Organisation du réseau informatique à l'officine : enjeu de la protection des données patients

Maxime Vdovytsya

université de BORDEAUX

U.F.R. DES SCIENCES PHARMACEUTIQUES

Année 2020 Thèse n°153

THESE POUR L'OBTENTION DU

DIPLOME D'ETAT de DOCTEUR EN PHARMACIE

Présentée et soutenue publiquement

Par VDOVYTSYA, Maxime

Né le 28 août 1993 à Kharkiv (Ukraine)

Le 9 décembre 2020 à 18h00

ORGANISATION DU RESEAU INFORMATIQUE A L'OFFICINE : ENJEU DE LA PROTECTION DES DONNEES PATIENTS

Sous la direction de : Brice AMADEO

Membres du jury :

Dr FORFAR Isabelle, présidente du jury

Dr AMADEO Brice, directeur de thèse

Dr COURTOIS Arnaud, membre du jury

Dr FREDERIC Rebecca, membre du jury

Remerciements

Au Dr Brice AMADEO, je vous remercie d'avoir accepté d'être mon directeur de thèse, et de m'avoir aidé dans sa réalisation.

Au Dr Isabelle FORFAR, d'avoir accepté de présider la soutenance de ma thèse.

Au Dr Arnaud COURTOIS et au Dr Rébecca FRÉDÉRIC, d'avoir accepté d'être membres du jury de ma soutenance de thèse.

Au Dr Sophie LOISEAU, je vous remercie d'avoir encadré mon stage de fin d'étude. Au Dr Alain BENOIT, au Dr Sylvain OTTIN-PECCHIO et à l'équipe de la Pharmacie Saint Géry, de m'avoir donné la chance de pouvoir faire une analyse d'impact à la pharmacie, et d'illustrer ma thèse avec.

À ma famille, et à ma belle-famille, qui m'ont soutenu et ont cru en moi.

À Maryne, pour ton aide et ton soutien sans faille.

À ma fille, Elisabeth, et mon futur enfant, qui m'ont donné la force et la motivation tout au long de mon parcours.

Table des matières

Table des figures :

Lexique

Adresse IP : adresse Internet Protocol. C'est une suite de 4 nombres entre 0 et 254 séparés par un point. Cette suite montre où se situe un ordinateur, serveur etc. En comparaison, c'est comme une adresse postale mais sur internet.

Chiffrement RSA : du nom de leurs 3 inventeurs, il fonctionne par le biais de 2 clé différente : une pour chiffre, la clé publique et une pour déchiffrer, la clé privée.

IMAP/POP : protocoles réseau permettant d'accéder à ses mails

Internet : réseau informatique mondial accessible au public, on y retrouve le web par exemple.

Malware ou **logiciel malveillant** : logiciel qui nuit à un système informatique. Il peut être développé pour le faire ou non.

Modem : périphérique informatique réseau permettant de transférer des données numériques par le biais analogique. Il permet notamment l'échange de données à travers internet. Depuis le début de ce siècle, il est de plus en plus intègré à un routeur.

NAS : Serveur ayant pour vocation de stocker des données, dans le but par exemple de les sauvegarder.

PDA : Préparation de Doses Administrées. La PDA permet de fabriquer des piluliers personnaliser à destination de patients .

Routeur : périphérique informatique réseau permettant la communication entre plusieurs périphériques informatiques au niveau local.

Serveur : ordinateur, généralement toujours allumé, sur lequel peuvent se connecter plusieurs postes clients, ou peut héberger des sites web.

SMTP : protocole réseau permettant l'envoi de ses mails

Switch Ethernet : commutateur réseau permettant de transférer des flux de données transités sur un câble RJ45 ou fibre et issu de plusieurs points à un seul point différent.

Abréviations

AIPD : Analyse d'Impact relative à la Protection des Données

CJUE : Cours de Justice de l'Union Européenne

CNAM : Caisse Nationale d'Assurance Maladie

CNIL : Commission Nationale de l'Informatique et de Libertés

CPS : Carte de Professionnel de Santé

CSP : Code de la Santé Publique

DCP : Donnés à Caractère Personnel

DMP : Dossier Médical Partagé

DP : Dossier Pharmaceutique

DPO/DPD : Délégué à la Protection des Données traduit de l'anglais Data Protection Officer

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

FAI : Fournisseur d'Accès à Internet

FSE : Feuille de Soin Électronique

HDS : Hébergeur de Données de Santé

HTTP : HyperText Transfer Protocol

IDE : Infirmier(e) diplômé(e) d'État

IMAP : Internet Message Access Protocol

LGO : Logiciel de Gestion d'Officine

LIL : Loi Informatique et Liberté

NAS : Network Attached Server

PIA : Privacy Impact Assessment

POP : Post Office Protocol

RAMAGE : Réseau informatique de l'Assurance MAladie du Régime Général

RGPD : Règlement Général sur la Protection des Données

RSS : Réseau Santé Social

SCOR : SCanerisation ORdonnance

SMTP : Simple Mail Transfer Protocol

1 Introduction

L'histoire de la pharmacie remonte à il y a bien longtemps, aux temps des apothicaires. Depuis cette période lointaine, les sciences pharmaceutiques sont en constante évolution. Avec l'arrivée massive du numérique au cours des deux dernières décennies, les officines ont dû s'adapter aux nouvelles technologies et évoluer vers une informatisation des outils de délivrance et une dématérialisation des documents papiers. Le grand public étant de plus en plus friand de cette nouvelle technologie, surtout depuis les dernières années, il a fallu s'adapter à cette nouvelle demande même au sein des pharmacies d'officine.

Aujourd'hui, toutes les entreprises, qu'elles soient en lien ou non avec la santé, doivent intégrer le numérique dans leurs activités avec une utilisation plus ou moins complexe du numérique. Cette intégration ne s'est pas faite sans mal, et a bouleversé les habitudes des officines et de toutes les structures qui y sont liées. Par exemple, tous les documents et registres écrits à la main sont aujourd'hui, pour la plupart, sous forme dématérialisée, permettant ainsi une réduction de l'utilisation du papier et la place occupée par ces derniers. De plus, l'outil numérique permet une meilleure sécurité de la délivrance, permettant d'éviter les interactions médicamenteuses et les contre-indications.

Les pharmacies d'officine étant des établissements de santé, leurs différents acteurs manipulent donc tous les jours des données liées à la santé. Ces dernières ne sont pas de simples données et sont donc particulièrement sensibles, méritant une attention particulière. Ces informations confidentielles peuvent donc poser potentiellement problème et doivent être protégées. Cette protection ne doit pas

être négligée, et doit suivre certaines précautions. Ainsi l'État a dû mettre en place différents textes pour encadrer l'informatique à l'officine.

La sécurisation de ces données étant primordiale et nécessitant des compétences bien spécifiques, différents prestataires se mirent à développer différentes solutions afin de pouvoir mettre en place des sécurités nécessaires à ces données. Ces prestataires offrent donc une solution clé en main aux pharmaciens et autres professionnels de santé dans le but d'avoir une certaine sécurité des différentes données. Les pharmaciens font donc confiance à leurs prestataires pour être conformes à la loi.

On peut remarquer qu'en officine, on manipule une masse importante de données numériques. Suite à cette constatation, on peut se poser un certain nombre de questions. Est-ce que les réseaux au sein des officines de France sont sécurisés ? Quels outils sont disponibles pour le pharmacien d'officine et sont-ils facilement utilisables au quotidien ?

Dans ce travail de thèse de pharmacie, je tenterai donc de répondre à ces questions qui visent à décrire l'impact du développement des outils numériques dans le milieu officinal. Pour cela, ce travail a été articulé en plusieurs parties. Dans une première partie, je présenterai un bref historique de l'utilisation de l'informatique à l'officine suivi d'un état des lieux du cadre législatif nécessaire pour garantir la sécurité des données. Ensuite, je détaillerai la structure et la complexité que peut avoir un réseau informatique dans une officine. Dans une avant dernière partie, J'illustrerai une mise en application de la sécurité informatique à l'officine à partir des outils mis à disposition pour les pharmaciens avec des exemples concrets. Enfin, je terminerai par des propositions d'axes d'amélioration.

2 Histoire de l'informatique à l'officine

Avant l'avènement de l'ère informatique, à l'officine, les pharmaciens utilisaient le support papier afin d'y inscrire leurs comptes, leur gestion des stocks et leur transmission à l'assurance maladie.

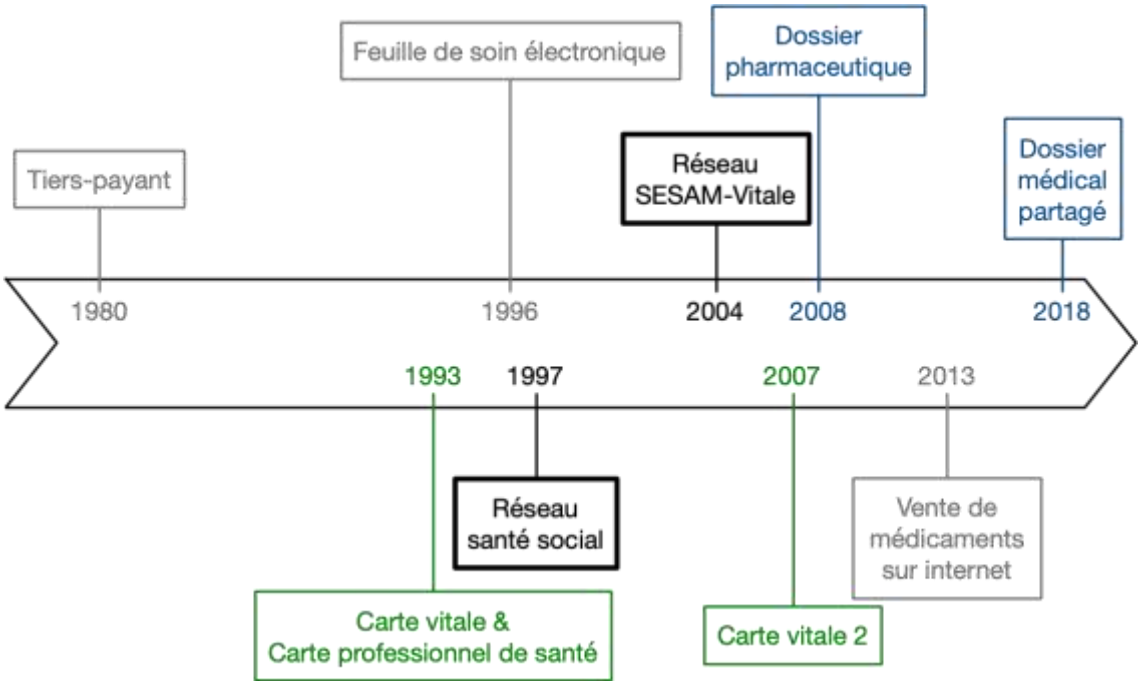


Figure 1 : Numérique à l'officine à travers le temps

Les premiers ordinateurs ayant intégré les officines servaient notamment à gérer le stock plus facilement et à faire les comptes de façon plus automatique. Le tiers-payant n'existant pas à l'époque, les patients payaient leurs médicaments directement aux pharmaciens, il y avait donc peu de documents papiers à transmettre à la sécurité sociale.

La Figure 1 : Numérique à l'officine à travers le temps met en avant le fait que l'ère de l'informatique officinale n'a réellement débuté qu'avec la mise en place du tiers-payant en 1980. Cela est dû à une augmentation considérable de papiers à gérer, étant donné que le nombre de médicaments réglés par l'assurance maladie au

pharmacien est passé de 1/8 au début des années 1980 à 1/3 début des années 1990[1].

Pour éviter d'avoir à envoyer toujours plus de papiers, les transmissions des feuilles de soin vers l'assurance maladie se sont faites par CD-ROM, ce qui a permis d'alléger le travail des pharmaciens. Par conséquent, les différents prestataires des logiciels de gestion des officines, se sont mis à modifier leurs logiciels afin d'y inclure de nouveaux modes de fonctionnement.

Puis, en 1993, la Carte Vitale-SESAM fut officiellement lancée et avec elle vinrent les cartes de professionnel de santé (CPS). Ce fut un véritable tournant de l'informatique officinale débuté 13 ans auparavant, avec une succession de modifications et de lois plus rapprochée. Cependant, ce n'est qu'à partir de 1998, qu'a eu lieu généralisation de ces cartes et du tiers-payant.

Le 25 avril 1996, l'ordonnance n° 96-345 officialisent les Feuilles de Soins Électroniques (FSE). A partir de ce moment, le réseau informatique de l'officine passe d'un réseau local, à un réseau connecté : le réseau propriétaire nommé RAMAGE appartenant à la Caisse Nationale d'Assurance Maladie (CNAM) avec une norme X.25. Ce réseau est rapidement dépassé à cause d'une augmentation rapide du nombre de professionnels de santé utilisant ce réseau et qui envoient de plus en plus de FSE. En 1997 est mis en place le Réseau Santé Social (RSS) basé sur le protocole TCP/IP, qui est le protocole utilisé communément pour le web, augmentant le nombre de connexions simultanées possibles. Puis en 2004, ce réseau est remplacé par Réseau SESAM-Vitale suite à l'expiration de la concession de ce réseau public. En 2014, le système SCOR (SCanerisation ORdonnance) est mis en

[1] Paul Dourgnon et Michel Grignon, « Le tiers-payant est-il inflationniste ? » (CREDES, avril 2000).

place pour toutes les officines, permettant d'envoyer à la sécurité sociale et aux complémentaires de santé toutes les pièces jointes nécessaires à un remboursement correct.

En 2007, la carte vitale 2 remplace la Carte Vitale-SESAM par l'arrêté du 14 mars 2007 relatif aux conditions d'émission et de gestion des cartes d'assurance maladie, avec plus d'informations contenues dans la puce et sur la carte elle-même, notamment la photo d'identité.

La sécurisation des données via la carte CPS et la carte vitale 2 a permis d'obtenir un dossier patient national dans lequel les porteurs des cartes CPS peuvent y noter différentes données. C'est ainsi que le dossier pharmaceutique fut créé le 30 janvier 2007 par la Loi n° 2007-127 et ouvert à toutes les officines par le biais de la délibération de la CNIL n°2008-487 du 2 décembre 2008[2]. Ce dossier pharmaceutique est composé de plusieurs « sous dossiers » : le DP-Patient, le DP-Vaccins, le DP-Rappels, le DP-Alertes, le DP-Ruptures et enfin le DP-Suivi sanitaire. Le DP-Patient permet d'avoir un recul de 4 mois sur les médicaments délivrés et de 3 ans sur les analyses biologiques ; le DP-Vaccins, quant à lui, permet une consultation de 21 ans sur les vaccins. Ces données sont stockées sur plusieurs serveurs agréés par le ministère de la santé et impose une connexion sécurisée en officine. Cette sécurité est effectuée par l'association de la carte « professionnel de santé » et de la « carte vitale ». De plus, le DP-Rappels permet l'envoie des alertes concernant des retraits de lot, le DP-Alertes permet de diffuser rapidement des alertes sanitaires, et le DP-rupture permet l'envoie et la réception d'alertes concernant les ruptures de certains médicaments. Tous ces DP sont présents sur des

[2] « Le Dossier Pharmaceutique (DP) | CNIL ». (consulté le 21 mars 2020). https://www.cnil.fr/fr/le-dossier-pharmaceutique-dp.

réseaux différents, gérés d'une façon quasi invisible en officine grâce aux différents prestataires.

Le dossier pharmaceutique ayant plutôt bien fonctionné, le ministère a voulu l'étendre aux autres professionnels de santé (qui ne sont ni pharmaciens ni biologistes). A partir de cette réflexion, est né le Dossier Médical Partagé (DMP), venu en complément du dossier pharmaceutique. Depuis le 6 novembre 2018, il est officiellement accessible suite à l'annonce d'Agnès Buzyn, ministre de la Santé à cette date[3].

Parallèlement au développement de la carte vitale et du DP, il y a eu la mise en place de la vente uniquement de médicaments sans ordonnance sur Internet de façon sécurisée. Mais ce n'est réellement qu'en 2013, que la vente de médicaments sur internet par les officines est autorisée en France par l'ordonnance n° 2012-1427 du 19 décembre 2012[4]. Cependant, l'histoire européenne de la vente sur internet de médicament est plus ancienne. En effet, en 2003, la pharmacie Doc Morris aux Pays-Bas vendait des médicaments sur leur territoire mais également au sein de la communauté européenne. En Allemagne, l'Arzneimittelgesetz (loi allemande sur le commerce des médicaments) interdit toute vente en ligne de médicaments. Pour régler ce contentieux, la Cour de justice de l'Union Européenne (CJUE) a été saisie. Ce n'est qu'en 2011, soit 9 années plus tard, que la directive 2011/62/UE a été adoptée. Elle permet notamment la vente en ligne de médicaments et devait être transposée avant le 2 janvier 2013. Cette transposition a lieu en France par le biais

[3] « Dossier médical partagé (DMP) : questions-réponses | CNIL ». (consulté le 21 mars 2020). https://www.cnil.fr/fr/dossier-medical-partage-dmp-questions-reponses.

[4] « Vente de médicaments sur Internet en France - Les patients - Ordre National des Pharmaciens ». (consulté le 21 mars 2020) http://www.ordre.pharmacien.fr/Les-patients/Vente-de-medicaments-sur-Internet-en-France.

de l'ordonnance n° 2012-1427. Depuis, la vente en ligne de médicaments est encadrée par le code de la Santé Publique et par l'arrêté du 28 novembre 2016 relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies d'officine, les pharmacies mutualistes et les pharmacies de secours minières.

En plus de la vente de médicaments et du conseil apporté à celui-ci, l'officine peut accueillir la télémédecine. Cette dernière a été mise en place en France par le décret n° 2010-1229 du 19 octobre 2010. La téléconsultation implique une stricte sécurité des données, la liaison entre le patient et le médecin doit se faire de façon sécurisée car elle passe par internet[5]. Depuis la crise sanitaire de la COVID-19, le nombre de téléconsultations a considérablement augmenté en passant de 10'000 par semaine à plus de 400'000 par semaine pendant la crise. Cette téléconsultation se fait de manière générale chez le patient, sans intervention physique d'un professionnel de santé (sauf si ce patient est accompagné par une IDE). Dans ce cas-là, l'examen clinique peut être incomplet, et donc la mise en place de téléconsultations au sein d'officines peut améliorer la prise en charge du patient. La télémédecine à l'officine implique la même sécurité qu'une téléconsultation au domicile du patient.

Quand on s'intéresse de plus près aux dernières innovations et projets de loi concernant le numérique pour la santé et surtout pour l'officine, on remarque la naissance du projet de Health Data Hub[6]. Le but de ce projet est de réunir toutes les informations de santé possibles pour permettre une meilleure approche dans la recherche, d'aider les professionnels de santé dans la prise en charge de leurs

[5] « La télémédecine ». (consulté le 21 mars 2020) https://solidarites-sante.gouv.fr/soins-et-maladies/prises-en-charge-specialisees/telemedecine/article/la-telemedecine.

[6] « HEALTH DATA HUB » (s. d.), https://drees.solidarites-sante.gouv.fr/IMG/pdf/hdh-aap.pdf.

patients et de les informer sur leurs maladies. Ce projet pose des problèmes au niveau de sa sécurité informatique car il faut absolument un réseau sécurisé du début à la fin sans qu'on puisse récupérer les données qui y transitent en clair.

Parallèlement aux différentes structures mises en place par le ministère de la santé, d'autres réseaux informatiques en officine voient le jour. Depuis les années 2000, de plus en plus d'officines s'équipent d'automates ou de robots pouvant gérer leurs stocks de médicaments, avec des équipements coûteux et surtout mis en réseau avec le reste du parc informatique officinal.

