de données personnelles...).

Faible taux de réponse :

Les résultats sont à interpréter avec précaution du fait du **taux de réponse à 18%**, pouvant s'expliquer en partie par la faible utilisation de Predice Pro selon les données d'utilisation de l'URPS.

c) Conflit d'intérêt :

Une partie de la documentation (concernant Predice PRO) a été fournie par l'URPS-ML-HDF, mais la création des questionnaires, une partie de la diffusion ainsi que l'analyse statistique ont été réalisées de manière indépendante.

3. Perspectives

a) Vers l'application des autres propositions de l'Ordre des médecins (2)

L'Ordre des médecins, avait émis plusieurs suggestions :

- L'existence d'un annuaire des adresses électroniques professionnelles en tant que reflet du tableau de l'Ordre : c'est le nommage ordinal de l'adresse électronique, non encore généralisé ni codifié au niveau national.
- La responsabilité de l'émetteur et du destinataire au travers des messageries instantanées reste à codifier. La traçabilité des flux de messagerie pourrait avoir lieu au travers d'un dispositif de notariation. Il s'agira d'une preuve des échanges entre émetteur et destinataire sur les messageries instantanées, accompagnée de leur horodatage.

- La mise en place de carte électronique d'identité professionnelle, afin de généraliser l'utilisation de la carte e-CPS. Une authentification forte au travers de cette carte e-CPS pourrait améliorer la rapidité de la connexion tout en maintenant le même niveau de sécurité.
- L'intégration de la messagerie instantanée sécurisée aux logiciels-métier de gestion des dossier-patients en libéral.

La pandémie SARS COV 2 a permis la mise en place d'outils numériques afin de rassembler des groupes d'échange de pratique. Une étude italienne (35), a mis en évidence l'utilisation des réseaux sociaux par les professionnels de santé durant la pandémie, cela prouvait la nécessité des outils numériques pour communiquer rapidement. Il devient urgent d'organiser leurs développements dans la communauté médicale.

b) Vers la standardisation des règles que doivent suivre les éditeurs

L'Interopérabilité des données de santé dépend des prestataires-éditeurs qui se lient les uns aux autres. La standardisation de cette interopérabilité permettrait au centre de santé de naviguer d'une application sécurisée à une autre avec plus de facilité et au travers de tarifs conventionnés sur tout le territoire.

Exemple : un logiciel de laboratoire pourrait s'interopéabiliser avec n'importe quel logiciel-métier de dossier-patient. De même, tous les logiciels-métier devraient être compatibles avec MON ESPACE SANTÉ gratuitement.

Les sous-traitants sont de plus en plus responsabilisés, ils doivent garantir le respect de la réglementation française et européenne en termes de sécurité et confidentialité des données.

c) Vers le consentement des patients au travers des échanges entre professionnels sur les messageries instantanées

Le consentement des patients et leur vision de la e-santé seraient intéressants à étudier en France (28, 29, 30). Le consentement devrait être recueilli sur les applications d'échanges de données-patient de manière formalisée.

De plus, **MSS citoyenne** est une messagerie sécurisée citoyenne qui verra le jour en 2023 : l'objectif est de placer l'utilisateur au centre de sa prise en charge (11). Cette messagerie permettra les échanges entre les médecins et leurs patients.

d) Vers la programmation de nouvelles fonctionnalités sur Predice PRO

- L'établissement du **NIR (numéro de sécurité social)** est en cours de programmation, en tant qu'intitulé des conversations instantanées permettant un risque quasi nul d'erreur d'identité.
- Une solution pour les modalités de **consentement électronique** des patients est en cours d'installation. Cela permettra au patient d'exercer leur droit d'opposition ; et d'autoriser l'entrée aux professionnels de leur choix au sein du cercle de confiance en temps réel (via un système de validation SMS).
- Si le patient dispose d'un dossier de coordination PREDICE (qui est un dossier médical partagé régional dans les Hauts-de-France) il sera possible d'accéder aux documents des patients (CR, prescriptions, synthèse...) via la messagerie instantanée.

e) Vers la formation des médecins dans le Numérique en Santé :

Une formation des futurs médecins à la maîtrise des technologies et des outils de communication d'information médicale devient une nécessité (2).

Une formation au choix judicieux du logiciel métier et d'une messagerie sécurisée semble primordiale.

Une étude de comparaison des logiciels-métier serait intéressante à réaliser afin qu'elle soit enseignée dans les facultés de médecine.

On peut imaginer également la création de formation pratique à l'utilisation des outils tels que les différents logiciel-métier, logiciel de téléconsultation, et de téléexpertise. Nous permettant ainsi d'effectuer un choix éclairé, à l'aune de nos connaissances acquises lors de nos études, en plus de celle enseignée en tant qu'interne SASPAS par nos différents MSU et lors de nos échanges de pratique. Des formations spécifiques effectuées par les créateurs d'outils numériques pourraient ainsi voir le jour.

La formation des médecins a été étudiée dans le recueil d'*Ali Zarzour* (33). Ces professionnels se formaient en majorité en présentiel plutôt qu'en ligne, la majorité en tirait un bénéfice et en était satisfaite. Ils en percevaient un effet bénéfique qui remet au centre la prise en charge du patient, ainsi que sa sécurité.

f) Vers l'incitation financière pour les médecins généralistes

Dès 2023 un logiciel de gestion de cabinet référencé SEGUR deviendra un pré-requis au versement du forfait structure. Ce forfait structure sera conditionné au fait :

- De remplir la partie « synthèse médicale » du DMP dans Mon espace santé ;
- D'utiliser une messagerie électronique sécurisée MSSanté ;
- D'utiliser la e-prescription via la version dématérialisée de la carte vitale ApCV.

Elle pourra être comprise entre 2000 et 3600 euros par an. Cette aide financière sera généralisée sur tout le territoire pour les médecins généralistes.

g) Vers l'acceptation des contraintes de sécurité

Dans une étude cross-over, *Chhanabhai et al.* ont interrogé 400 usagers néo-zélandais afin d'analyser l'opinion publique (27). Les résultats principaux indiquaient qu'ils étaient capables d'accepter la transition du numérique en santé tant que les conditions de sécurité étaient réunies.

Une dizaine d'années plus tard, les problèmes de sécurité sont partiellement résolus mais d'autres obstacles s'annoncent : notamment l'acceptation des contraintes de sécurité par les médecins généralistes. Les médecins sont-ils prêts à les accepter ?

L'ergonomie dans l'usage de ses outils de e-santé selon l'exercice libéral est une priorité pour les médecins généralistes. Dans leur pratique, ils ont besoin de normaliser la qualité de leurs échanges afin d'améliorer la coordination des soins tout en améliorant la fluidité de leur travail.

Pour analyser cette problématique, le Score e-Santé contient un **sous-score e-Santé Satisfaction** (nommé **Score globale d'évaluation**) faisant l'objet de la thèse de Chahrazad Kheder et permettant d'évaluer la satisfaction des professionnels de santé utilisant la messagerie instantanée Predice PRO.

CONCLUSION

A ce jour, la sécurisation des outils numériques en santé ainsi que leur comparaison n'est pas évaluée par la communauté médicale en France.

Ce travail est une comparaison des différents moyens de communication utilisés par les médecins généralistes des Hauts-de-France concernant leur sécurisation.

Nous avons prouvé que le niveau de sécurité de la messagerie Predice PRO est supérieur aux autres moyens de communication.

Des études de plus grande ampleur pourraient permettre notamment de mettre en évidence d'autres caractéristiques des médecins généralistes n'utilisant pas un moyen de communication sécurisé, afin que le ministère de la santé puisse répondre efficacement à ses problématiques.

Enfin, la formation des futurs médecins semble indispensable afin qu'ils puissent choisir les meilleures options en termes d'outils numérique.

REFERENCES

- (1) Securing shared medical records, la sécurisation du dossier partagé, A. MARCELLI, D. SOLARET, Science Direct, Bull Acad Méd, 2010, 194, numero4, 767-778
- (2) LUCAS J. L'information de la santé : le livre blanc du conseil national de l'Ordre des médecins, mai 2008
- (3) The Role of Text Messaging and TeleHealth Messaging Apps, Sashikumar Ganapathy, et al
- (4) Giordano V, Koch H et al : WhatsApp messenger as an adjunctive tool for telemedicine : an overview. Interact J Med Res 2017
- (5) Electronic Communication of protected health information : privacy, security and HIPAA Compliance, Brian C. Drolet et al, The journal of hand surgery, june 2017, page 411-416
- (6) WhatsApp in clinical practice : a literature review, Maurice MARS, Richard E SCOTT
- (7) Bouamrane MM, Mair FS. A study of general practitioners' perspectives on electronic medical records systems in NHSScotland. BMC Medical Informatics and Decision Making. 2013 May;13 :58.
- (8) Qin Yong S. Attitudes and Perceptions of General Practitioners towards the National Electronic Health Record (NEHR) in Singapore; 2020. Library Catalog : www.emjreviews.com Section : Uncategorised.
- (9) Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare : how safe are we ? BMJ. 2017 Jul;358. Publisher : British Medical Journal Publishing Group Section : Analysis.
- (10) Ahern, D. K., Kreslake, J. M., & Phalen, J. M. (2006). What is eHealth (6): perspectives on the evolution of eHealth research. J Med Internet Res, 8
- (11) mssante.fr/ps/medecinG, esante.gouv.fr
- (12) Mailiz : <https://mailiz.mssante.fr>
- (13) Conseil-etat.fr :
Le juge des référés ne suspend pas le partenariat entre le ministère de la santé et doctolib pour la gestion des rendez-vous de vaccination
- (14) Legifrance.gouv.fr et esante.gouv.fr
- (15) Canada Health Infoway
<https://www.infoway-inforoute.ca/en/component/edocman/2911-methodology-for-administering-a-system-and-use-survey/view-document?Itemid=101>
- (16) Conseil du numérique en santé
<https://esante.gouv.fr/actualites/conseil-du-numerique-en-sante-synthese-du-groupe-de-travail-evaluation-des-benefices-de-la-e-sante>
- (17) Questionnaire canadien sur l'utilisation d'un outil de e-santé
<https://www.infoway-inforoute.ca/en/component/edocman/2907-system-and-use-e-views/view-document?Itemid=101>
- (18) Handbook of eHealth evaluation, University Victoria Colombie Britannique