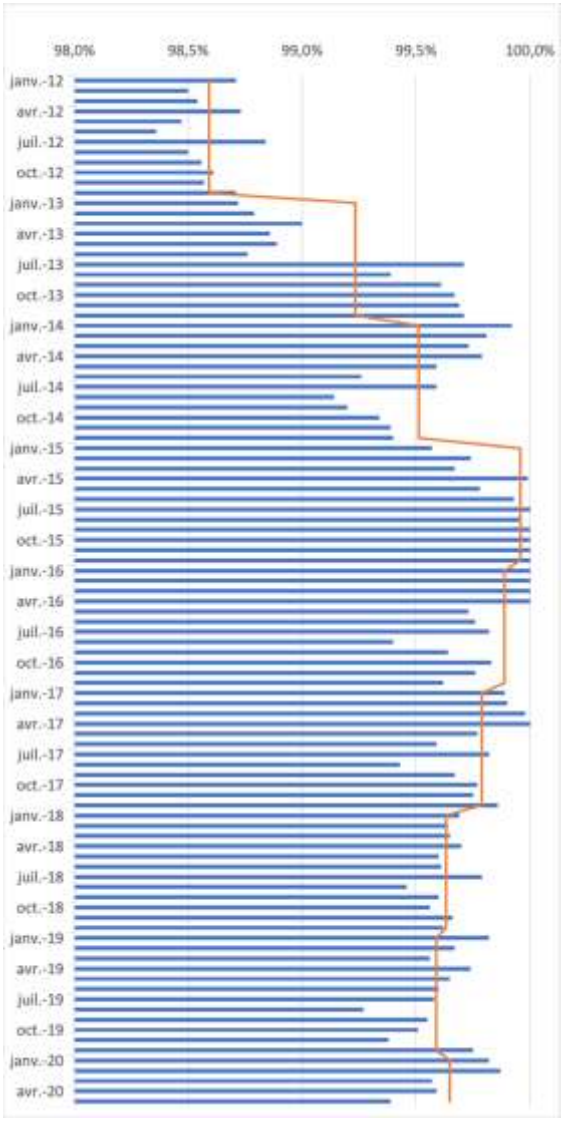


Figure 2 : Taux de télétransmission entre janvier 2012 et mai 2020

L'informatisation de la majorité des officines françaises a commencé dans les années 1990, période à laquelle de plus en plus d'officines se sont équipés d'outils numériques. Aujourd'hui la plupart des officines possède plusieurs ordinateurs capables de gérer l'essentiel pour le bien-être de l'officine. La télétransmission à distance est l'outil nécessaire à toutes les officines disposant d'outils numérique et d'une connexion internet. Cet outil puissant permet de cartographier les officines disposant du numérique.

Le rapport entre le nombre d'officines ayant effectué des télétransmissions par le biais informatique et le nombre total d'officines reflète le taux d'informatisation des officines, visible sur la Figure 2 : Taux de télétransmission entre janvier 2012 et mai 2020 qui regroupe les données fournit par le site de SESAM-Vitale. Sur ce graphique, le rapport entre le nombre d'officines qui ont télétransmis et le nombre total d'officines est en bleu ; la courbe orange représente la moyenne de ce taux sur l'année. On remarque que depuis 2012, le taux d'informatisation des officines françaises oscille entre 98% et 100%, avec un taux de 98,36% en juin 2012, taux le plus bas jamais enregistré.

Avec ce taux d'informatisation élevé, des règles strictes ont été mises en place afin d'éviter des fuites de données ayant pour conséquence la visibilité de données sensibles par tout le monde et sans chiffrement.

3 Cadre législatif concernant l'informatique à l'officine

Cette partie a pour but d'expliquer la législation concernant l'informatique en officine. Tout d'abord, je vais vous définir ce quelles sont les différentes données informatiques utilisées en officine. Ensuite, on pourra comprendre comment ces données sont traitées. Enfin, le serment de Galien et les règles éthiques seront évoqués car ils s'intègrent la législation des données officinales.

3.1 Données informatiques selon la législation

Les données informatiques sont nombreuses et toutes ne sont pas au même niveau de sensibilité.

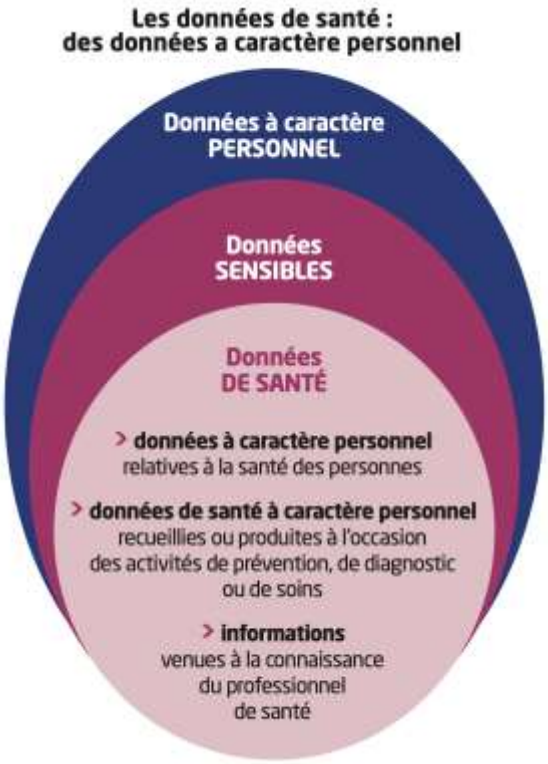


Figure 3 : Données informatiques selon la loi[7]

[7] « Respect de la confidentialité des données de patients dans l'usage de l'informatique - Recommandations de Janvier 2013 - Ordre National des Pharmaciens ». (consulté le 11 janvier 2020). http://www.ordre.pharmacien.fr/Communications/Publications-ordinales/Respect-de-la-confidentialite-des-donnees-de-patients.

Pour les différencier, l'État a fait voter la loi la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, communément appelée loi informatique et liberté. Ces données sont classées dans différents groupes visibles dans la Figure 3 : Données informatiques selon la loi. Il faut distinguer les données à caractère personnel qui englobent des données sensibles contenant elles-mêmes les données de santé.

Les données à caractère personnel ou DCP sont rattachées à une personne physique et permettent son identification de manière directe ou indirecte. Cette définition englobe un immense domaine lié à l'information. On y retrouve, par exemple, le nom, prénom, adresse physique ou électronique, adresse IP, date de naissance, numéro de téléphone, etc. Avec ce genre de données, on peut retrouver une personne, et même retracer un parcours numérique, pour voir quel site consulte cette personne, ou quel achat effectue-t-il sur internet. Ces données ne concernent pas seulement les pharmacies d'officine. Toute entreprise recueillant ces informations, quel qu'en soit le but, doit obligatoirement le déclarer.

Les données sensibles définies par l'article 6 de la loi informatique et liberté, quant à elles, font partie d'un groupe plus réduit. Celui-ci comprend les origines raciales et ethniques, les convictions religieuses, l'appartenance syndicale et l'orientation sexuelle, etc. Il comporte aussi les données génétiques et biométriques permettant d'identifier une personne physique. Les données de ce type, tombées entre de mauvaises mains, pourraient conduire à des actions répréhensibles comme des actes de racismes, d'homophobie, ou antireligieux. La collecte et le traitement de ces données sont interdits, sauf dérogation ou consentement explicite de la personne.

Enfin ce groupe contient également les données de santé qui sont donc considérées comme sensibles. Ce sont des données à caractère personnel se rapportant à la santé des personnes, pouvant aussi être recueillies par un professionnel de santé lors d'un acte médical ou paramédical. On retrouve ce genre de données constamment dans les officines, par conséquent les pharmaciens et leurs partenaires doivent être vigilants.

Ces données étant définies de façon législative, il faut voir et comprendre ce qu'est un traitement informatique de données.

3.2 Le traitement des données

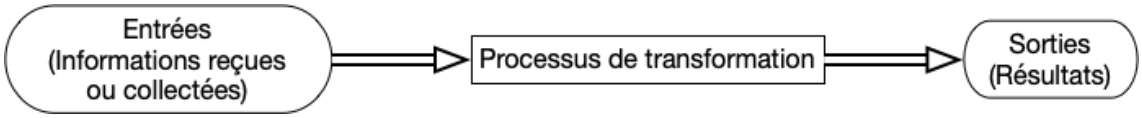


Figure 4 : Processus de traitement des données

D'après la Figure 4 : Processus de traitement des données, pour avoir un traitement des données, il faut une collecte préalable d'informations. Dans une officine, les données personnelles de tous les patients sont récupérées et peuvent être utilisées pour subir un traitement si l'officine accepte de les transmettre à ses sous-traitants (comme les prestataires informatiques ou encore les fournisseurs de logiciels de gestion d'officine).

Après la collecte, les informations vont subir un traitement consistant en une transformation de ces données permettant de sortir des résultats précis demandés.

Après la définition des données et leur traitement, il faut comprendre quels textes et lois s'y appliquent et comment peut-on les utiliser.

3.3 Serment de Galien et règles d'éthique

Le Serment de Galien ne fait pas partie des textes règlementaires et n'a aucune valeur juridique. Cependant, il est quand même étudié et récité dans les différentes facultés de pharmacie au moment de la soutenance de thèse. C'est un des premiers textes évoquant les données de santé, même si le terme « donnés de santé » n'est pas explicitement énoncé, la première version datant d'avant l'ère informatique. Après différentes modifications au fil de l'histoire, aujourd'hui une partie du texte rappelle le respect des lois en vigueur[8].

Le code pénal, contrairement au Serment de Galien, a lui une valeur juridique. Le 1er mars 1994, le nouveau code pénal français remplace celui de 1810[9]. Dans ce code figurent diverses lois dont certaines concernent les données de santé. La divulgation de ces informations, que cela se fasse de façon délibérée ou non, est punie par la loi. Le code pénal prévoit jusqu'à 1 d'emprisonnement et de 15 000 euros d'amende, sauf cas exceptionnel décrit par l'article 226-14 du code pénal.

En plus du code pénal, le code de la santé publique s'adresse aux professionnels de santé et aux patients. L'article L1110-4 du Code de la santé publique définit ce que l'on appelle communément le « secret professionnel » en santé mis en place par la loi Kouchner de mars 2002. De même, ce code prévoit la création d'un code de déontologie des pharmaciens par le conseil de l'ordre selon lequel le pharmacien est responsable de la protection des données quel qu'en soit le support prévu par l'article R4235-9 du code de la santé publique.

---

[8] Eugène-Humbert Guitard, « Les serments professionnels de la pharmacie de l'antiquité à nos jours (suite et fin) », *Revue d'Histoire de la Pharmacie* 35, no 117 (1947): 122-32, https://doi.org/10.3406/pharm.1947.10903.

[9] « Code pénal », Code pénal §. (consulté le 18 janvier 2020). https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719.

En plus de lois ciblant explicitement le monde de la santé, il existe d'autres lois, plus générales mais impactant quand même l'utilisation de données au sein d'établissements de santé et d'officine.

3.4 Législation de l'informatique impactant l'officine

3.4.1 Loi informatique et liberté et règlement général sur la protection des données

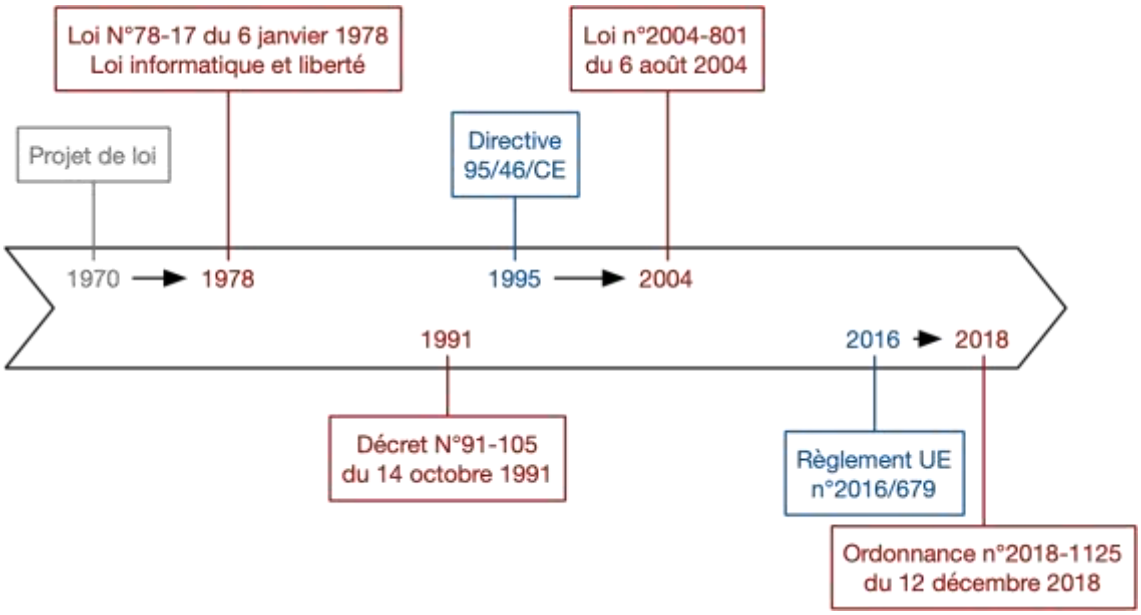


Figure 5 : Chronologie de la loi informatique et liberté

Promulguer une loi ne se fait pas rapidement. Pour être appliquée, une loi doit être votée. Pour ce faire, un projet est d'abord élaboré puis modifié jusqu'à qu'il puisse être soumis au vote définitif.

Selon la Figure 5 : Chronologie de la loi informatique et liberté, la loi informatique et liberté a mis 8 ans avant d'être votée, avec un projet de loi commençant en 1970. Signée initialement le 6 janvier 1978, la loi informatique et

liberté numérotée 78-17 a été modifiée par trois fois : la première par décret le 14 octobre 1991, la deuxième par une loi rentrée en vigueur le 6 aout 2004 afin de transposer les dispositions de la directive 95/46/CE[10].

Enfin, pour la dernière modification, l'État a transposé le règlement général européen 2016/679 sur la protection des données. Communément appelé RGPD, il est adopté au mois de mai 2016 et mis en œuvre le 25 mai 2018. Le RGPD a entièrement bouleversé le monde de l'informatique. En effet, les grands groupes tout comme les petits sites internet ont dû s'adapter au RGPD en un peu plus de deux ans. De ce fait, l'État français a dû remanier entièrement la loi informatique et liberté en supprimant la quasi-totalité de ses articles pour y transposer ce règlement.

En 2020, la loi informatique et liberté, composée de 5 titres incluant 128 articles différents, inscrit l'informatique et les données informatiques en tant que droit fondamental. Ces dernières ne peuvent donc « porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Cette loi est axée sur la réglementation du traitement informatique des données personnelles, telles qu'elle les définit, comme nous avons pu le voir précédemment. La loi informatique et liberté permet aux citoyens français d'être maîtres de leurs données personnelles et notamment leurs données de santé qui sont couramment utilisées en officines.

[10] « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » (s. d.). (consulté le 11 janvier 2020).

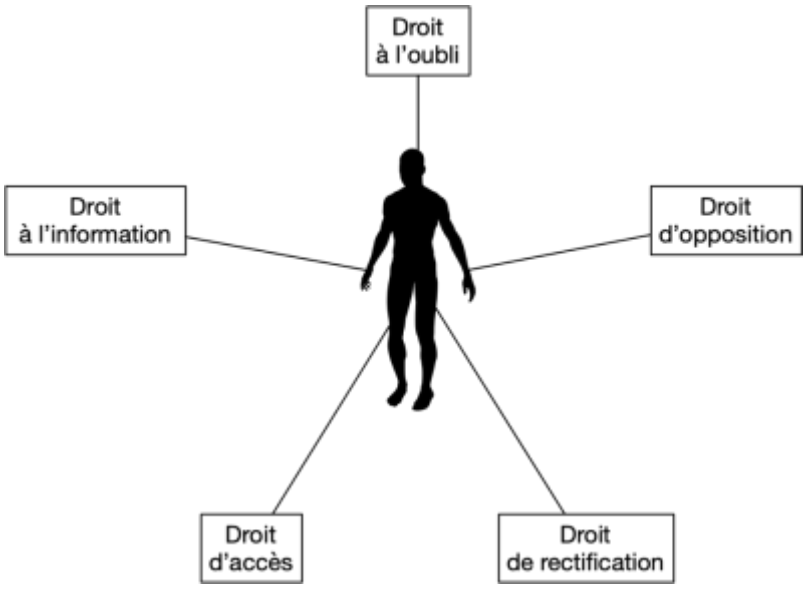


Figure 6 : Les différents droits des citoyens définis par la LIL

Afin de garantir aux Français la maîtrise de leurs données, ce texte définit 5 droits fondamentaux en informatique, comme illustré sur la Figure 6 : Les différents droits des citoyens définis par la LIL : le droit à l'information, à l'accès, à la rectification, à l'opposition et à l'oubli.

3.4.1.1 Le droit à l'information

Le droit à l'information est défini par l'article 48 du chapitre II de la loi informatique et liberté, qui est une transposition des articles 12 à 14 du règlement (UE) 2016/679. Le responsable des fichiers informatiques doit informer chaque personne avant de collecter et de traiter ses données. De plus, il doit utiliser un langage clair et facilement compréhensible lors de la collecte de données auprès de mineurs de moins de 15 ans.

Dès qu'il y a collecte de ces données, le responsable du traitement doit fournir un certain nombre d'informations essentielles :

- Identité et coordonnées du responsable du traitement et/ou du délégué à la protection des données
- Finalités du traitement
- Intérêts légitimes poursuivis par le responsable du traitement
- Destinataires des données à caractère personnel
- Transferts de données à caractère personnel vers un pays tiers ou une organisation
- Et autres informations complémentaires :
    - Durée de conservation des données
    - Le droit d'accès, de rectification, d'effacement, d'opposition
    - Le droit d'introduire une réclamation auprès d'une autorité de contrôle
    - L'existence d'une prise de décision automatisée
    - Etc.

Une entorse à ce droit est prévue par la loi informatique et liberté : si les données sont traitées et utilisées pour le compte de l'État dans un cadre de sécurité publique.

Concrètement, à l'officine, dès qu'il y a une récolte des données ayant des fins de traitements, le pharmacien doit informer sa patientèle et fournir toutes les informations relatives à ce traitement.

Par exemple, on retrouve ce droit lors d'une ouverture d'un Dossier Médical Partagé (DMP). Le pharmacien a l'obligation d'informer son patient que les données envoyées dans son Dossier Médical Partagé peuvent être sujettes à des traitements.

De plus, à chaque ouverture d'un Dossier Médical Partagé, une feuille imprimée est remise au patient. Elle contient le code confidentiel du patient et

toutes les informations relatives à son dossier et notamment des liens internet concernant l'utilisation des données.

Lors de vente par internet de médicaments par une officine, l'utilisateur fournit un certain nombre d'informations le concernant (nom, prénom, adresse mail et postale, etc.) en plus de la liste des médicaments qu'il achète. L'officine vendant sur internet doit donc prévenir l'utilisateur de l'utilisation de ses données. Ce droit est généralement décrit dans les conditions générales de ventes ou d'utilisation.

Le projet de loi du Health Data Hub va mettre à contribution les pharmaciens d'officine qui seront en première ligne pour le recueil et le traitement des données selon la délibération n°2018-289 du 12 septembre 2018 de la Commission Nationale de l'Informatique et des Libertés. Le pharmacien devra donc prévenir tous ses patients de toutes les possibilités d'utilisation de leurs données.

3.4.1.2 Le droit d'opposition

Le droit d'opposition est prévu par l'article 21 du règlement (UE) 2016/679, et transposé dans l'article 56 de la loi informatique et liberté.