- https://dspace.library.uvic.ca/bitstream/handle/1828/7814/Lau_Francis_Handbook%20of%20eHealth%20Evaluation_REV%20Oct2017.pdf?sequence=67&isAllowed=y
- (19) Delon, WH (2003), The DeLone and McLean model on information systems success : a ten year update, Journal of management information systems 9-30 , <https://eli.johogo.com/Class/p7.pdf>
 - (20) Guide CNIL / CNOM pour bonnes pratiques relativement données patients <https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf>
 - (21) RGPD et professionnels de santé libéraux : ce que vous devez savoir, juin 2018, CNIL.fr <https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir>
 - (22) Devenir délégué à la protection des données, novembre 2021 : <https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees>
 - (23) Registre CNIL, RGPD https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
 - (24) NIST Special Publication : 800-63-3, Digital Identity Guidelines, Grassi P, Garcia M, Fenton J, US Department of Commerce, June 2017, <https://doi.org/10.6028/NIST.SP.800-63-3>
 - (25) A study of general practitioner's perspectives on electronic medical records systems in NHSScotland, Bouamrane MM, Mair M., BMC Medical Informatics and Decision Making
 - (26) A Holistic Framework to improve the uptake and Impact of eHealth Technologies, Van Gemert Pijnen J, Nijland N, Van Limburg M et al.
 - (27) Chhanabhai, P., & Holt, A. (2007) : Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. Medscape General Medicine, 9 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1924980/>
 - (28) Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001;322:283–287.
 - (29) Hunter I. Patient Attitudes to Electronic Medical Records. Auckland, New Zealand: Privacy Commissioner; 2003
 - (30) Dubow J. National Survey on Consumers' Experiences With Patient Safety and Quality Information. February 24, 2005. Available at: Accessed January 2, 2007
 - (31) Measuring interoperable EHR adoption and maturity : a Canadian example, Gheorghiu Bobby, Gahens Simon, BNM Medical Informatics and decision Making
 - (32) Bassi et al. (2012) Perceived Impact of Electronic Medical Records in Physician Office Practices: A Review of Survey-Based Research
Jesdeep Bassi, F. Lau, M. Lesperance, Published 28 July 2012

- (33) How can improve our understanding of successful implementations in eHealth?
MHD Ali Zarzour, University of manchester, Manchester Business School, 2015
- (34) <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042675720>
- (35) Social media as a tool for scientific updating at the time of COVID pandemic:
Results from a national survey in Italy
Rita Murri 1 2, Francesco Vladimiro Segala 3, Pierluigi Del Vecchio 3, Antonella Cingolani 1 2, Eleonora Taddei 1 2, Giulia Micheli 3, Massimo Fantoni 1 2, COVID II Columbus Group
- (36) <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706>
- (37) Délibération SAN-2020
<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042675720#:~:text=Par%20une%20d%C3%A9cision%20du%202022,disposait%20d%C3%A9j%C3%A0%20la%20CNIL%20et>
- (38) Guide homologation de sécurité de l'ANSSI
https://www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_eta_pes.pdf
- (39) Atlas de la démographie médicale en France, Dr Patrick Bouet, Dr Jean-françois GÉRARD-VARET, Ordre national des médecins
https://www.conseil-national.medecin.fr/sites/default/files/external-package/analyse_etude/11jksb5/cnom_atlas_demographie_medicale_2022_tome_1.pdf

ANNEXES

Sécurité des échanges entre Médecins Généralistes et Paramédicaux.

Utilisez-vous la messagerie instantanée PREDICE PRO ?

- oui
 non

Quel est le moyen de communication interprofessionnelle que vous utilisez le plus souvent ?

Conversation téléphonique	SMS ou MMS	Email personnel
Email professionnel	Fax	Courrier postal
MSSanté (Apicrypt,Mailiz)	Proton Mail	DSIH
Lifen	Autre	

Autre :

Quelle messagerie instantanée utilisez-vous le plus souvent pour vos échanges interprofessionnels ?

WhatsApp	Messenger	Hangout
Viber	Wickr	Signal
Telegram	Obvid	Idomed
DoctolibTeam	PredicePRO	Autre

Autre :

Parmi les deux réponses choisies ci-dessus, utilisez-vous le plus souvent :

<input type="radio"/> Le moyen de communication usuel (réponse à la question 2)
<input type="radio"/> La messagerie instantanée (réponse à la question 3)

Concernant votre moyen de communication privilégié, indiquez le degré d'accord ou de désaccord :

	Parfaitement d'accord	Plutôt d'accord	Modérément en désaccord	En total désaccord	Non Applicable
L'accès est verrouillé (ex : verrouillage de l'appareil, code chiffré, reconnaissance faciale...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
La sécurisation de la connexion possède une authentification à double facteur (mot de passe et envoi d'un code de confirmation par SMS ou email)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Les paramètres d'authentification sont de bonne qualité (ex: mot de passe fort, absence de connexion automatique, changement régulier de mot de passe...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
L'utilisation de votre carte CPS pour l'identification est possible	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre session se verrouille automatiquement en cas d'inactivité	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen de communication respecte le Règlement Général sur la Protection des Données-Patient (RGPD)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A votre connaissance, l'hébergement des données relatives au patient est assuré par un « Hébergeur de données de santé » qui relève de la législation européenne	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Je sais à qui m'adresser en cas de problème concernant les données-patient (Délégué de la protection des données)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lorsque j'initie un échange interprofessionnel, je suis certain de l'identité de mon interlocuteur (l'identité est vérifiée)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen de communication n'est accessible qu'aux professionnels de santé	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen de communication est utilisé uniquement dans l'exercice du soin (pas de confusion possible entre échanges personnels et professionnels)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
D'après vous, l'utilisation de votre moyen d'échange respecte le secret médical	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen d'échange offre la possibilité pour les patients de visualiser l'historique d'accès aux informations de santé les concernant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
L'obtention du consentement du patient pour initier un échange interprofessionnel est une option possible	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Une restriction d'accès aux données partagées par des Sources Externes est garantie (piratage potentiel, vol de données, espionnage...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen d'échange facilite le partage d'informations concernant le patient au sein de l'équipe soignante de façon sécurisée	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Votre moyen d'échange facilite le partage de documents au sein de l'équipe soignante de façon sécurisée	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Il existe une restriction d'accès pour les personnes n'appartenant pas au cercle de soin	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Au sein du cercle de soin, le partage des données-patient respecte les différents niveaux de confidentialité (normal, restreint, privé) selon le type de professionnel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
J'estime avoir confiance en mon moyen d'échange quant au non-partage et la non-vente des données patients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Terminons avec quelques informations démographiques vous concernant : Quelle est votre profession ?