Toute personne, à tout moment, possède le droit de s'opposer au traitement ses données. Cette opposition n'est valable que si le responsable du traitement des données ne peut présenter de motif légitime et impérieux empêchant l'opposition.

Ces motifs doivent prévaloir sur les intérêts, les droits et libertés de la personne concernée, ou l'utilisation en justice de ces données. De plus, si le traitement est nécessaire à une mission d'intérêt public, le droit d'opposition ne peut s'appliquer.

Par conséquent, l'État peut inclure toutes données à caractère personnel, y compris les données de santé, dans une étude à des fins épidémiologiques sans que le patient ou le pharmacien ne puissent s'y opposer. Cependant, le droit à l'information de la personne concernée est maintenu : les données étant utilisées pour une raison de Santé Publique et non de sécurité publique. La personne doit donc obligatoirement être prévenue de l'utilisation de ses données. Les informations collectées par les services publics, tels que la sécurité sociale, les services de police ou encore le service des impôts, font donc partie de cette exception car elles sont considérées comme informations obligatoires et d'intérêt public.

Le caractère obligatoire et d'intérêt public de ces informations s'inscrit dans le projet de loi du Health Data Hub. En effet, le patient ne pourra donc utiliser son droit d'opposition car ce projet de loi est considéré comme d'utilité publique.

En reprenant le cas du Dossier Médical Partagé, le patient a le droit de s'opposer au traitement de ses données à caractère personnel, sauf si elles sont utilisées dans une mission d'intérêt public ou nécessaires à la défense de ses droits en justice. Dans un autre cas de figure, lors d'une vente en ligne par une officine, l'utilisation des données à des fins de traitements peut être révoquée dès que le patient s'y oppose.

3.4.1.3 Le droit d'accès

L'article 49 du chapitre II de la loi informatique et liberté prévoit le droit d'accès conformément à l'article 15 du règlement (UE) 2016/679. En justifiant son

identité, une personne a le droit de savoir si ses données personnelles sont traitées ou non ; le responsable doit donc fournir une copie des données qui sont traitées.

En reprenant le cas du DMP, un patient pourra donc demander une copie intégrale ou partielle de son DMP ainsi que du traitement effectué dessus, ou encore une copie des données traitées par le projet Health Data Hub.

3.4.1.4 Le droit de rectification

Le droit de rectification est établi par l'article 50 de la loi informatique et liberté conformément à l'article 16 du règlement (UE) 2016/679. La personne dont on utilise les données à caractère personnel a le droit les rectifier si elles sont inexactes. Cela se fait par le biais du responsable du traitement de données.

Concrètement, la personne se rendant compte que des données inexactes ont été fournies à un organisme, peut contacter cet organisme afin de rectifier les inexactitudes. Par exemple, une mauvaise adresse ou un mauvais numéro de téléphone ont été fournis, la personne peut contacter l'organisme pour les modifier.

3.4.1.5 Droit à l'oubli

Le droit à l'oubli ou le droit à l'effacement est établi par l'article 17 du règlement (UE) 2016/679 du 27 avril 2016, transposé dans l'article 51 de la loi informatique et liberté.

La personne, dont les données ont été utilisées à des fins de traitements, a le droit d'obtenir l'effacement complet de ses données. Pour cela, elle doit en informer le responsable des fichiers, qui doit les effacer dans les meilleurs délais. Si au bout d'un mois (voire trois mois si les données sont complexes), les données ne sont toujours pas effacées, la personne concernée peut demander des explications au

responsable. Si la réponse obtenue est insatisfaisante, elle peut saisir la CNIL. Bien sûr, la personne ne peut exercer son droit d'effacement, si ce même droit va à l'encontre de la liberté d'expression et d'information, de l'intérêt public, d'une obligation légale, et de la justice.

Toujours dans le cas du DMP, le patient a, à tout moment, le droit de demander la fermeture et l'effacement entier de son DMP. Un formulaire de contact a été mis en place pour pouvoir fermer et détruire les données de son DMP[11].

Dans le cas du Health Data Hub, ce droit à l'oubli est plus difficile à exercer. La personne, dont les données personnelles ont été utilisées dans le cadre du Health Data Hub, peut demander un effacement pur et simple de ses données. Cependant, le responsable des données concernant ce projet pourra refuser s'il estime que l'effacement peut aller à l'encontre de l'intérêt public.

3.4.1.6 Délégué à la protection des données

Le délégué à la protection des données, ou DPO, est une personne désignée par l'organisme dans lequel elle travaille. Elle est responsable de la conformité vis-à-vis de la protection des données. Elle informe et conseille l'organisme et ses employés, et contrôle l'application de tous les textes législatifs qui concernent la protection des données.

Cette même personne peut être contactée pour toute information relative à l'utilisation des données au sein de son organisation, par quelqu'un d'interne mais aussi de l'extérieur. Donc, quand une personne souhaite savoir si des données

[11] « Formulaire de demande d'intervention sur le compte d'accès au DMP », s. d., https://www.dmp.fr/documents/formulaire-demande-intervention.

personnelles sont utilisées au sein d'un organisme, elle doit contacter le délégué à la protection des données. Le DPO doit répondre à sa demande en l'informant directement de l'utilisation de ses données et peut lui remettre les coordonnées du responsable du traitement des données.

Toute entreprise traitant des données, devra désigner un DPO pour être conforme avec la loi et le RGPD. Les pharmacies d'officine sont une exception, la CNIL n'oblige pas les officines à désigner un DPO sauf si elles traitent un grand nombre de données. Cependant, un pharmacien titulaire d'officine peut, s'il le souhaite, nommer un DPO. Il ne peut se nommer soit même ou nommer un autre pharmacien titulaire car il y aurait conflit d'intérêt. Il peut nommer n'importe quel salarié de son officine à la condition que celui-ci soit formé et possède des connaissances suffisantes dans la protection des données.

3.4.2 Hébergeur de santé (HDS)

Les hébergeurs de santé (HDS), sont des hébergeurs de données particuliers.

Les hébergeurs web simples, hébergent des sites web et leurs données sur des serveurs situés dans des locaux qui leur sont alloués. Généralement, un hébergeur fournit soit un serveur entier à un organisme ou un particulier, soit une partie d'un serveur (partage du serveur entre plusieurs organismes permettant des baisser les couts d'hébergement).

Les hébergeurs de santé sont définis par l'article L111-8 du code de la Santé Publique. Ils hébergent des données ayant un statut particulier. Cela concerne toutes

les données de santé à caractère personnel ayant été rassemblées au cours d'actes de santé (prévention, diagnostic, soin, ou suivi médico-social).

Pour pouvoir héberger des données de santé, un hébergeur doit être titulaire d'un certificat de conformité selon l'article L1111-8 du code de la Santé Publique. Ce certificat émis par un organisme de certification. Il y a plusieurs organismes de certifications, selon l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie. Ces organismes sont accrédités par l'instance d'accréditation de la France ou d'un autre État membre de l'Union Européenne

3.4.2.1 La justification de l'emploi d'hébergeurs de santé

Les données de santé sont des données sensibles qui sont encadrées par la loi[12]. Il faut donc garantir une disponibilité optimale, une traçabilité et une intégrité de ces données. De plus, il faut sécuriser au maximum l'authentification pour accéder aux différentes ressources.

3.4.2.2 La certification

Il y a 2 types de certifications, un pour les hébergeurs d'infrastructures physiques, et un pour les hébergeurs infogéreurs. Pour être certifié, un hébergeur doit passer par plusieurs étapes[13].

Tout d'abord, l'hébergeur doit être certifié ISO 27001 : cela définit les exigences d'un système de management de la sécurité de l'information.

Ensuite, l'hébergeur effectue un audit documentaire afin de pouvoir présenter un dossier incluant les exigences des normes ISO 20000-1, ISO 27017 et

[12] « Hébergement des données de santé ». (consulté le 21 mars 2020). https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante.

[13] « HDS Hébergeur de données de santé - AFNOR Certification » (consulté le 21 mars 2020). https://certification.afnor.org/numerique/certification-hds-hebergement-des-donnees-de-sante.

ISO 27018. Puis, un audit sur site est effectué dans le but de recueillir les preuves des conformités techniques dans les locaux.

Et enfin, il y a l'étape de la certification par un organisme certifié par la COFRAC (Comité français d'accréditation).

La certification est valable 3 ans. L'hébergeur doit effectuer un audit de suivi annuel et un audit de renouvellement au bout de 3 ans pour conserver la certification.

3.4.2.3 L'officine et les HDS

Dans son fonctionnement quotidien, une officine va devoir faire appel à un hébergeur de santé. La plupart du temps, les différents prestataires de logiciels de gestion incluent une offre comprenant une prestation d'hébergement de données de santé. Cela leur permet d'offrir une solution clé en main et simplifier le suivi fonctionnement des officines.

A chaque dispensation d'ordonnance, le pharmacien stocke des données de santé liées à son patient sur un appareil appartenant à son officine ou à son prestataire. Dans ce cas-là, il intègre la définition d'un hébergeur de santé et devrait donc avoir une certification pour effectuer ce métier quotidiennement.

Cependant, les hébergeurs de santé ont été créés pour sécuriser le traitement des données de santé. Le pharmacien d'officine utilise l'outil informatique pour facturer des ordonnances, et envoyer le tout aux différentes caisses de l'assurance maladie et des complémentaires de santé. Le pharmacien ou tout autre personne n'effectue aucun traitement sur les données stockées dans une officine. Seules les données détenues par l'assurance maladie ou les complémentaires recueillies en officine peuvent subir un traitement de données.

Par conséquent, une pharmacie d'officine ne peut être qualifiée d'hébergeur de santé et n'a pas besoin d'effectuer une certification pour héberger des données de santé.

3.4.3 L'utilisation du mail

Les mails ou courriers informatiques sont des messages ayant un titre et un corps qui contient ou non des pièces jointes. Ces messages ainsi que leurs pièces jointes sont stockés sur des serveurs afin d'être accessibles par le biais soit d'un site web soit d'un logiciel de messagerie.

Selon l'arrêté du 28 novembre 2016 relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies d'officine, les pharmacies mutualistes et les pharmacies de secours minières, mentionnées à l'article L. 5121-5 du code de la santé publique, s'il veut pouvoir délivrer des médicaments, le pharmacien doit s'assurer de la validité et de l'authenticité de l'ordonnance.

Avant l'essor du mail, les pharmaciens d'officine utilisaient et peuvent encore utiliser de nos jours des fax télécopiés. Déjà à l'époque, cette utilisation était controversée. En effet, il y a un risque de falsification d'ordonnance et la délivrance ne se faisait que sur une copie et non sur l'original de l'ordonnance.

Aujourd'hui, de plus en plus d'officines utilisent le courriel pour communiquer entre professionnels de santé. Cette utilisation est encore plus controversée que l'utilisation du fax. Cela est dû au fait que chaque communication est hébergée par un prestataire. Une ordonnance envoyée à un pharmacien, que cela soit par le prescripteur ou par le patient lui-même, est donc hébergée sur un serveur appartenant au prestataire qui fournit le service de messagerie informatique. Cela

ne pose pas de problèmes si le prestataire possède une certification pour être hébergeur de santé. Cependant, la plupart des services de messagerie gratuits, ne sont pas certifiés et donc leur utilisation pour l'envoi ou la réception d'ordonnances n'est pas conforme au regard de la loi. De plus, un professionnel de santé qui communique via les services de messagerie simple ne peut être sûr de l'identité de son interlocuteur. Le pharmacien qui choisit délibérément d'utiliser ce genre de service de messagerie peut donc être poursuivi car c'est lui qui doit garantir de la sécurité des données qu'il utilise.

Pour éviter cela, le ministère de la santé a décidé de mettre en place une messagerie gratuite et sécurisée nommée Mailiz intégrée dans le service MSSanté[14]. Pour pouvoir créer un compte cette messagerie sécurisée fournie par l'État, il suffit d'être professionnel de santé, de posséder une carte CPS avec son propre code confidentiel lié à la carte CPS et enfin d'être en possession d'un lecteur de carte CPS. Pour y accéder depuis n'importe où, l'identifiant et le mot de passe créés suffisent. On peut aussi s'y connecter par le biais de sa carte CPS et d'un lecteur de carte CPS. Cette messagerie permet donc d'être conforme à la loi et surtout d'avoir un lien fiable et sécurisé avec d'autres professionnels de santé.

Le pouvoir législatif et le pouvoir exécutif ont mis en place différentes lois et divers services permettant d'encadrer les données et notamment les données de santé. Dans le cadre de l'application de ces différentes lois, une instance a dû être créée.

[14] « MSSanté ». (consulté le 21 mars 2020) https://mailiz.mssante.fr/ps/decouvrir.

3.5 Commission Nationale de l'Informatique et des Libertés

La commission nationale de l'informatique et des libertés, CNIL, est née suite à l'adoption de la loi informatique et liberté en 1978. En effet, l'article 6 originel désigne la CNIL et nomme ses missions.

Cette commission possède un comité d'expert composé de 18 membres nommés pour cinq ans. Ils sont soit élus par les assemblées soit désignés par le premier ministre ou les présidents des deux assemblées. La présidente actuelle, élue en février 2019, est Marie-Laure DENIS. Sur ordre de la présidente de la CNIL, ses membres se réunissent afin de délibérer sur les différents problèmes liés à ses missions.

Les missions de la CNIL sont expliquées sur leur site web : https://www.cnil.fr .

La CNIL possède quatre missions distinctes[15] :

- Informer et protéger les différents droits des citoyens et des organismes liés à l'informatique
- Accompagner et conseiller dans la conformité informatique des organismes
- Anticiper et innover : la CNIL constitue des débats de société et conduit des réflexions sur les enjeux éthiques
- Contrôler et sanctionner les différents organismes.

Concernant sa dernière mission, la loi du 6 aout 2004 confère en peu plus de pouvoir à la CNIL. Elle acquière notamment le pouvoir de contrôler les locaux d'une

[15] « Les missions de la CNIL | CNIL », consulté le 20 février 2020, https://www.cnil.fr/fr/les-missions-de-la-cnil.

entreprise. Avant une réelle sanction, la CNIL avertie les organismes qui ne sont pas conformes avec la loi. Si les organismes ne modifient pas leur mode de fonctionnement, alors la CNIL les met en demeure et peut infliger une amande pouvant aller jusqu'à vingt millions d'euros ou jusqu'à 4% du chiffre d'affaire mondial de l'entreprise. Au total, il y a eu 79 mises en demeure, dont 5 publiques en 2019. On retrouve des entreprises comme EDF ou Engie mais aussi le ministère de l'intérieur et des établissements scolaires.

La CNIL fournit des guides pour permettre à tout le monde de se mettre en conformité vis-à-vis du RGPD. Sur son site web, on peut trouver en plus d'exemples de fichiers à mettre en place pour être conforme, tels que des registres de traitements.

Chaque état membre de l'Union Européenne a ses propres lois. L'Union Européenne essaye d'uniformiser tout ce qui est lié aux médicaments mais aussi à l'informatique. On peut le constater avec la mise en place des RGPD. Les autres pays membres de l'Union Européenne possèdent eux aussi des autorités compétentes dans la protection des données et de la vie privée, tel que l'APD (Autorité de protection des données) belge ou encore la BfDI (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) allemande. En plus des autorités propres à chaque pays membres, l'Union Européenne a mis en place une autorité de contrôle indépendante européenne, nommée CEPD (Contrôleur européen de la protection des données). Elle supervise le traitement des données personnelles dans les institutions européennes, possède un rôle de consultation auprès de la commission européenne, du conseil de l'Union Européenne et du parlement européen. Il coopère aussi avec les autorités de tous les états membres de l'Union Européenne.

3.6 CLOUD Act aux États-Unis d'Amérique

Contrairement aux terres matérielles, il est difficile de créer des frontières au sein d'internet et de ses infrastructures. Certaines organisations liées à un pays peuvent avoir des données stockées dans un autre pays. Par conséquent, les États-Unis ont adopté différentes lois permettant d'accéder à des données d'investigation pour des affaires judiciaires.

En 2018, les États-Unis ont adopté le Clarifying Lawful Overseas Use of Data Act ou CLOUD Act. Cette loi fédérale permet aux instances judiciaires des États-Unis d'Amérique d'accéder par mandat à toutes données concernant une enquête, qu'elles soient situées sur le sol des États-Unis ou dans un autre pays, tant que l'hébergeur des données est enregistré aux États-Unis.

Dans ce cas-là, la législation des États-Unis prévôt sur les autres lois. Cependant, un pays ne peut intervenir dans un autre pays à moins d'avoir des accords bilatéraux passés entre les États-Unis et le pays concerné. Sauf qu'en utilisation concrète des services fournit par des entreprises venant des États-Unis, on ne sait pas où sont stockées les données qu'on envoie. Donc, quand une officine utilise par exemple les services fournies par Google pour s'échanger des mails, ces données peuvent être vus par des autorités judiciaires des États-Unis alors que ces données sont françaises. De plus, si on fait transiter une ordonnance par ce biais, rien n'interdit la divulgation de celle-ci à un autre pays, alors que ces données-là sont sensibles. On peut nuancer ces propos, parce que ces entreprises possèdent la plupart du temps des serveurs basés en Europe pour éviter de saturer le réseau des États-Unis, et que donc normalement mais pas avec certitude, tous données transitant dans l'Europe sont stockées dans l'Europe et donc la loi de l'Union européen et notamment le règlement général sur la protection des données prévôt

sur le Cloud Act. L'article 48 du RGPD européen précise clairement qu'aucun pays tiers, sauf si des accords internationaux sont signés, ne peut demander à récupérer des données au sein de l'union européen. Dans tous les cas, si les données sont correctement chiffrées par le client pendant les échanges entre le serveur et le poste client et s'ils sont stockés sous forme chiffrées sur le serveur, alors personne ne pourra y accéder à moins d'avoir la clé de déchiffrement.

L'Europe, ses états, mais aussi les différents états du monde ont mis en place des mesures pour contrôler les données transitant par internet, et surtout pour sécuriser des données importantes, tel que les données personnelles dont les données de santé. Ces données transitent à travers le monde par le biais de flux contenu dans des réseaux et sous-réseaux.

4 La structure du réseau informatique à l'officine

Dans cette partie, nous verrons plus précisément le réseau informatique à l'officine. Bien sûr, dans un premier temps, je définirais le réseau informatique avant d'en faire un historique. Nous verrons ensuite les différents types de réseaux informatiques comme le domestique ou celui des entreprises pour enfin comprendre le modèle de réseau informatique officinal.

4.1 Définition

Un réseau informatique est une interconnexion entre plusieurs équipements capables de fonctionner en réseau tels que des ordinateurs, serveurs, imprimantes, etc. reliés entre eux par le biais d'équipements de réseau tels que des switches Ethernet, des modems et des routeurs.

4.2 Historique

Les réseaux informatiques ont été créés pour communiquer entre équipements informatiques.

Au début, seulement quelques équipements étaient reliés entre eux. En 1965, l'un des premiers réseaux informatiques créé a permis de communiquer entre le Massachusetts et la Californie. A partir de cette année-là, différents protocoles de communication furent créés. En 1969, la communication par paquets fut choisie et adoptée avec la création du réseau ARPANET présenté en 1972. Ce réseau permis de relier plusieurs villes des États-Unis : c'est le réseau précurseur à l'internet que l'on connait aujourd'hui. Cette communication par paquets, adaptée à ARPANET en 1984, est la base des flux régissant internet aujourd'hui, avec le protocole TCP/IP

choisit en 1974. En 1983, les premiers serveurs DNS sont créés. Ils permettent de simplifier les échanges : il suffit de retenir un nom de domaine (par exemple : ameli.fr) pour accéder aux informations d'un serveur, plus besoin de retenir des suites de chiffres appelée adresse IP (Internet Protocole). Puis en 1990 est né le World Wide Web (WWW) utilisant le protocole http : réseau constitué de serveurs permettant d'afficher des pages internet accessibles par le biais d'un navigateur web. Aujourd'hui, on confond le World Wide Web et Internet. Par abus de langage, on parle souvent d'Internet pour ne designer que le WWW.