- Médecin Généraliste
- Médecin Généraliste Remplaçant
- Interne en Médecine Générale Remplaçant
- Interne en Médecine Générale non-remplaçant
- Médecin d'autre spécialité médicale
- Interne d'autre spécialité médicale

Quelle type d'activité exercez-vous ?

- Libéral
- Salarié
- Mixte à prédominance libérale
- Mixte à prédominance hospitalière

Quel âge avez-vous ?

Quel est votre genre ?

- Féminin
- Masculin

Quel est votre lieu d'exercice libéral ? (Code postal et Ville)

Cochez les réponses qui décrivent le mieux la zone où vous exercez

- Zone urbaine
- Zone rural
- Zone semi-rural
- ZAC
- ZIP
- ZAR

Quels outils de communication utilisez-vous régulièrement dans votre pratique libérale ?

- Téléphone personnel
- Téléphone professionnel
- Ordinateur de bureau
- Ordinateur portable
- Tablette
- Montre ou bracelet connectés

Comment qualifieriez-vous votre aisance avec les outils informatiques ?

- Mauvaise
- Passable
- Moyenne
- Bonne
- Excellente

Lors de votre pratique libérale, quel est le nombre moyen de patients que vous prenez en charge quotidiennement?

- Entre 1 et 10
- Entre 10 et 15
- Entre 15 et 20
- Entre 20 et 30
- > 30 par jour

Lors de votre pratique libérale, combien de visites à domicile par jour effectuez-vous ?

- 0
- Moins de 5
- Entre 5 et 10
- >10

Lors de votre pratique libérale, combien de téléconsultations effectuez-vous par jour ?

- 0
- Entre 1 et 5
- Entre 5 et 10
- >10

Concernant votre patientèle, vous estimez qu'elle est constituée majoritairement de (3 réponses possibles)

Enfants 0-18 ans	Adultes jeunes 18- 30 ans	Adultes 30-65 ans
Seniors > 65 ans	Patients âgés > 75 ans polypathologiques	Patient âgé dépendant en EHPAD
Femmes	Hommes	Équivalent en terme de genre

Quelle est la durée moyenne d'une consultation ?

- Entre 5 et 15 minutes
- Entre 15 et 20 minutes
- Entre 20 et 30 minutes
- > 30 minutes

Quels sont les motifs de consultation les plus fréquents ?

SUITE
AIGU
Les deux, de manière équivalente

Quelle est votre fréquence d'échanges interprofessionnelles (notamment avec les infirmiers, kinésithérapeutes, pharmaciens etc...) sur les 6 derniers mois ?

- Au moins une fois par jour
- Plusieurs fois par semaine
- Une fois par semaine
- Plusieurs fois par mois
- Une fois par mois

Avec quels types de professionnels de santé communiquez-vous le plus souvent ? (plusieurs réponses possible)

Autre Médecin Généraliste	Médecin Libéral d'autre spécialité	Médecin Hospitalier d'autre spécialité
Interne en Médecine Générale	Interne d'autre spécialité médicale	Infirmier Libéral
Infirmier Hospitalier	Masseur-Kinésithérapeute	Auxiliaire de vie
Pharmacien	Sage Femme	Biologiste
Autre		

Autre :

De façon générale, j'échange le plus souvent :

Dans un cadre urgent nécessitant une réponse rapide (dans l'heure) à une question d'un confrère médecin ou paramédical

Dans un cadre non urgent ne nécessitant pas de réponse rapide

Dans les 2 cadres de manière équivalente

Quelles sont les motifs de vos échanges interprofessionnels ? Cochez les trois motifs les plus fréquents

Création d'une discussion autour d'un patient	Création d'une discussion autour d'une prise en charge (ex suivi patient chronique, suivi de plaies, adaptation thérapeutique, etc.)	Demande de RCP
Demande d'avis spécialisé	Demande d'avis d'un autre confrère (même spécialité)	Partage de connaissances (éducation interprofessionnelle)
Mise à jour des recommandations et pratiques professionnelles (ex: consignes d'isolement COVID)	Création d'une discussion autour de l'organisation de la CPTS (coordination, protocolisation des soins... etc)	Récupération d'informations médicales avec le milieu hospitalier (ex: préciser les traitements, le mode de vie du patient, récupérer les comptes-rendus d'hospitalisation...)

Annexe 1. Questionnaire utilisé lors du recueil de données, logiciel Sphinx Declic.

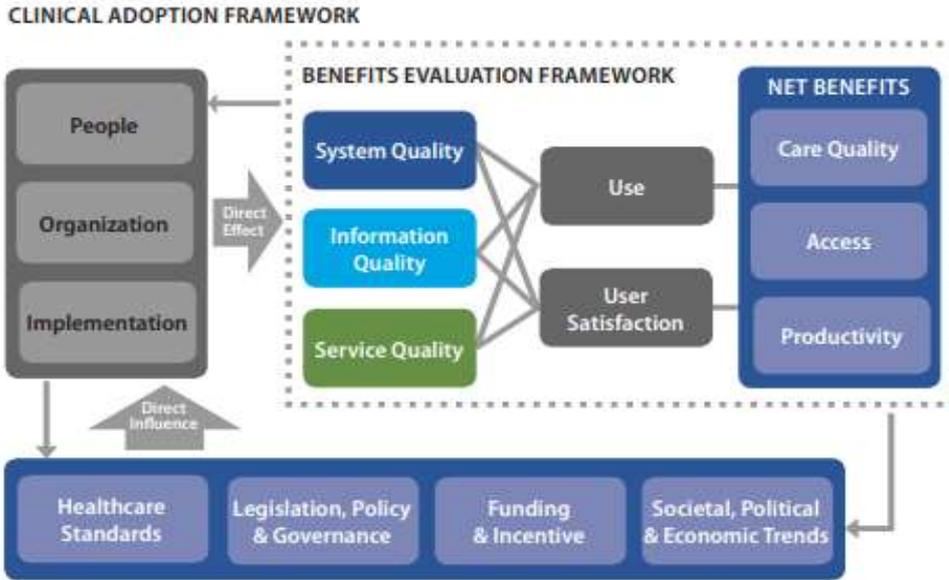


Figure 3.3. Clinical adoption framework with its micro, meso and macro dimensions.

Note. From "From benefits evaluation to clinical adoption: Making sense of health information system success in Canada," by F. Lau, M. Price, and K. Keshavjee, 2011, *Healthcare Quarterly*, 14(1), p. 41. Copyright 2011 by Longwoods™ Publishing Corp. Reprinted with permission.

Annexe 2. Evaluation du bénéfice d'un outil de e-santé : Benefits Evaluation
 Site : *Hanbook of ehealth*

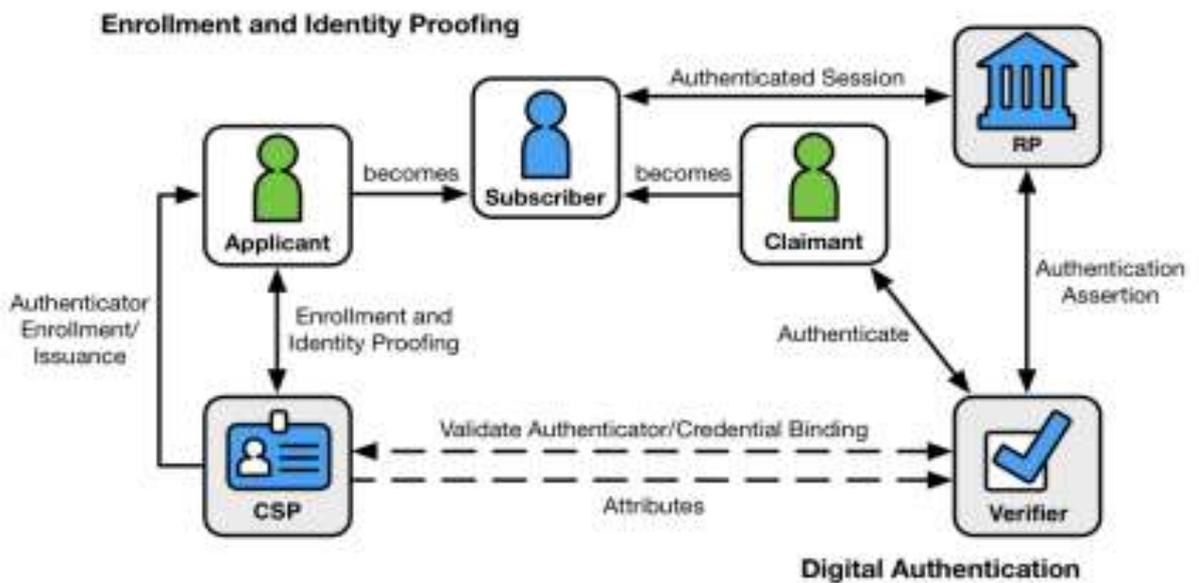


Figure 4-1 Digital Identity Model

Annexe 3. NIST, Authentification à double facteur.
 Site : *Handbook of eHealth*

Prédice est un bouquet de services régional : aucune donnée n'est revendue ou utilisée à des fins commerciales.