Aujourd'hui, plusieurs milliards d'ordinateurs, de serveurs et d'équipements réseaux communiquent entre eux chaque jour. Pour se faire, plusieurs réseaux différents existent dans le monde. On différencie par exemple les flux permettant de visiter des pages web et ceux permettant la télétransmission, puisqu'ils n'appartiennent pas au même réseau.

Pour comprendre les différents réseaux informatiques disponibles à l'officine, il faut partir d'un réseau local simple, puis complexifier les différentes connexions possibles.

4.3 Réseau informatique domestique

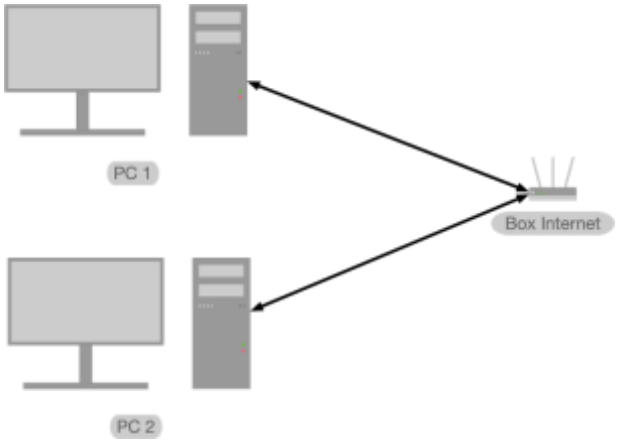


Figure 7 : Réseau local simple

Le premier réseau rencontré, lors d'une utilisation à domicile est le réseau local, schématisé sur la Figure 7 : Réseau local simple. Constitué d'un ou plusieurs ordinateurs (ici pour l'exemple, il y en a 2), ce réseau permet aux différents ordinateurs de communiquer entre eux par le biais d'une box internet (constituée d'un modem et d'un routeur).

Les 2 ordinateurs ne communiquent pas directement entre eux : un ordinateur fait une demande à la box internet qui redirige le flux vers le second ordinateur. Les ordinateurs peuvent être connectés en filaire par le biais de câbles RJ45 ou sans fil par le biais du Wi-Fi. La box internet est le centre d'un réseau domestique local simple : elle permet de rediriger les données transitant dans le réseau local.

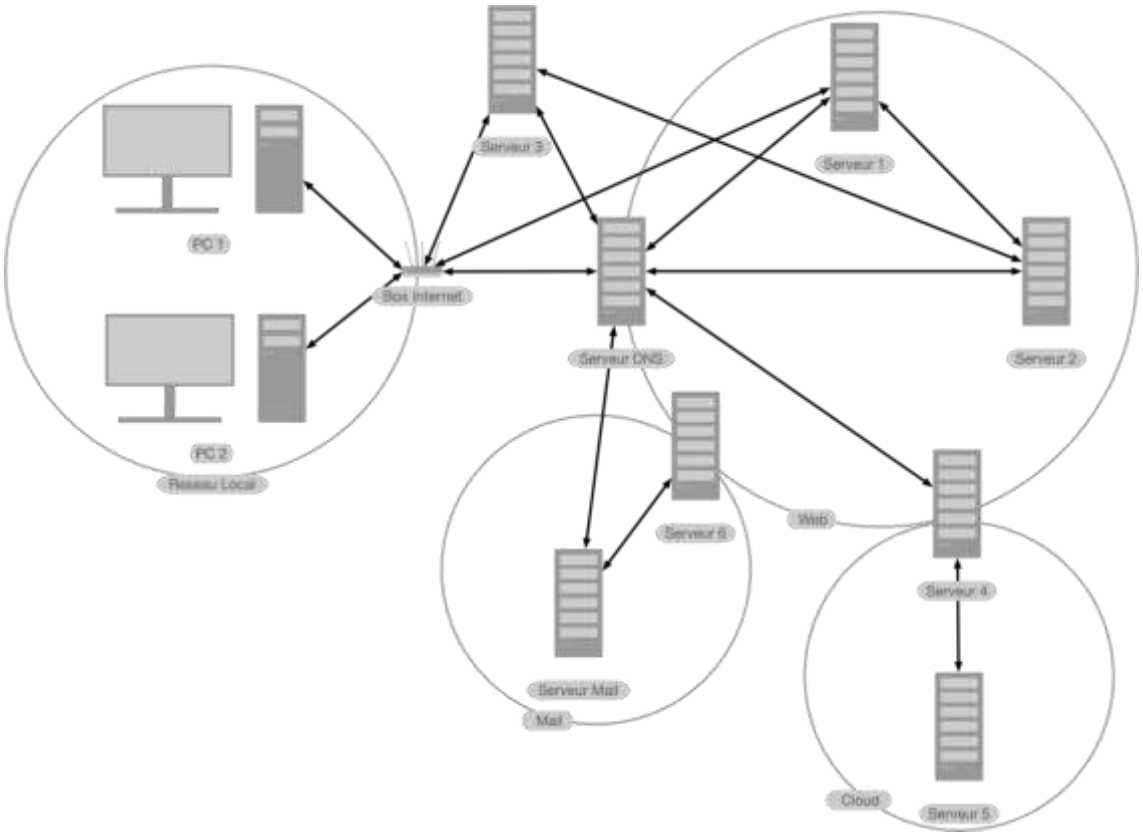


Figure 8 : Réseau domestique connecté à Internet

Au-delà d'une utilisation locale, une box internet permet de se connecter au réseau internet lui-même par le biais d'une connexion filaire ADSL ou Fibre ou d'une connexion sans fil satellitaire (souvent utilisée dans des lieux où l'ADSL et la fibre ne sont pas accessibles ou offrent des débits médiocres).

La Figure 8 est une simplification des différents réseaux les plus utilisés au niveau domestique. Même après simplification, on peut voir la complexité des différents réseaux et flux de données. Le PC d'un utilisateur demande à la box d'accéder à différents serveurs. Ces serveurs communiquent par le biais de la box internet, par le biais du serveur DNS ou encore entre eux. Chaque connexion d'un pc parcourt différents chemins pour accéder à un serveur qui renvoie les données. Elle parcourt ensuite le chemin inverse pour afficher ces mêmes données sur le pc de l'utilisateur.

Les principaux réseaux utilisés sont le web, le mail et le cloud. Pour accéder au mail ou au cloud, la plupart des services proposent des pages web pour y accéder. Il faut une cascade de serveurs. Dans le cas du mail, on peut soit y accéder par le biais d'une page web soit directement par le biais de protocoles de communication spécifique (SMTP, IMAP et POP) et de logiciels client de messagerie.

4.4 Réseau informatique d'entreprise

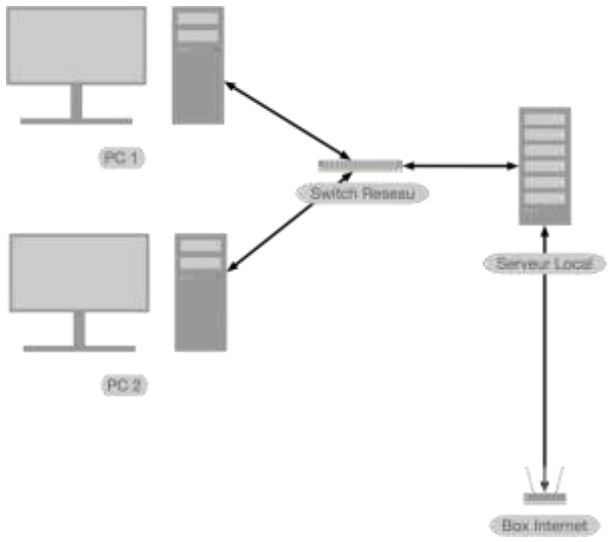


Figure 9 : Réseau local d'entreprise

La Figure 9 montre le fonctionnement de la plupart des réseaux d'entreprise. Cette fois, les PC communiquent entre eux par le biais d'un switch ethernet mais aussi avec un ou plusieurs serveurs locaux permettant d'accéder à la box internet.

Le serveur local permet de gérer toutes les connexions entre les ordinateurs et internet. Le gestionnaire du parc informatique de l'entreprise peut établir des protocoles afin sécuriser ou non les échanges entre les différentes pièces informatiques de l'entreprise.

La présence d'un serveur local fait la différence. Elle permet de distinguer les réseaux domestiques et ceux d'entreprises qui ont besoin d'avoir un réseau plus sûr. Dans un réseau domestique, il n'y a pas de demande spécifique. Il nécessite seulement un accès à internet et doit garantir une connexion assez stable à l'ensemble des périphériques réseaux. Dans une entreprise, il faut garantir une meilleure stabilité que dans un réseau domestique ainsi qu'un accès à l'ensemble des fichiers communs à l'entreprise et à tous périphériques qui en font la demande. Ces fichiers peuvent être cruciaux, donc il faut garantir leur intégrité et une sauvegarde si le serveur un problème.

Dans une entreprise, les différents PC peuvent accéder aux mêmes services qu'au domicile de son utilisateur. Donc, toutes les connexions entre la box internet domestique et le reste d'internet sont possibles en entreprise. Pour simplifier, sur la figure 9, les services décrits pour le réseau domestique ne figurent pas.

Les officines sont des entreprises, par conséquent les règles informatiques d'entreprise s'appliquent aussi à l'officine. Cependant, dans une officine, les connexions sont différentes et nécessitent plus de moyen.

4.5 Réseau informatique officinal

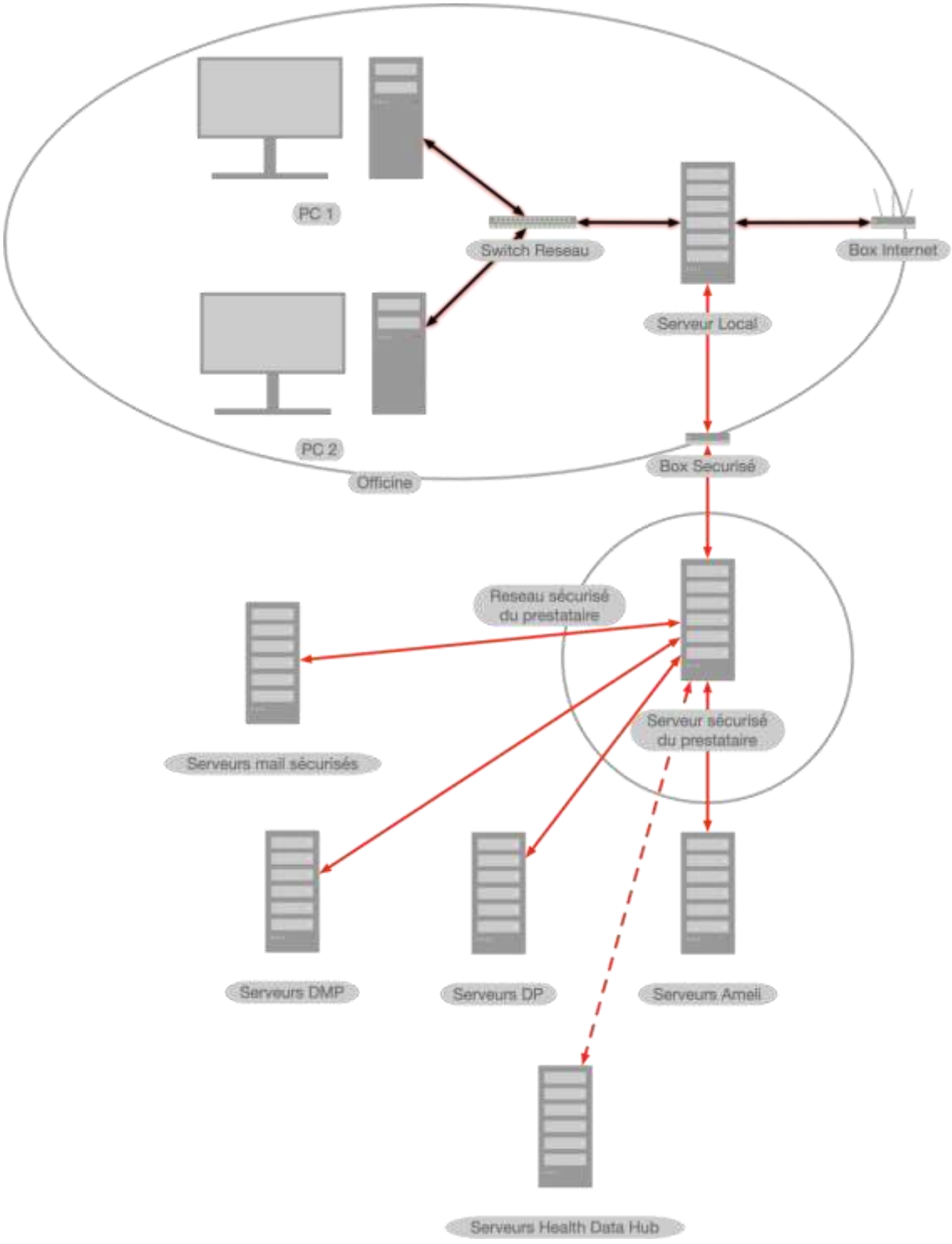


Figure 10 : Exemple de réseau d'une officine

Les connexions dans les officines sont encore plus complexes que dans une entreprise lambda, la Figure 10 en est un exemple. Les données y transitant sont plus sensibles, un réseau complètement sécurisé est donc indispensable.

Le plus simple pour sécuriser le réseau officinal est de se fier à un prestataire qui est souvent le même que celui qui fournit le logiciel de gestion d'officine (LGO). Ce prestataire s'occupe de fournir une connexion sécurisée entre l'officine et les différents serveurs de l'assurance maladie. Pour cela, le prestataire fournit un serveur local par lequel transitent toutes les données de l'officine. Ce serveur s'occupe de rediriger les flux destinés à internet vers la box internet d'un fournisseur d'accès à internet (FAI). Quant aux flux destinés aux serveurs de l'assurance maladie, le serveur les redirige vers des serveurs propres au prestataire par le biais d'une box Internet sécurisée. Les serveurs du prestataire gèrent l'envoi des données aux serveurs de l'assurance maladie. Ces flux font donc bien partie d'Internet mais ne constituent pas des flux du World Wide Web, car il n'y a pas besoin de navigateur web pour envoyer ou recevoir des informations. En effet, ils sont à part pour éviter certains problèmes de sécurité. Ils sont censés être sécurisés par le biais informatique et sont représentés en rouge sur la Figure 10. C'est donc le prestataire qui s'occupe de sécuriser les flux de données de l'officine.

Le pharmacien accorde donc sa pleine confiance au prestataire qui lui fournit ce service. Cependant, au regard de la loi c'est le pharmacien qui est responsable de la sécurité des flux. Même s'il a confiance en son prestataire, le pharmacien a des obligations informatiques vis-à-vis de la loi et doit donc connaitre et mettre en place une stratégie de sécurité informatique au sein de son officine.

5 La sécurité informatique à l'officine

Maintenant que l'on connait la composition d'un réseau informatique à l'officine, nous allons essayer de comprendre comment est sécurisé ce réseau. Pour cela nous étudierons les différents outils mis à disposition des officines en commençant par l'analyse d'impact et pour finir avec les sites Internet et les hébergeurs de Santé. Enfin, nous pourrons observer les utilisations réelles de ces outils de sécurité.

5.1 Les outils de sécurité numérique mis à la disposition des pharmaciens

5.1.1 Analyse d'impact

Une analyse d'impact, quel que soit son domaine, est la cartographie d'un projet ou d'un évènement prévisible et de ses conséquences. C'est une étude permettant limiter certains coûts. Elle aide à prévoir des incidents susceptibles d'influer sur le projet ou de modifier l'évènement en question et/ou encore de prévoir et d'évincer des effets néfastes potentiels.

Dans le cadre d'un traitement de données, l'objectif est d'éviter des fuites. On fait donc une analyse d'impact relative à la protection des données (AIPD). Cette analyse d'impact n'est pas obligatoire au sein d'une pharmacie d'officine tout comme l'obligation de nommer un DPO. Donc seules de grosses officines effectuant des traitements à grande échelle ont pour obligation d'effectuer cette analyse.

On remarque qu'il n'y a pas que les officines qui sont exclues de ces obligations : tous les professionnels de santé travaillant dans de petites structures ne requièrent pas de DPO ni de AIPD. Les professionnels de santé sont donc les

seules exceptions pour la CNIL, alors que les autres entreprises sont dans l'obligation d'effectuer ces démarches.

Cependant, dans le cadre du RGPD et de la certification ISO 9001 des pharmacies d'officine, il est fortement recommandé d'effectuer une AIPD. L'objectif étant d'avoir les données et leurs échanges les plus sécurisés possible, que cela soit pour prévenir les vols ou les pertes de données.

Une AIPD doit avoir 3 parties distinctes selon les recommandations de la CNIL qui sont élaborées conformément à la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) créé par la direction centrale de la sécurité des systèmes d'information faisant lui-même partie du Secrétariat général de la Défense et de la Sécurité nationale.

Figure 11 : Écran de démarrage du logiciel PIA de la CNIL

Afin d'aider les entreprises, la CNIL fournit un logiciel pour créer cette AIPD. Ce logiciel est nommé PIA de l'anglais Privacy Impact Assessment traduction de AIPD. Il est traduit en plusieurs langues visibles sur la Figure 11 et permet de produire une AIPD selon une méthode rigoureuse et testée. C'est un produit qualifié par la CNIL de « prêt à l'emploi »[16].

5.1.1.1 Contexte

En première partie, on retrouve la description du traitement des données effectué. Dans une officine, peu voire aucuns traitements ne sont effectués mais des données utilisables sont quand même récoltées. Les pharmaciens peuvent fournir ces données récoltées à leurs fournisseurs de LGO qui eux peuvent faire un traitement de ces données. Le pharmacien étant responsable de ces données, quand il veut faire une AIPD, il doit inclure le traitement de ces données effectué par les sous-traitants.

[16] « Outil PIA : téléchargez et installez le logiciel de la CNIL | CNIL ». (consulté le 21 mars 2020). https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

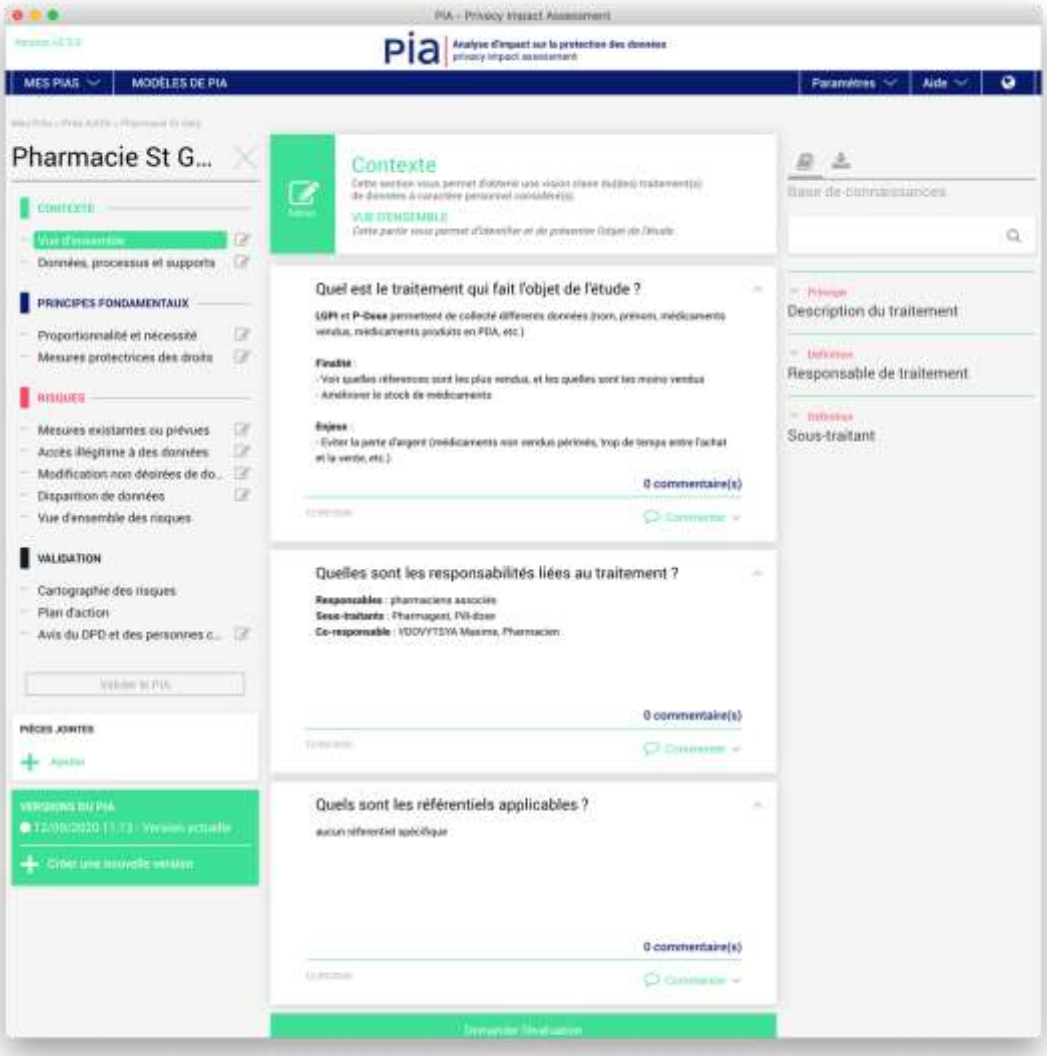


Figure 12 : Logiciel PIA, vue sur contexte, vue d'ensemble

Dans cette partie, on retrouve donc la description rapide du traitement, les responsables ainsi que les référentiels applicables regroupé dans le menu « vue d'ensemble », visible sur la Figure 12. Les données traitées, le cycle de vie des données, et le support des données sont regroupés dans le menu « données, processus et supports ».

Dans le menu « données, processus et supports », on retrouve des questions concernant les données traitées : quelles sont ces données, quels sont les destinataires des traitements et les personnes pouvant y accéder.

Les principales données récoltées en pharmacie vont être le nom, prénom, mail, numéro de téléphone, numéro de sécurité sociale et les médicaments vendus. Dans un LGO, le traitement effectué sur ces données afin de voir la quantité vendue de chaque médicament par personne et par mois est primordial à l'officine car il permet de gérer correctement les stocks et d'avoir une perte d'argent minimale.

Le cycle de vie des données permet de voir comment les données rentrent dans le traitement, donc de leur collecte, et jusqu'à leur modification et/ou leur destruction. Un schéma peut aider à compléter cette partie pour plus de compréhension. Il faut décrire toute la vie de ces données dans le but de voir les points faibles de la sécurité de ces données.

La dernière section concerne le support de ces données. Là aussi, on peut rapidement voir les points faibles liés au stockage.

5.1.1.2 Principes fondamentaux

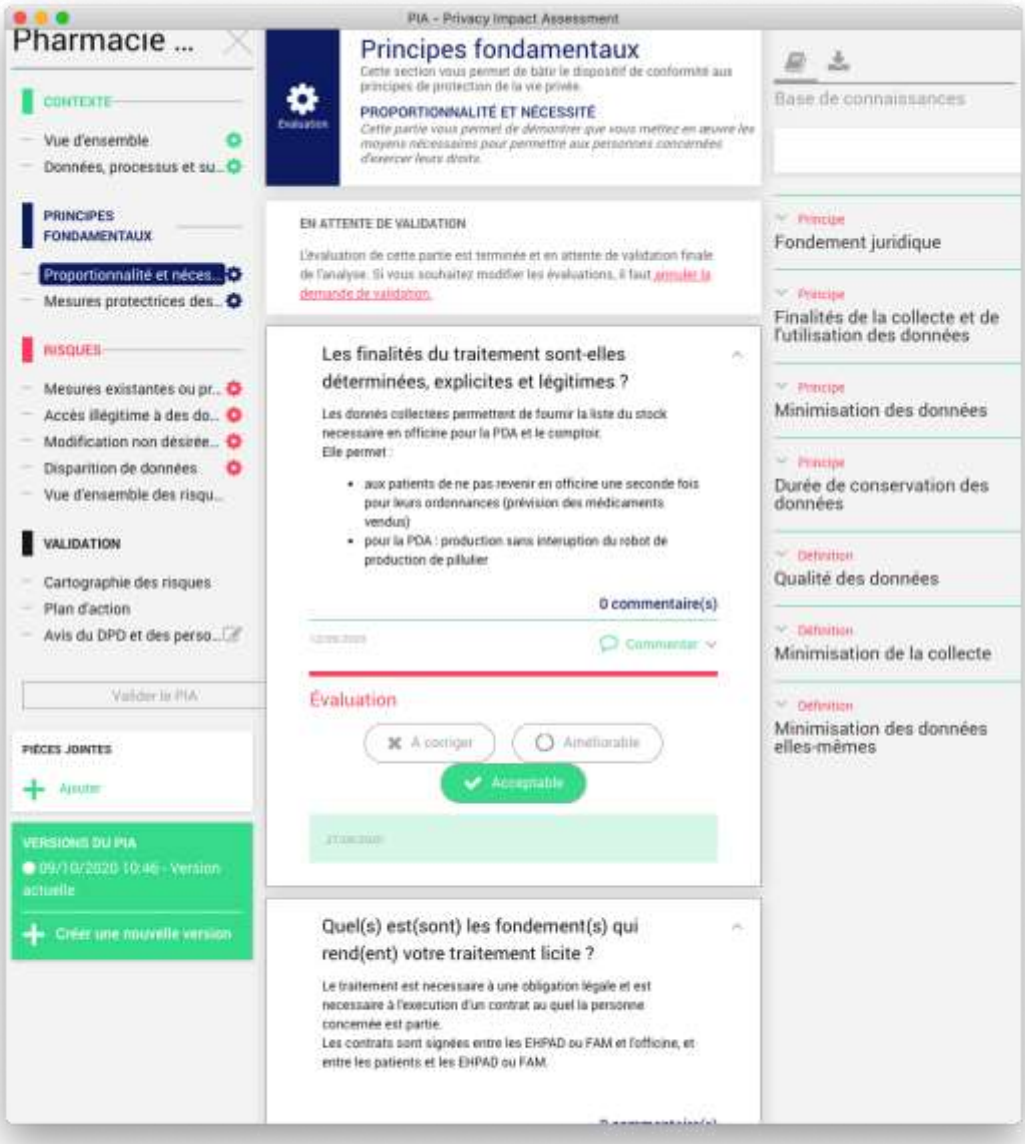


Figure 13 : PIA, vue sur principes fondamentaux, proportionnalité et nécessité

Dans la partie principes fondamentaux, il faut décrire les raisons et méthodes du traitement dans la sous partie « proportionnalité et nécessité », visible sur la Figure 13, et aussi les mesures déjà mises en place pour la protection des droits dans ce traitement.

Tout d'abord, il faut vérifier que les finalités du traitement soient déterminées, explicites et légitimes, afin d'être en conformité avec l'article 4 de la loi

informatique et liberté transposition de l'article 5 du RGPD. Toujours dans la même perspective du traitement décrit précédemment, la finalité est la gestion du stock dans l'optique d'éviter d'avoir trop de boites en stock ou d'avoir à faire revenir la patientèle. Cette finalité est bien déterminée, explicite et bien légitime.

Vient ensuite la légalité du traitement, notamment la présence ou non d'un contrat signé avec les personnes fournissant leurs données et l'entreprise qui les traite, ou encore les obligations légales de conservation de ces données. Concernant la gestion du stock, les données sont collectées et stockées par obligation légale. En effet, il faut conserver les ordonnances pendant au minimum 3 ans, et avoir un registre (les médicaments vendus, le prescripteur, et le nom du patient) pendant au moins 10 ans. Si on regarde de plus près les services proposés par certaines officines, on peut voir que la PDA joue un rôle important. Pour la PDA, un contrat entre l'EHPAD et l'officine est obligatoire, signé par le patient ou son représentant légal et par l'officine ou l'EHPAD est fortement conseillé. Dans ce contrat, on peut stipuler que les données collectées pour produire les piluliers peuvent être utilisées pour des traitements.

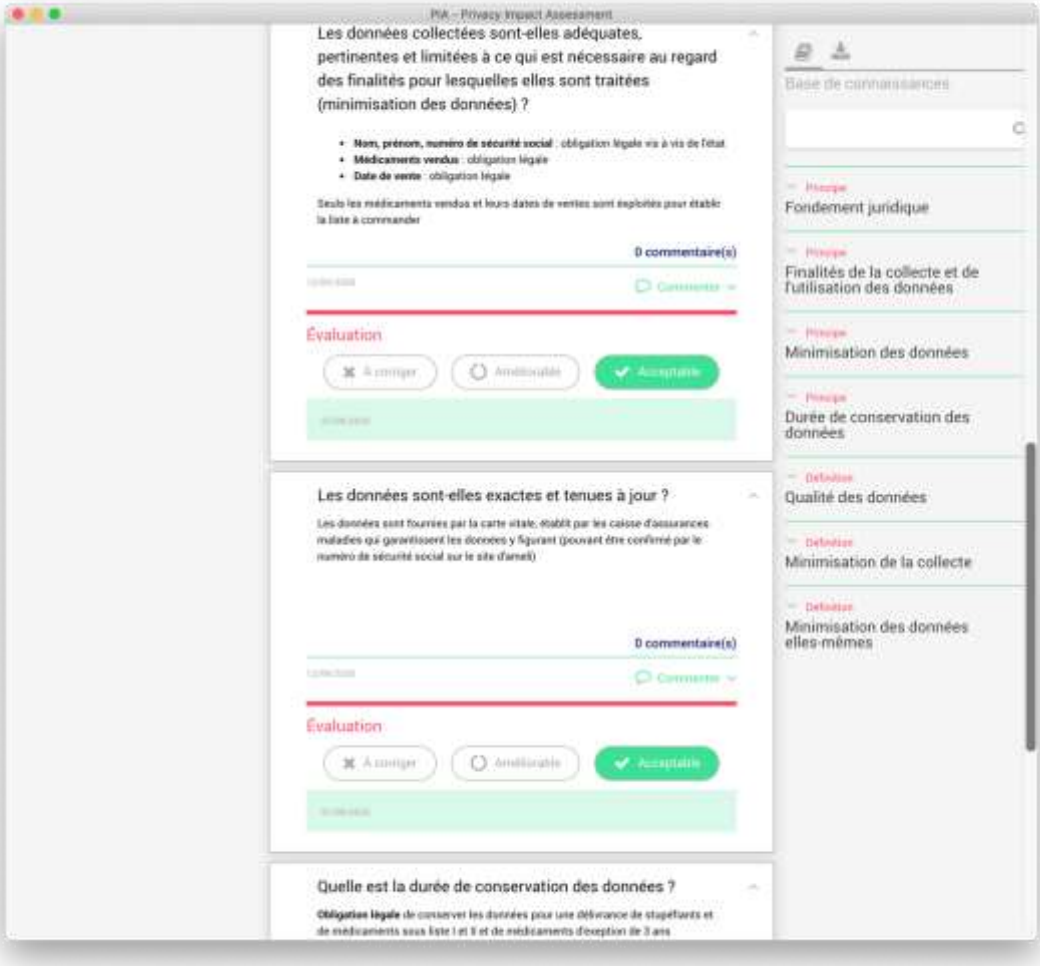


Figure 14 : PIA, vue sur principes fondamentaux, proportionnalité et nécessité, suite

Puis, le logiciel demande si les données collectées sont limitées au strict minimum nécessaire pour le traitement effectué, visible sur la Figure 14. En effet, collecter des données non utiles au traitement est d'une part contre-productif, et d'autre-part n'est pas en adéquation avec le RGPD. Cependant, en officine, pour la gestion du stock, lors de la collecte de données, certaines données ne sont pas utiles mais nécessaires d'un point de vue légal. Par exemple, lors d'un retrait de lots, le pharmacien doit pouvoir contacter le patient afin de le prévenir.

Il faut, par la suite, signaler l'exactitude et l'actualisation des données précédemment collectées pour ce traitement. Lors de la collecte, en officine, le

pharmacien ou le préparateur utilise la carte vitale du patient. Ce sont les caisses d'assurances maladies qui ont pour devoir de garantir la véridicité des données inscrites sur la carte vitale ou disponibles par le biais du numéro de sécurité sociale. L'exécuteur de la collecte uniquement les médicaments vendus et les coordonnées du patient.

Enfin, il faut renseigner la durée de conservation des données collectées. Pour rappel, en officine, la durée légale de conservation est de 3 ans pour les ordonnances et de 10 ans pour les registres. Cependant, les médicaments ne révélant pas de la liste des stupéfiants, de la liste I et II, n'ont de durée de conservation ni obligatoire ni légale mais sont généralement conservés une décennie avec les médicaments listés.

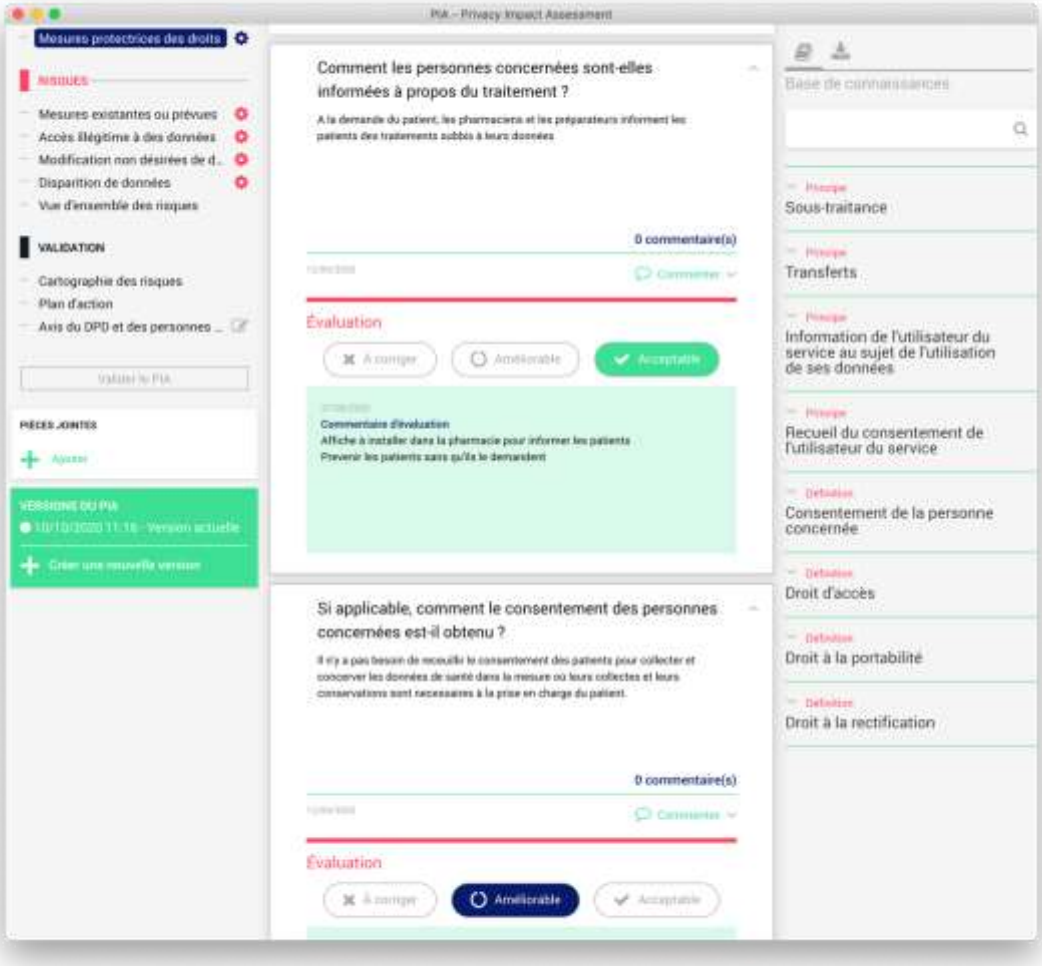


Figure 15 : PIA, vue sur principes fondamentaux, Mesures protectrices des droits

Après avoir renseigné le menu « proportionnalité et nécessité », il faut remplir le menu « mesures protectrices des droits pour compléter le menu principes fondamentaux ».

Ce menu, visible sur la Figure 15, se concentre essentiellement sur les droits informatiques fondamentaux de la loi informatique et liberté décrit précédemment.

Dans un premier temps, il faut démontrer que le patient peut exercer son droit à l'information. En officine, il est donc obligatoire de prévenir le patient si ses données sont traitées. En pratique, l'équipe officinale n'informe que peu les patients lors de leurs passages sur le traitement des données. Souvent, les informations sont

données sur demande du patient auprès de l'équipe officinale. L'ouverture de DMP est le seul cas où cette information est donnée, car les logiciels nécessitent l'approbation du patient.

Vient un point crucial, celui du consentement des personnes concernées. Dans n'importe quelle entreprise, il faut obligatoirement demander le consentement des patients avant de pouvoir récolter et traiter les données. Cela peut se faire sous forme de contrat à signer ou par le biais informatique, en cliquant sur « j'ai lu et accepté » lors d'un achat sur internet par exemple. Les professionnels de santé sont une exception. En effet, ils dirigent des petites entreprises mais le consentement du patient n'est pas obligatoire, car les données récoltées font partie d'une obligation légale du fait qu'elles soient nécessaires à la bonne prise en charge du patient. Par ailleurs, le logiciel PIA le précise bien, il y a la mention « si applicable » dans la question posée aux responsables.