Prédice en toute confiance

Prédice respecte ma vie privée

- Pour plus de **transparence**, je peux consulter toutes les informations en rapport à la **protection de mes données** sur www.predice.fr

Prédice protège mes données

- Mes données de santé sont **stockées en France**, chez un **hébergeur certifié** par le Ministère de la Santé
- Seuls les **professionnels intervenant dans ma prise en charge** sont autorisés à accéder à mes données

Prédice requiert mon consentement

- Je **reçois une information adaptée** me permettant de **consentir** à l'utilisation de Prédice en toute connaissance de cause

Prédice protège mes droits

- Je **peux retirer mon consentement** à tout moment
- Je **peux faire valoir l'ensemble de mes droits** sur mes données sur www.predice.fr

Pour en savoir plus sur mes droits et mon consentement, je scanne le **QR Code** avec mon smartphone ou je vais sur www.predice.fr



Ce projet est cofinancé par l'Union européenne avec le Fonds européen de développement régional (FEDER)



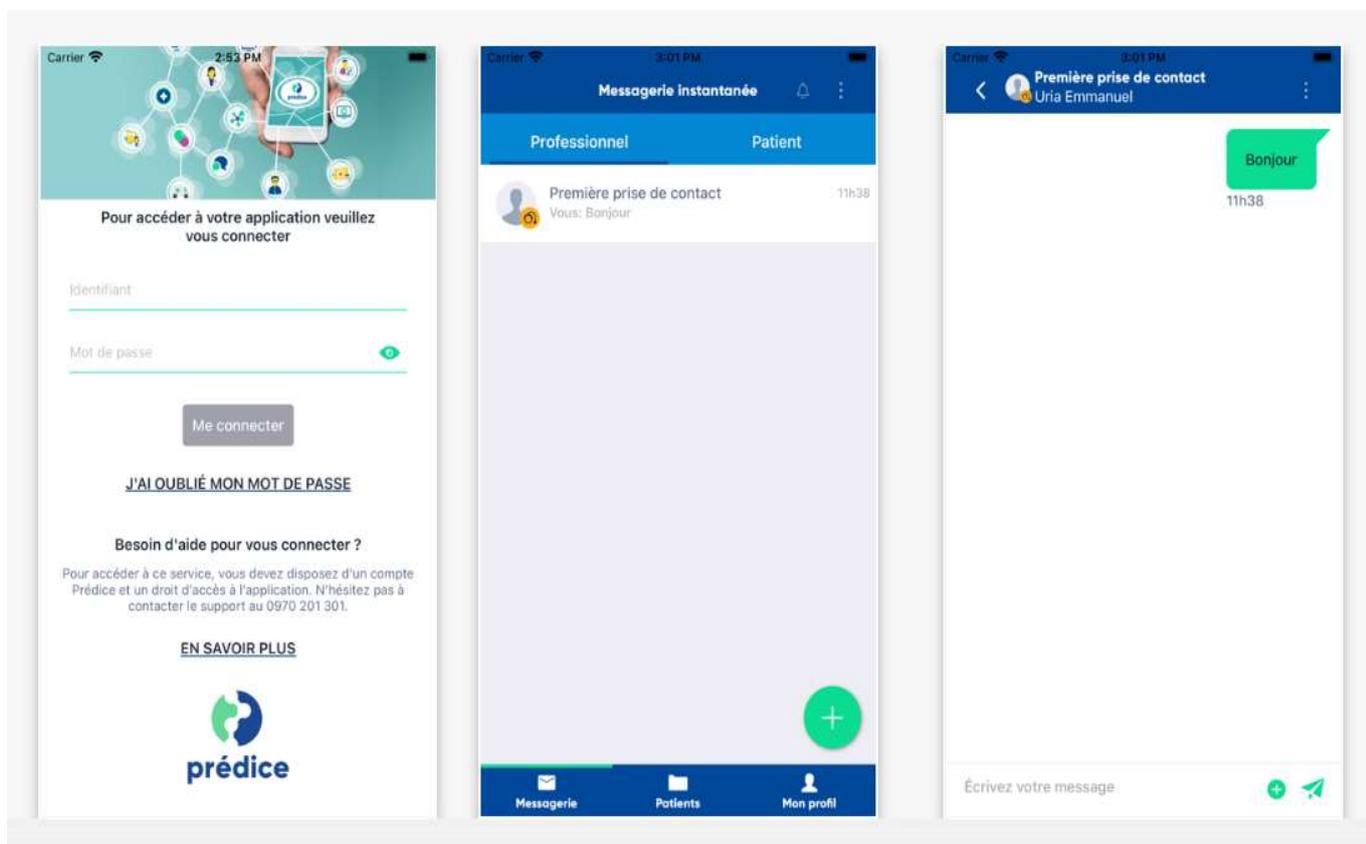
Version 1 - © Sant& Numérique Hauts-de-France 2020, Tous droits réservés

Annexe 4. PREDICE, équivalent MONESPACESANTE au niveau régional
Site : Predice.fr