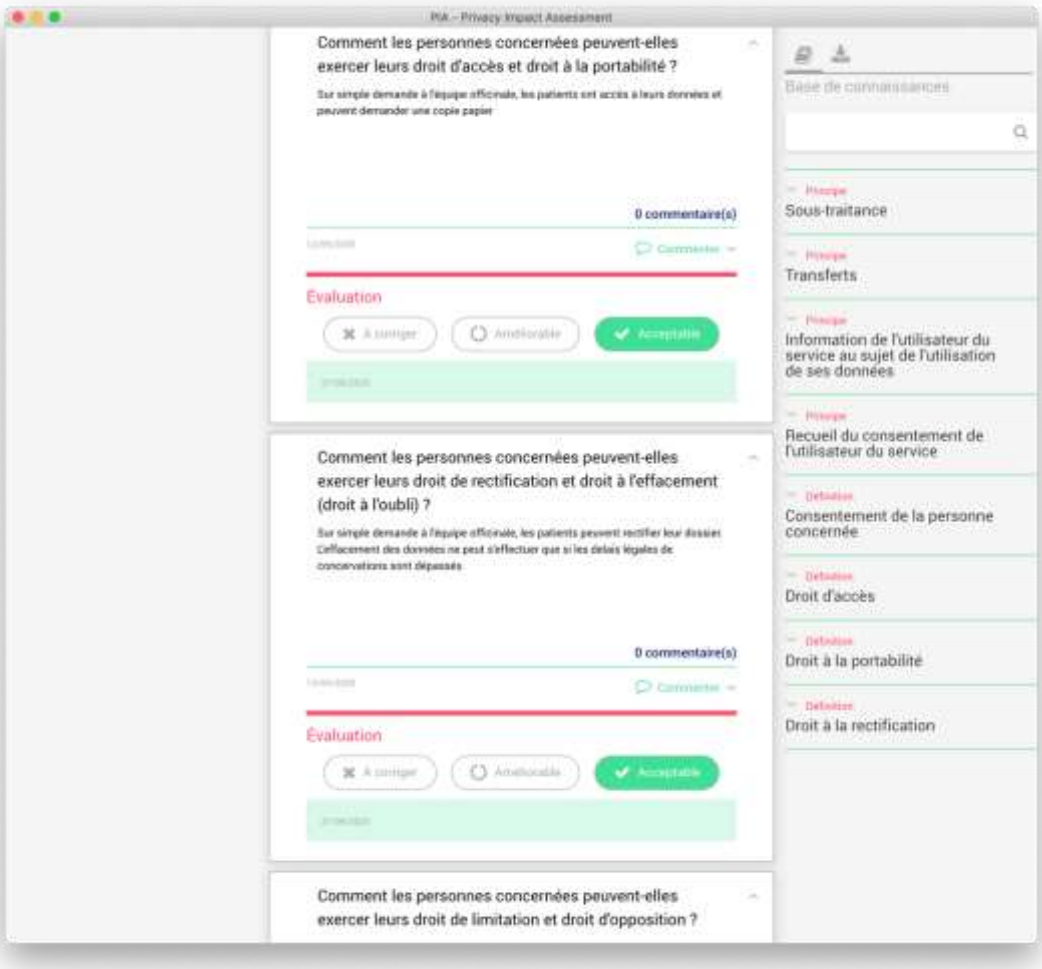


Figure 16 : PIA, vue sur principes fondamentaux, Mesures protectrices des droits, suite

Après le consentement, il y a le droit d'accès et de portabilité, visible sur la Figure 16. Le droit de portabilité est inclus dans le droit d'accès : à tout moment, la personne concernée peut récupérer toutes ou une partie de ses données. Sur simple demande du patient, l'équipe officinale doit être en capacité de montrer les données qu'elle possède sur le dit patient. Dans la plupart des LGO, des commentaires peuvent être écrits dans la fiche du patient. Ces données-là sont affiliées à un nom, et doivent être accessibles par le patient. Ces commentaires ne doivent donc servir qu'à aider l'équipe officinale à correctement effectuer leur travail.

Ensuite, le logiciel demande des informations sur le droit de rectification et le droit à l'oubli. Sur simple demande du patient, l'équipe officinale peut normalement modifier certaines données (adresses, e-mail, téléphone). Les données concernant les ordonnances ne peuvent être modifiées sauf s'il y a eu une mauvaise délivrance. Cependant, les données récoltées pour la bonne prise en charge du patient, ne peuvent être effacées du fait de l'obligation légale de les conserver. Par conséquent, le droit à l'oubli ne peut être appliqué par un patient sur l'intégralité de ses données, mais uniquement sur les données non obligatoires.

Les droits d'opposition et de limitation sont restreints en officine au même titre que le droit à l'oubli. Les patients ne peuvent donc s'opposer en officine à la collecte et au stockage de leurs données. Cependant, ils peuvent s'opposer à leur traitement et à la collecte des information non nécessaires à la bonne prise en charge sur une simple demande au responsable ou à un membre de son équipe.

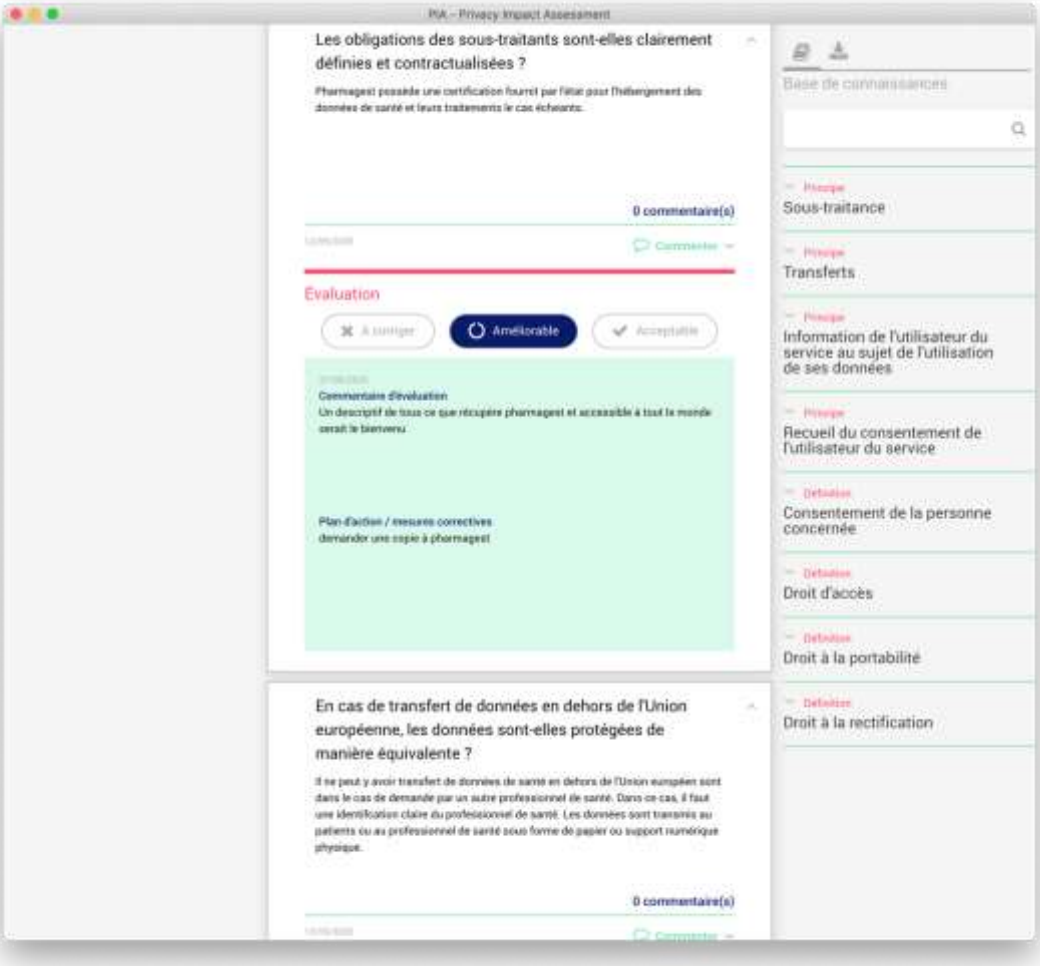


Figure 17 : PIA, vue sur principes fondamentaux, Mesures protectrices des droits, fin

Les entreprises peuvent, si elles le souhaitent et ou si elles ont la possibilité légale, vendre leurs données collectées ou sous-traiter leur traitement. Pour cela, il faut obligatoirement un contrat permettant d'identifier clairement ces sous-traitants. En officine, la plupart du temps, le fournisseur du LGO peut être sous-traitant du traitement, ou simplement fournir le logiciel permettant le traitement. Le pharmacien ou le responsable des données doit obligatoirement fournir à la CNIL, si elle le demande, le contrat entre l'officine et le sous-traitant, ainsi que le descriptif des traitements effectués par le sous-traitant. En pratique, le pharmacien peut

simplement demander au fournisseur du LGO tout le descriptif des traitements effectués, et le montrer à la CNIL le cas échéant.

Pour finir les mesures protectrices des droits, et donc le menu « principes fondamentaux », visible sur la Figure 17, il ne reste plus qu'à compléter la partie concernant les transferts de données en dehors de l'Union Européenne. En fait, les données collectées quotidiennement à l'officine concernant la vente de médicament ne peuvent être envoyées qu'au patient, son représentant légal le cas échéant, à son médecin traitant, au médecin spécialiste consulté, au médecin urgentiste en cas d'urgence ou encore à un autre pharmacien si le patient est client chez lui. Donc, hormis au patient lui-même ou à un professionnel de santé, on ne peut faire transiter ces données en dehors de l'Union Européenne. Pour les envoyer, il faut donc clairement identifier leur receveur et la remise ne peut s'effectuer qu'en main propre ou par papier sous pli confidentiel ou support physique.

5.1.1.3 Risques

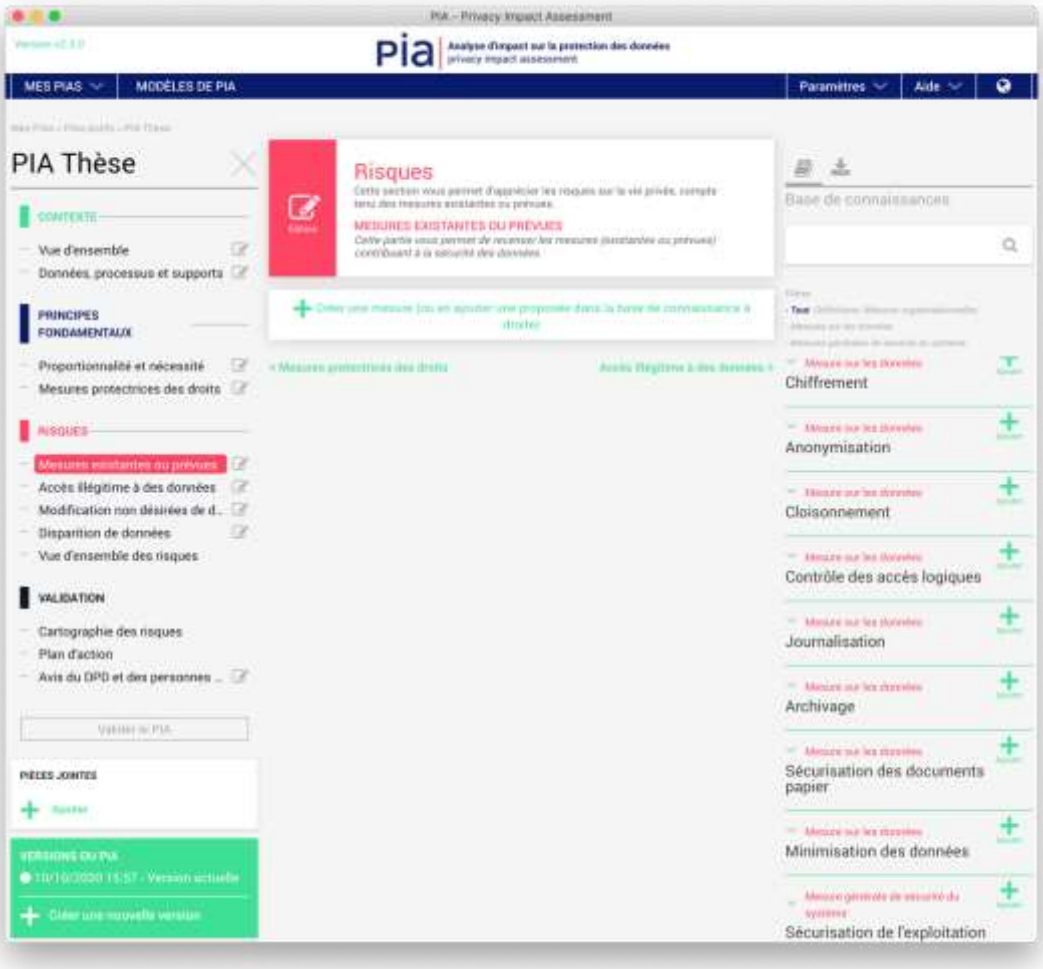


Figure 18 : PIA, vue sur Risques, Mesures existantes ou prévues

Après avoir renseigné les points clés du traitement des données, il faut compléter toute la partie risque, qui représente réellement l'analyse d'impact.

En premier lieu, il faut faire l'inventaire des mesures existantes, puis intégrer les mesures prévues. Comme le montre la Figure 18, il y a un certain nombre de mesures préétablies par le logiciel, il suffit juste de les ajouter en cliquant sur « créer une mesure ».

Parmi les mesures proposées par le logiciel PIA, certaine sont applicables à l'officine (liste exhaustive) :

- Le chiffrement : concernant les sauvegardes, les postes de travail et les serveurs
- La journalisation et la traçabilité : chaque acte est renseigné dans un fichier de journalisation avec l'identification de celui qui s'en occupe, cette mesure fournie par le LGO est automatique
- La sécurisation des documents papiers : tout papier présentant des données privées non utilisées doit être broyé (ordonnances, tickets de dûs, …)
- La sécurisation de l'exploitation : alarmes, rideau de fer, portes fermées à clefs …
- La lutte contre les logiciels malveillants : antivirus sur chaque poste
- La gestion des postes de travail (avec l'authentification et les mots de passe)
- La protection des sites web : avec un site héberger sur un HDS
- La sauvegarde des données, pour éviter les pertes de données
- La maintenance, avec des contrats en bonne et due forme
- Le ou les contrat(s) de sous-traitance et la gestion des tiers accédant aux données
- La sécurisation des canaux informatiques (grâce aux cartes CPS et carte vitale)
- La sécurisation des matériels et l'éloignement des sources de risques : armoires ignifugées, extincteurs aux normes, …
- Gestion des personnels : chaque personne touchant aux données doit être habilitée (avec un diplôme ou en cours de formation)

Après avoir identifié toutes les mesures réalisées ou prévues, le logiciel permet d'accéder aux menus suivants étant donné qu'il y a besoin de ces mesures pour compléter la suite de l'analyse d'impact.

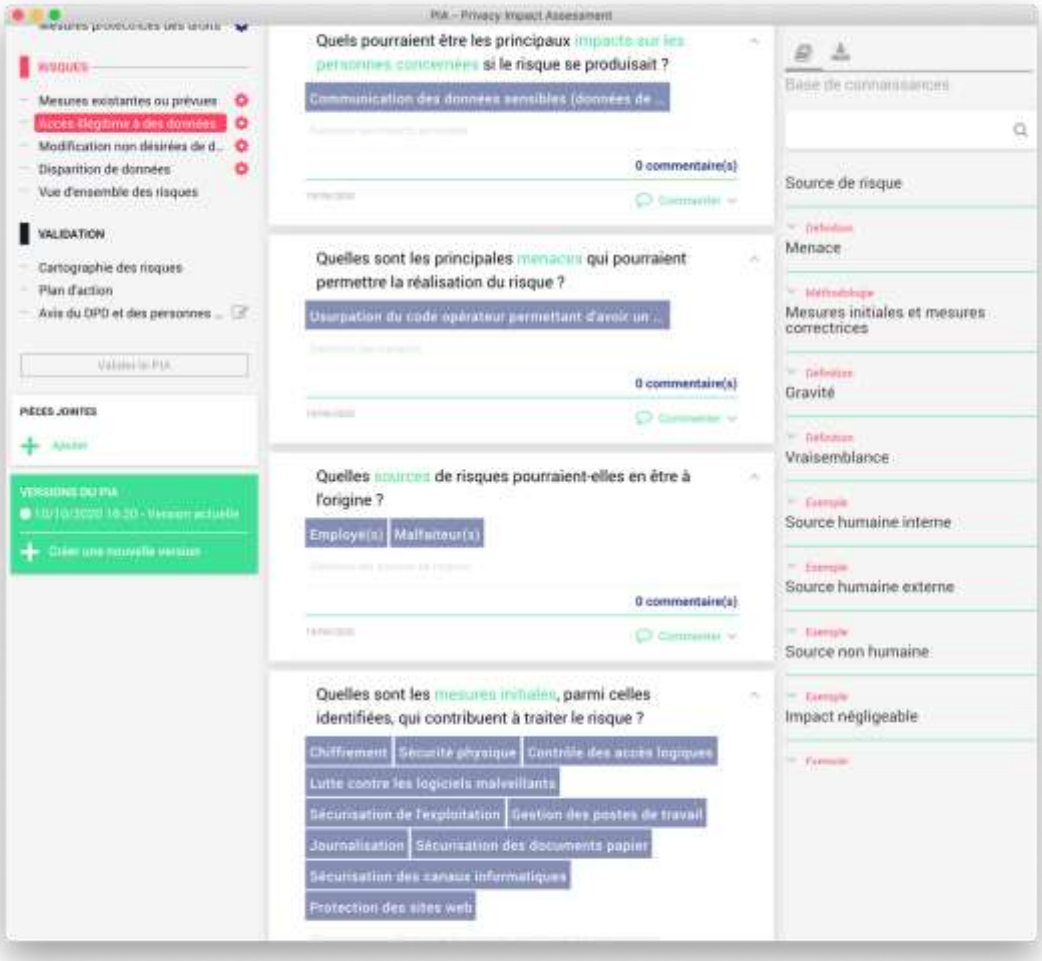


Figure 19 : PIA, vue sur Risques, Accès illégitime à des données

Il y a au total 3 grands risques dans cette étude d'impact :

- Accès illégitime à des données, visible sur la Figure 19
- Modification non désirée des données
- Disparition des données

Dans chacun de ces risques, le logiciel PIA demande :

- L'impact si le risque se produit sur la personne concernée
- Les menaces permettant la réalisation du risque
- Les sources qui pourraient être à l'origine du risque
- Les mesures identifiées précédemment permettant de diminuer le risque
- La gravité du risque, avec le choix entre : Non définie, Négligeable, Limitée, Importante, Maximale
- La vraisemblance du risque au vue des mesures, donc les chances que le risque se produise. Le logiciel propose entre : Non définie, Négligeable, Limitée, Importante, Maximale

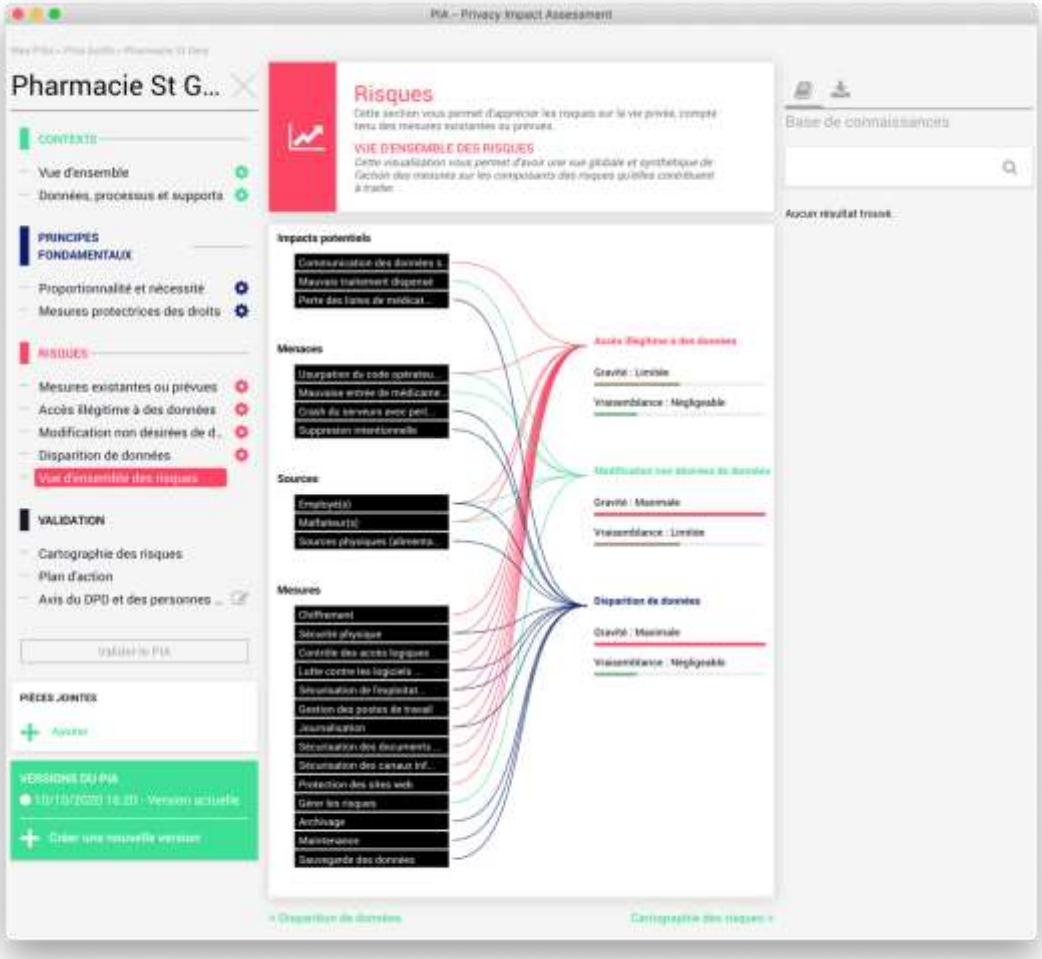


Figure 20 : PIA, vue d'ensemble des risques

Après avoir dument complété l'ensemble des risques et des mesures associées, le logiciel PIA crée automatiquement un graphique sur la vue d'ensemble des risques. Sur la Figure 20, on peut voir un exemple de la vue d'ensemble des risques. Il y a donc listés les impacts potentiels, les menaces, les sources et les mesures liées à chaque risque. On peut y voir que les impacts potentiels sont différents pour chaque risque, mais que les différentes sources peuvent être la cause de risques différents, et enfin que les mesures mis en place peuvent réduire plusieurs risques à la fois.

5.1.1.4 L'évaluation

Après avoir entièrement complété les informations demandées, la personne responsable de la PIA demande l'évaluation de cette analyse d'impact à une autre personne de l'entreprise pour y interpréter et valider ces différentes informations. Cette dernière personne évalue donc l'analyse d'impact et juge si les mesures mises en place sont conformes, à améliorer ou non conforme avec le RGPD. Il peut y rajouter des commentaires pour améliorer la sécurité des données dans la structure.

Au terme de l'évaluation, la personne en charge peut accéder à la partie validation.

5.1.1.5 Validation

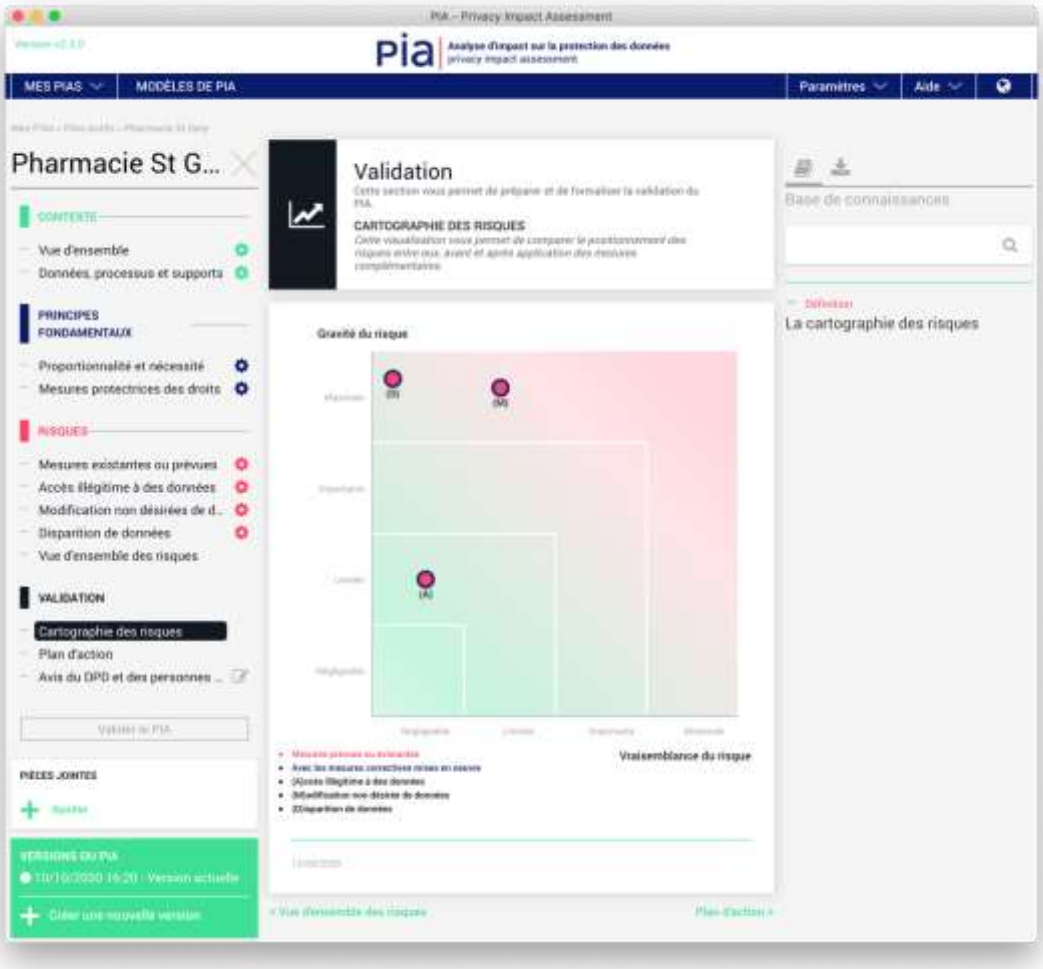


Figure 21 : PIA, Cartographie des risques

Après l'évaluation, le logiciel PIA cartographie les risques et crée un graphique, visible sur la Figure 21, permettant de voir l'impact de ces risques.

Suivant la gravité et la vraisemblance du risque, il faut plus ou moins s'inquiéter afin de pouvoir réévaluer les mesures si besoin. Bien sûr, la cartographie des risques est faite à un instant T. Par définition : la gravité de chaque risque ne peut être diminuée. Seules les mesures supplémentaires prises ou les mesures entérinées qui pourraient modifier ce graphique en modifiant la probabilité du risque.

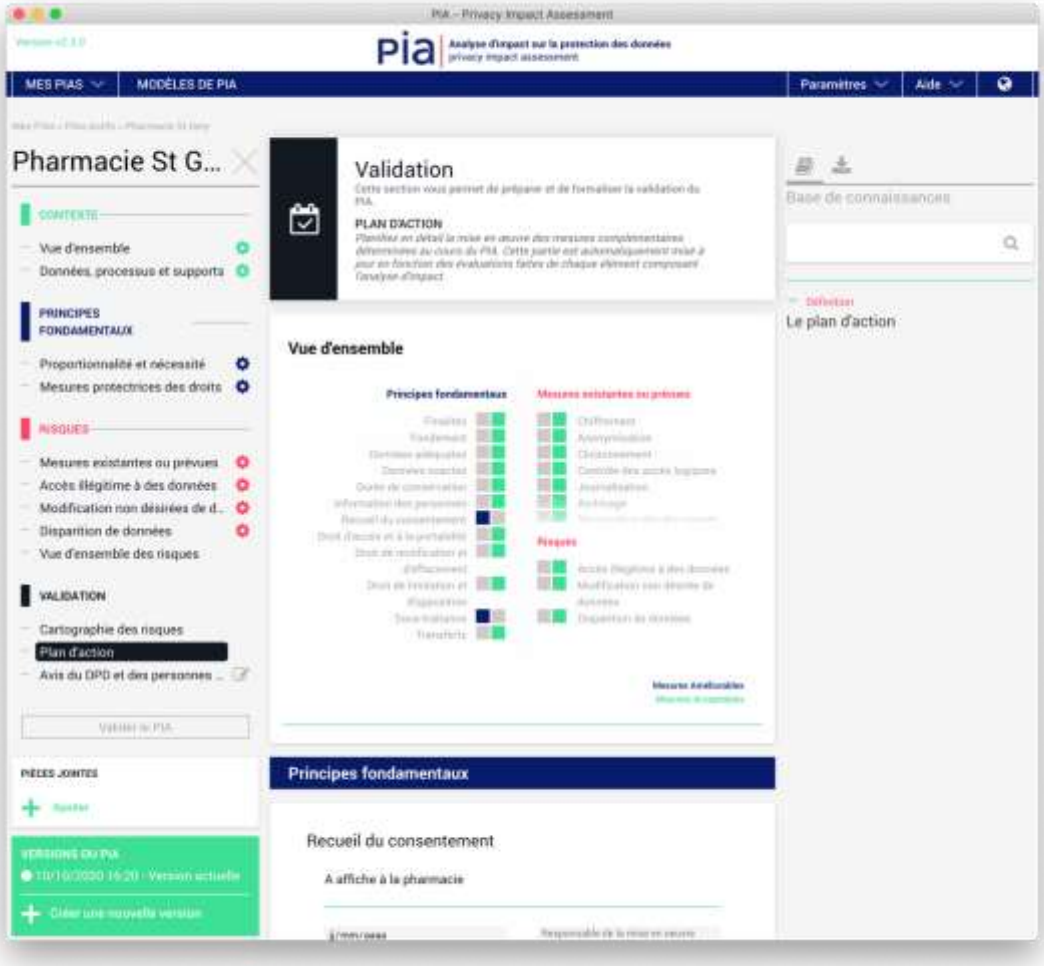


Figure 22 : PIA, Plan d'action

Ensuite, le logiciel PIA regroupe toutes les données rentrées et évaluées pour créer un plan d'action. Ce plan répertorie chaque point de l'analyse de risque et met en avant l'évaluation avec les mesures acceptables et celles à améliorer. Sur la Figure 22 : PIA, Plan d'action : un exemple de plan d'action, on peut voir que suite à l'évaluation, les points recueil du consentement et la sous-traitance sont à améliorer ; le reste étant acceptable. Plus bas, le responsable de l'analyse d'impact peut planifier avec une date précise chaque point améliorable et en y désignant un référent.

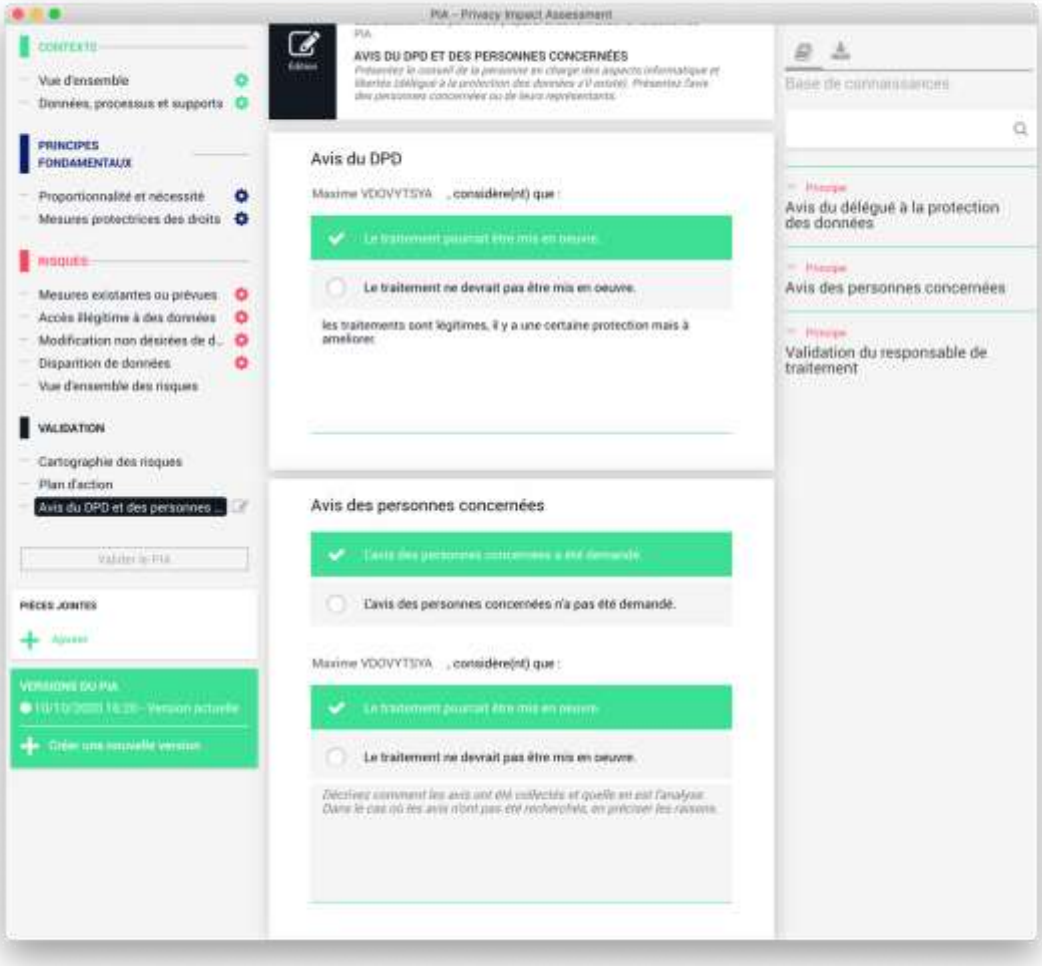


Figure 23 : PIA, Avis du DPD

Enfin, pour conclure l'analyse d'impact, le DPO doit se prononcer sur le traitement, un exemple est représenté sur la Figure 23 : PIA, Avis du DPD. On remarque que l'analyse d'impact doit se faire en théorie en amont de la mise en place d'un traitement. Cependant, on peut aussi effectuer cette analyse d'impact après que le traitement ait été mis en place, comme c'est le cas ici.

Le logiciel PIA est un logiciel ciblant tous types d'entreprises faisant transiter des données informatiques. Il n'est donc pas spécifique à l'officine, de ce fait il dispose d'outils non nécessaires à l'officine.

D'autres outils non spécifiques à l'officine sont disponibles dans le but de sécuriser le stockage et l'échange de données patients, certains sont même cités au sein du logiciel PIA.

5.1.2 Anti-virus

Les logiciels anti-virus se sont développés suite à l'apparition de virus informatique dans les années 1980. Pour contrer ces virus, diverses compagnies ont mis en place plusieurs solutions : Avira a été créé en 1986, McAfee en 1987, Norton en 1991 et Kaspersky en 1997.

Il y a différentes classes de virus informatiques circulant dans le monde. Parmi ces virus, on y retrouve divers types de logiciels. Certains sont capables de copier l'intégralité d'un disque et peuvent donc conduire à une fuite de données. D'autres sont des rançongiciels ou ransomware cryptant les données (les utilisateurs ne peuvent plus accéder à leurs données) et demandant une rançon pour pouvoir débloquer ces données. En mai 2017, a eu lieu une des plus grandes attaques informatiques par rançologiciel, nommé WannaCry, touchant plus de 300 000 ordinateurs. On retrouve aussi d'autres virus, comme des malwares type wiper qui effacent des données. Toujours en 2017, il y a eu l'attaque NotPetya, virus qui effaçait les données du disque dur.

Pour protéger ses données, une entreprise, affiliée ou non à la santé, doit obligatoirement recourir à un ou plusieurs antivirus ainsi qu'à d'autres outils associés. Les différents éditeurs d'antivirus proposent des suites informatiques comportant l'antivirus lui-même et les autres outils associés (pare-feu, protection des mots de passe, anti-bannières, …). Aujourd'hui, les 6 plus grands éditeurs

d'antivirus représentant à peu près 70% du marché sont Norton de NortonLifeLock (anciennement Symantec Corporation), NOD32 d'ESET, McAfee VirusScan de McAfee, les diverses solutions de Bitdefender, les suites de Karspersky Lab et Avast Antivirus d'Avast Software.

Il n'y a pratiquement plus de différence entre ces différentes solutions de protection. Pour savoir lequel est le plus adapté à son officine, il faut surtout comparer les prix et la composition des différents packs proposés par les éditeurs.

Le réseau informatique est un ensemble d'ordinateurs (PC ou serveurs) fonctionnant côte à côte. En sécurité informatique, ce réseau se comporte comme une chaine avec des maillons. Si un des maillons de cette même chaine n'est pas correctement protégé, alors toute la chaine n'est pas protégée. Il faut donc installer des solutions antivirales sur tous les postes et serveurs à l'officine pour éviter les fuites ou pertes de données.

Les antivirus ne sont efficaces qu'à la condition qu'ils soient correctement employés et dans un système correctement mis à jour.

5.1.3 Mises à jour des logiciels

Dans une officine, les mises à jour à exécuter sont nombreuses et dépendent des logiciels utilisés. On retrouve deux sortes de mises à jour à l'officine.

D'une part il y a les mises à jour automatiques. Les antivirus y ont recours pour éviter d'être dépassés par les nouveaux virus. Il y a aussi les LGO qui en font usage afin que l'équipe officinale puisse correctement facturer avec les nouvelles lois et arrêtés promulgués.

Dans cette catégorie, on peut classer les systèmes d'exploitation. Cependant, la plupart du temps, pour les mises à jour de sécurité, le système d'exploitation télécharge les mises à jour et les installe automatiquement lors d'un arrêt ou redémarrage du système. Lorsque ce ne sont pas des mises à jour de sécurité, cela dépend des réglages de l'utilisateur. Par exemple, par défaut les systèmes d'exploitation de Microsoft® alertent quand il y a une mise à jour et c'est l'utilisateur qui doit exécuter la mise à jour.

D'autre part, d'autres logiciels sont installés sur les postes et serveurs des officines ne faisant pas de mises à jour automatiques. C'est à l'utilisateur de sans cesse vérifier s'il y a une nouvelle mise à jour.

Mettre à jour les divers logiciels et le système d'exploitation est primordial. Les mises à jour bouchent des failles de sécurités (on appelle ça des mises à jour de sécurités) qui auraient permis à des malandrins des récupérer ou d'effacer des données sans même que l'antivirus intervienne. Les plus grosses failles informatiques découvertes au début de ce siècle sont les failles Meltdown et Spectre qui sont des failles matérielles, donc impossibles à corriger. Cependant, une mise à jour de sécurité est sortie pour éviter que ces failles ne puissent être utilisées. Il faut absolument avoir mis à jour son système, car les antivirus ne peuvent détecter les logiciels utilisant ces failles.

Quand quelqu'un veut accéder à des données stockées sur un poste ou un serveur, avant de programmer un virus, il peut tout à fait essayer d'y accéder de manière physique.

5.1.4 Les mots de passe

Pour protéger les intrusions physiques sur un poste, il faut que la protection soit efficace. Une des premières protections est le mot de passe. Cette solution figure parmi les mesures à appliquer ou prévues dans le logiciel PIA.

Il y a plusieurs niveaux de contrôle gérés par des mots de passe et tous ces niveaux sont différents en termes de sécurité de données.

5.1.4.1 Mot de passe session et compte d'utilisateur

S'il est mis en place, c'est le premier mot de passe à rentrer lorsqu'on allume un ordinateur et que le système d'exploitation démarre. Ce mot de passe permet d'éviter que des intrus ne pénètrent simplement sur un ordinateur pour y récupérer ou effacer des données confidentielles.

Pour encore plus sécuriser le système, la meilleure solution est d'avoir 2 comptes utilisateurs : un compte administrateur et un compte utilisateur simple. Évidemment les deux sont protégés par des mots de passes différents. Cela permet une protection par mot de passe. De plus, utiliser un compte utilisateur simple au quotidien permet d'éviter certains problèmes : avec ce genre de compte on ne peut ni modifier les configurations système ni installer de logiciel. Ce type de fonctionnement est plus compliqué au quotidien, car il faut obligatoirement se connecter au compte administrateur à chaque mise à jour afin qu'elle puisse s'effectuer correctement, mais cela assure une sécurité plus importante du système.