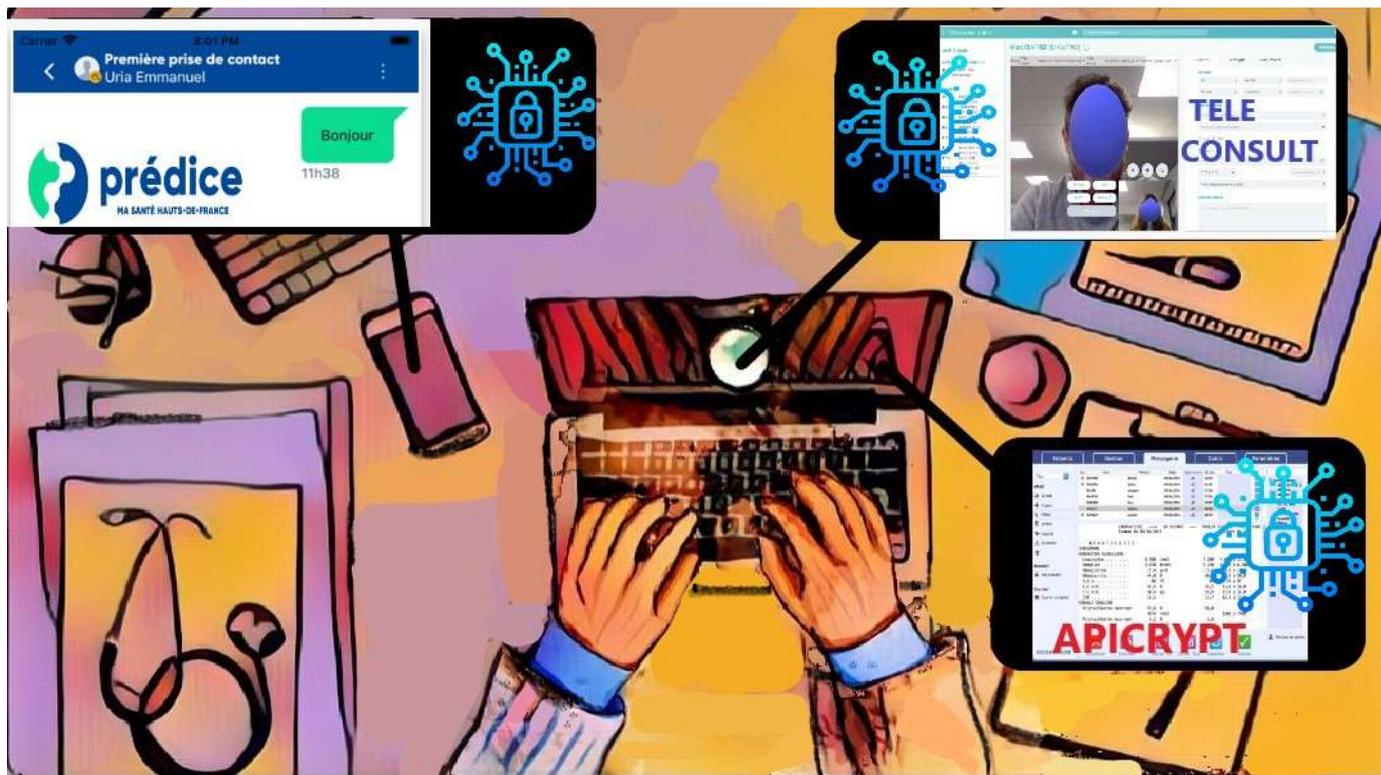
Prérequis d'utilisation de "Prédice Pro"

1. L'utilisateur doit être équipé d'un smartphone  connecté au WIFI ou connecté à la 4G
2. L'utilisateur doit avoir téléchargé gratuitement Prédice Pro   
3. L'utilisateur doit être inscrit à Prédice  [Lien d'inscription www.predice.fr/kiosque_pro](http://www.predice.fr/kiosque_pro)
4. L'utilisateur peut ensuite ouvrir l'application  Ouvrir l'application
5. L'utilisateur peut se connecter  Se connecter

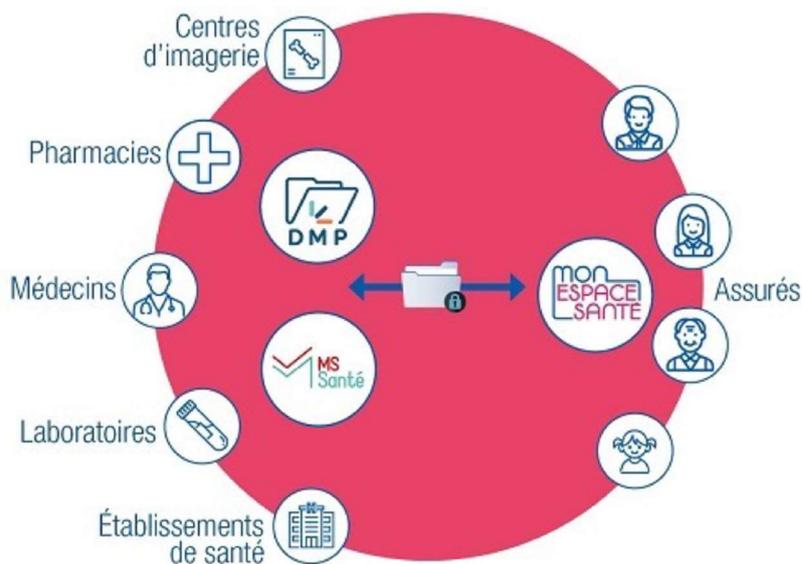
S&N-HDF



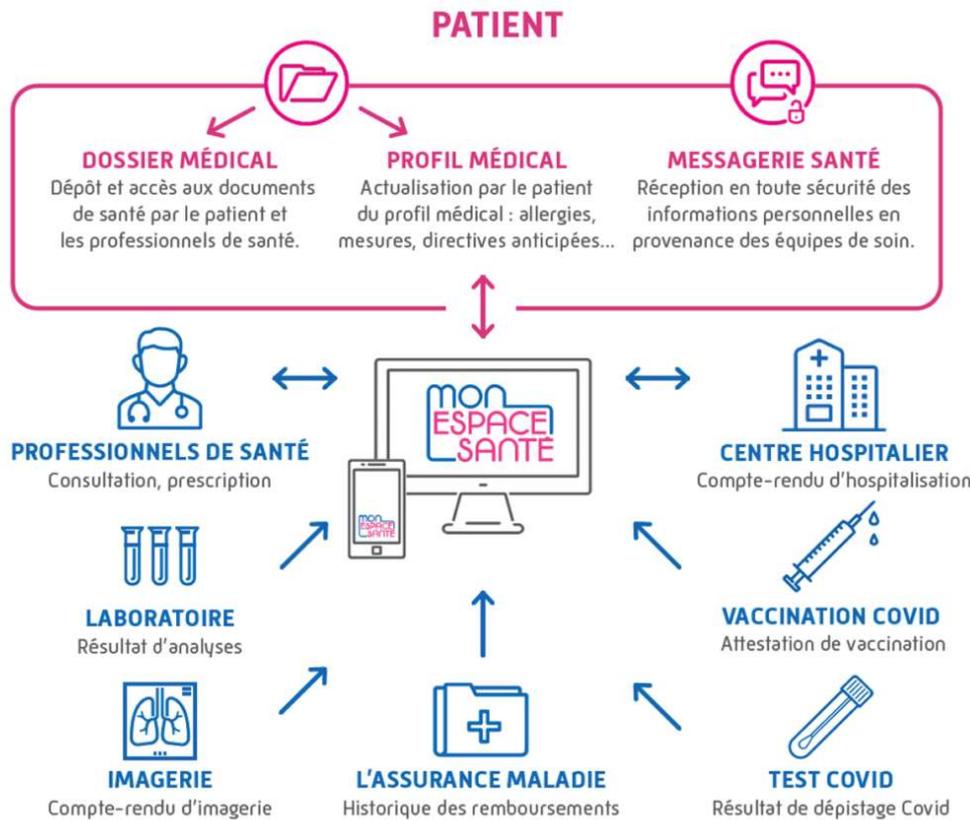
Annexe 5. Messagerie instantanée Prédice PRO
Source : Predice.fr, documentation URPS



Annexe 6. Exemples de services socles sécurisés utiles au Médecin Généraliste : la messagerie instantanée Predice PRO, la messagerie électronique Apicrypt, le service de téléconsultation Maiaia.



Annexe 7. Messagerie électronique MSSanté : schéma de son interopérabilité avec mon espace santé. Partager des informations et des documents de santé en toute sécurité.



Tout ce qui se trouve sur "Mon Espace Santé"

- Professionnels de santé**
Consultation, prescription
- Laboratoire**
Résultats d'analyses
- Imagerie**
Compte-rendu d'imagerie
- Assurance maladie**
Historique des soins
- Centre hospitalier**
Compte-rendu d'hospitalisation
- Vaccination COVID**
Attestation de vaccination
- Test COVID**
Résultat de dépistage Covid

Annexe 8. MON ESPACE SANTÉ : Dossier médical partagé permettant une bonne coordination entre les professionnels de santé : médecins généralistes, pharmaciens, laboratoires, services d'imagerie, services d'urgence et autres services hospitaliers. Site : Mon Espace Sante.fr

AUTEUR : Nom : GUEFIF **Prénom :** SAFIYA

Date de Soutenance : 02/02/2023

Titre de la Thèse : Evaluation de la sécurisation des données de santé de la Messagerie Instantanée Interprofessionnelle Predice PRO : comparaison entre les Médecins Généralistes utilisateurs et non-utilisateurs des Hauts-de-France.

Thèse - Médecine - Lille 2023

Cadre de classement : Médecine Générale **DES + FST ou option :** Médecine Générale

Mots-clés : Sécurité, RGPD, Messagerie instantanée interprofessionnelle, e-Santé, Médecine Générale, Predice PRO

Résumé :

Contexte : En 2022, le SEGUR de la santé promeut le virage numérique notamment dans la coordination des soins. Les relations interprofessionnelles impliquent des échanges de données-patient, pour cela des solutions émergent au travers de messageries instantanées sécurisées telle que Predice PRO.

Matériel et Méthodes : Il s'agit d'une étude observationnelle, transversale et quantitative, réalisée de façon prospective. Elle est multicentrique, menée dans les Hauts-de-France pour des médecins généralistes interrogés entre juin et septembre 2022. Le critère de jugement principal est la comparaison du Score e-Santé Sécurité (e-SS) entre les utilisateurs et non-utilisateurs de Predice PRO. Les critères de jugement secondaires sont la comparaison de ce même score entre les messageries sécurisées et non-sécurisées, entre Predice PRO et les autres messageries sécurisées et enfin la recherche de facteurs prédictifs de l'utilisation d'un moyen de communication sécurisé ou non.

Résultats : 81 professionnels de santé étaient inclus (21 dans le groupe Predice PRO, et 60 parmi les non-utilisateurs). On notait une augmentation de 16.6 points ($p < 0.001$) au profit du groupe utilisateurs de Predice PRO et une augmentation de 21.2 points ($p < 0.001$) au profit du groupe moyen de communication sécurisée. Les scores e-SS des utilisateurs de Predice PRO et des autres moyens sécurisés étaient comparables. Le modèle de régression logistique identifiait l'excellente aisance informatique en tant que facteur prédictif de l'utilisation d'un moyen de communication sécurisé.

Conclusion : Nous avons prouvé l'augmentation du Score e-Santé Sécurité estimé par les médecins généralistes chez les utilisateurs de Predice PRO. Des études de plus grande ampleur pourraient permettre l'étude plus approfondie de la sécurisation des outils numériques en santé dans la communauté médicale en France.

Composition du Jury :

Président : Monsieur le Professeur Marc HAZZAN

Asseseurs : Monsieur le Professeur Nassir MESSAADI

Directeur : Madame la Doctoresse Isabelle BODEIN