5.1.4.2 Mot de passe des sauvegardes et des serveurs

Comme on a pu le voir précédemment, pour gérer toute l'officine, il faut généralement recourir à un serveur. Sur ce serveur, on retrouve un LGO avec un mot de passe serveur obligatoire.

Pour plus de sécurité, on peut avoir recours à un serveur de sauvegarde qui est généralement constitué d'un NAS. Sur ce NAS, il faut obligatoirement un mot de passe pour y accéder et modifier les réglages. Cependant, si l'on ne paramètre pas correctement un NAS, on peut s'y connecter en tant qu'utilisateur anonyme sans mot de passe et accéder à toutes les données. Afin d'y remédier, il faut désactiver l'accès aux utilisateurs anonymes et chiffrer les données présentes sur le disque dur du NAS. Toutes ces options sont disponibles dans les réglages du NAS.

5.1.4.3 Mot de passe des Carte Professionnelle de Santé et des Cartes de Personnel d'Établissement

Dans le cadre de la facturation des ordonnances, il faut obligatoirement une carte CPS ou CPE. Chacune de ces cartes dispose d'un code à 4 chiffres permettant de s'identifier. Sans ce code, on ne peut ni accéder aux DP et DMP ni télétransmettre les ordonnances facturées.

5.1.4.4 Mots de passe et code opérateur des LGO

Les différents LGO mis sur le marché permettent d'accéder à l'intégralité ou seulement une partie des données grâce à un code opérateur créé par le responsable de l'officine. Ce code permet surtout une certaine traçabilité : toutes les actions effectuées par un code opérateur sont enregistrées et peuvent être consultées à posteriori.

Ce code opérateur est généralement composé de 2 chiffres, et ne peux être désigné comme mot de passe. Toute personne ayant accès au LGO, peut sans moindre effort, accéder à au moins une partie des données. Il lui suffit d'essayer de mettre 2 chiffres au hasard, et il pourra tomber facilement sur un code opérateur fonctionnel. Donc ce n'est réellement pas une protection adéquate.

A ce code on peut, de façon non obligatoire, y ajouter un mot de passe. Donc pour pouvoir accéder à des données, il faut une combinaison correcte du code opérateur et du mot de passe associé.

5.1.5 Logiciels de gestion d'officine

Les LGO sont les outils les plus utilisées quotidiennement en officine. Pour pouvoir être installé dans une officine et y manipuler des données de santé, il faut obtenir une certification auprès d'un organisme certificateur. Cela confère une certaine sécurité dans l'esprit des utilisateurs.

Les connexions entre l'officine, les serveurs du prestataire LGO et les serveurs des caisses d'assurance maladie sont obligatoirement sécurisés par chiffrement. Toutes les informations, que cela soit l'ordonnance numérisée envoyée par le biais de la norme SCOR ou les médicaments facturés en FSE sont chiffrées de bout en bout grâce aux carte CPS ou CPE et la Carte Vitale.

5.1.6 Cartes Professionnelle de Santé, de Personnel d'Établissement et Vitale

Les Cartes Professionnelles de Santé, de Personnel d'Établissement et Vitale sont géré par le groupement d'intérêt économique SESAM-Vitale crée en 1993.

Ce groupement gère l'attribution des CPS et Cartes vitales mais aussi leur chiffrement et celui de la communication faite grâce à ces cartes. Lors du chiffrement, chaque CPS ou CPE génère par le biais logiciel une bi-clé RSA (une clé publique et une clé privée) par le biais du logiciel afin de sécuriser les données. Pour communiquer, l'officine possède un certificat SSL/TLS fourni automatiquement par

le GIE SESAM-Vitale dès lors que les CPS ou CPE sont utilisées. Ce certificat permet l'authentification entre les serveurs, l'intégrité et la confidentialité des données envoyées ou reçues. Pour signer, l'officine possède un certificat S/MIME toujours fourni par la GIE SESAM-Vitale[17].

Ces chiffrements sont opérés de façon invisible à l'utilisateur. Il faut simplement insérer la CPS ou la CPE dans le lecteur, s'identifier par le code à 4 chiffres et puis introduire la carte vitale dans le lecteur pour que le logiciel interne du lecteur puisse chiffrer les différentes données à envoyer sans aucune intervention.

[17] « Certificats SSL/SMIME de l'agence du numérique en santé | Intégrateurs CPS ». (consulté le 4 septembre 2020). https://integrateurs-cps.asipsante.fr/pages/Certificats-SSLSMIME-de-lASIP-Sant%C3%A9.

5.1.7 Séparation locale des réseaux

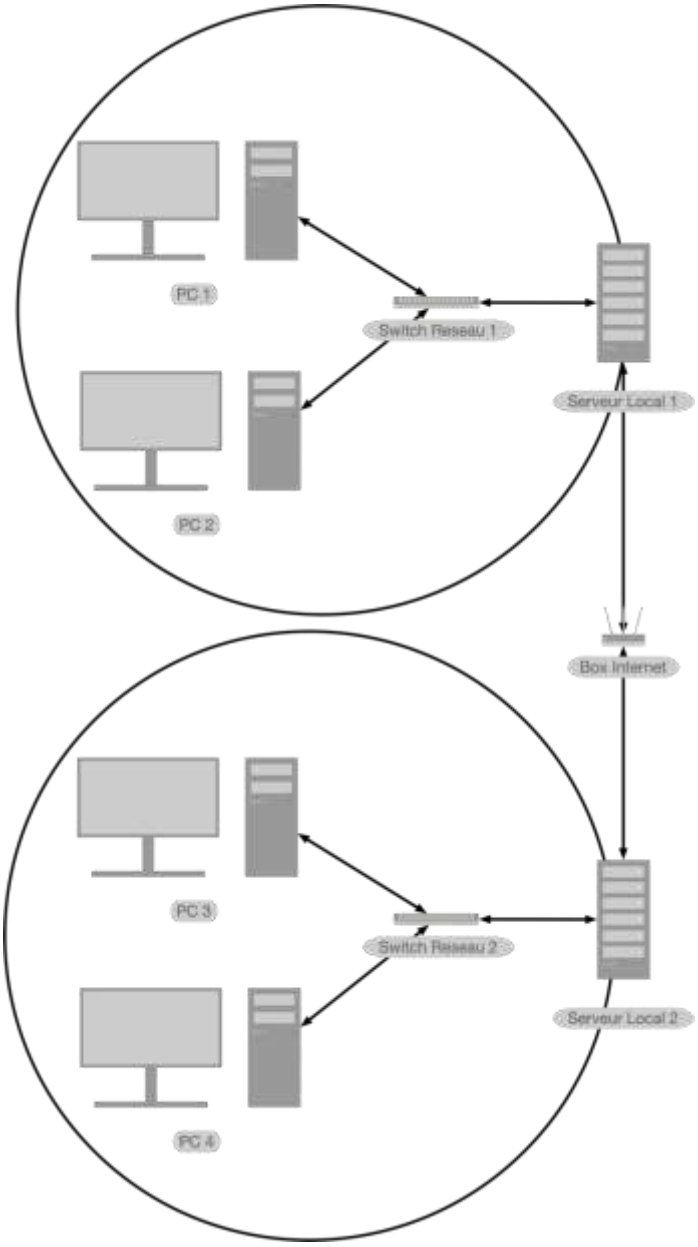


Figure 24 : Réseaux locaux séparés

Dans le monde de l'entreprise, il existe des outils servant à sécuriser encore plus les divers réseaux. On retrouve la séparation du réseau de l'entreprise en plusieurs petits réseaux locaux séparés les uns des autres, comme illustré en Figure 24 : Réseaux locaux séparés. Dans cette figure, on peut voir que les PC 1 et 2 ne peuvent communiquer simplement avec les PC 3 et 4. En reprenant l'exemple de la chaine avec des maillons, ici l'entreprise possède plusieurs chaines, donc quand un

pc est infecté par un virus, ce virus reste dans le réseau local du pc et ne pourra infecter les PC des autres réseaux locaux.

Cette méthode est compliquée à mettre en place, surtout au sein d'une officine, où il faut obligatoirement communiquer avec le serveur fournit par le prestataire du LGO. De bonnes connaissances en réseau informatique sont nécessaires pour avoir ce type de réseau dans une officine. Cela reste malgré tout faisable et beaucoup plus sécurisé que d'avoir des PC reliés entre eux sans fractionnement.

5.1.8 Messagerie sécurisée

Pour rappel, l'État a créé Mailiz par MSSanté, une messagerie sécurisée compatible avec la plupart des logiciels de messagerie. Pour simplifier la mise en place de cet outil, une brochure a été éditée. Elle montre étape par étape l'utilisation de Mailiz : de sa création à son intégration à un logiciel tel que Mozilla Thunderbird[18].

[18] « Créer son compte MSSANTE », s. d., https://www.ameli.fr/sites/default/files/creer_sa_mss.pdf.

Figure 25 : Page initiale de Mailiz

Pour ouvrir un compte sur MSSanté, il faut une CPS, de son code et un lecteur. Il faut ensuite se rendre sur le site de MSSanté. Après avoir cliqué sur « J'ACTIVE MON COMPTE », comme montré sur la Figure 25 : Page initiale de Mailiz, il faut s'identifier par le biais de sa CPS, en vérifiant que tous les logiciels associés au lecteur de carte soient bien installés et allumés.

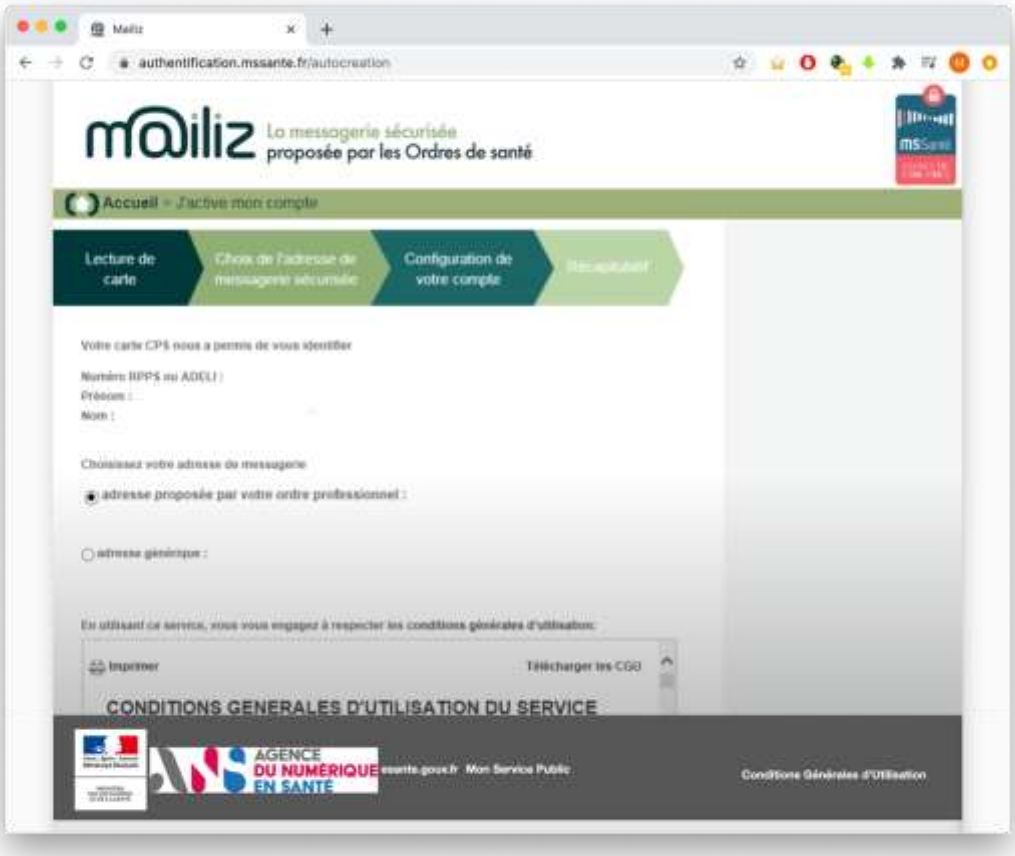


Figure 26 : Mailiz : choix de l'adresse mail

Après avoir entrée le code de la CPS, le professionnel de santé doit choisir son adresse mail d'identification, visible sur la Figure 26. Cette adresse mail se compose comme suit :

prenom.nom@spécialité.mssante.fr ou prenom.nom@pro.mssante.fr.

Les différentes spécialités disponibles sont listées ci-dessous :

- nom.prenom@masseur-kinesitherapeute.mssante.fr
- nom.prenom@medecin.mssante.fr
- nom.prenom@infirmier.mssante.fr
- nom.prenom@sage-femme.mssante.fr
- nom.prenom@chirurgien-dentiste.mssante.fr
- nom.prenom@pharmacien.mssante.fr

- nom.prenom@pedicure-podologue.mssante.fr

Après avoir créé un mot de passe, rentré une adresse mail de secours et son numéro de téléphone, le compte est enfin activé et peut être utilisé. Ce mot de passe sert à accéder à son compte si l'on n'a pas sa CPS à disposition.

On peut accéder à un annuaire de tous les professionnels de santé ayant une adresse mail sécurisée activée pour les contacter. L'État garantit donc l'authenticité de la personne contactée et le chiffrement des données de bout en bout.

Le mail sécurisé fourni par l'État est hébergé sur un hébergeur certifié HDS. Certaines officines possèdent un site internet avec de la vente en ligne, il faut donc que ce site soit hébergé sur un HDS.

5.1.9 Site internet et Hébergeur De Santé

Depuis plusieurs années, les pharmacies d'officine ouvrent leurs propres sites internet. Certaines ont seulement un site vitrine, sans vente en ligne, alors que d'autres ont intégré la vente en ligne de médicaments. Dans ce cas-là, il faut obligatoirement que le site soit hébergé sur un HDS.

L'officine peut soit créer son propre site soit demander à un prestataire qui lui fournit une offre avec un hébergement sur un HDS.

Tous les outils numériques disponibles en officine doivent obligatoirement être sécurisés afin d'éviter des problèmes avec les données de santé. Cependant, entre la théorie et la pratique, il y a une énorme différence. En effet, au quotidien, ces outils peuvent être mal utilisés.

5.2 Utilisations réelles de ces outils numériques

5.2.1 Analyse d'impact

L'analyse d'impact étant non obligatoire pour les professionnels de santé exceptée pour les grosses entreprises, il y a vraiment très peu d'officine ayant effectué cette analyse impact.

5.2.2 Anti-virus

Les différents antivirus disponibles sur le marché peuvent, suivant différents cas, détecter des faux positifs : un logiciel qui n'est pas un virus va être bloqué voire supprimé par l'antivirus. On constate ce comportement à chaque installation ou lors des différentes mises à jour des LGO. Pour éviter cela, la majorité du temps, les prestataires demandent la désactivation de l'antivirus pendant les mises à jour ou les installations. On constate souvent un manquement à la sécurité des données en officine, avec une désactivation pure et complète de l'antivirus afin d'éviter d'avoir à contacter l'assistance technique quand une mise à jour a lieu.

Donc, certaines officines paient un service qu'elles n'utilisent que partiellement et mettent en danger les données de leur patientèle sans aucune raison. Toutes les suites d'antivirus, dignes de ce nom, proposent des solutions pour éviter ce genre de problème. Communément appelée liste blanche et accessible par le biais de réglages, on peut y inscrire tous les fichiers que l'on veut exclure de l'analyse de l'antivirus. En officine, il faudrait donc mettre sur cette liste son LGO et les différents logiciels associés, comme les fichiers de mise à jour pour éviter tout problème. Cependant, cela constitue malgré tout une faille de sécurité, même si elle est de moindre mesure comparée à la désactivation pure et complète de l'antivirus.

Il suffirait, pour un individu mal intentionné, de récupérer le nom d'un fichier exclu pour ensuite renommer son virus par ce même nom et ainsi pouvoir infecter une officine. A moins que des personnes ne ciblent particulièrement des officines, ce qui est peu probable, il n'y a que très peu de risque.

5.2.3 Mises à jour des logiciels

Dans les entreprises, que cela soit des officines ou non, il y a une peur des mises à jour. En effet, on remarque que certains ne mettent pas à jour leur système d'exploitation ou ont peur d'avoir les logiciels qui ne fonctionnent plus et ainsi appeler un service technique qui peut parfois mettre du temps à réparer les différents postes. Sauf que certaines failles, comme Meldown et Spectre, permettent d'accéder à n'importe quelles données, et donc de mettre en péril des données patients. Il est donc préférable de perdre du temps avec un service technique plutôt que d'avoir des données-patients qui ont fuité et donc d'être jugé à la cour pénale à cause cette fuite de données.

En officine, ces pratiques sont courantes, comme le souligne la thèse du Dr BETTEGA, La sécurité informatique des données patients en officine[19]. Dans cette thèse, on remarque que seules 58% des officines interrogées étaient certaines d'avoir une version mise à jour de leurs systèmes d'exploitation, et 19% avaient un contrôle des mises à jour de tous leurs logiciels.

[19] BETTEGA, François, « La sécurité informatique des données patient en officine » (Université Granoble Alpes, 2018), https://dumas.ccsd.cnrs.fr/dumas-01922819/document.

5.2.4 Les mots de passe

On remarque que la mesure des mots de passe n'est pas souvent appliquée. Dans la majorité des cas, il n'y a pas de mot de passe session, ou encore le mot de passe est le nom du poste ou est écrit sur un papier collé sur l'ordinateur. Selon la thèse du Dr BETTEGA, seules 2,1% des officines avaient un mot de passe de session.

L'association code opérateur et mot de passe n'a guère plus d'adeptes : seulement 18% avaient un mot de passe assigné au code opérateur selon la même thèse.

Il reste aussi le chiffrement des sauvegardes, mais là encore, seuls 9% des sondés avaient une sauvegarde chiffrée de leurs serveurs.

Ces mesures sont simples à appliquer mais, on les retrouve peu dans les officines.

5.2.5 Cartes Professionnelle de Santé, de Personnel d'Établissement et Vitale

Les cartes professionnelles sont associées à des codes pour plus de sureté et pour éviter l'usurpation. Surtout qu'avec cette carte on peut s'identifier sur un site comme Mailiz et envoyer des mails à la place du professionnel de santé. Cependant, dans énormément d'officines, on trouve le code de la carte inscrit sur le lecteur ou sur le poste de travail associé à cette carte.

5.2.6 Séparation locale des réseaux

La séparation locale des réseaux ne sert pratiquement à rien dans des petites structures. Donc on ne retrouve pas ce type de configuration dans les petites officines. Ce genre de cloisonnement se retrouve par contre dans de très grandes officines ayant plusieurs unités différentes. Dans ces grandes structures, il faut obligatoirement une personne dédiée pour gérer le réseau s'il y a un nombre important de postes différents. Dans les moyennes structures, on peut employer une personne sachant gérer des réseaux mais qui ne sera pas forcément dédiée uniquement à cette tâche.

5.2.7 Messagerie sécurisée

La messagerie sécurisée étant gratuite, on aurait pu penser qu'il aurait énormément de demande dans les officines. Cependant, on constate que beaucoup d'officines utilisent encore des mails non sécurisés ou encore des fax. Selon la thèse du Dr BETTEGA, 74% des officines contactées utilisent des solutions de messagerie conventionnelles et 70% utilisent encore le fax.

Même s'il y a un écart entre la législation et la réalité, plusieurs choses peuvent être améliorées.

6 Pistes d'amélioration

Afin d'améliorer la sécurité informatique sur le terrain, diverses solutions sont envisageables.

Pour la première piste, les différentes instances devraient montrer l'exemple. En effet, elles devraient montrer qu'il y a des règles de sécurité des données à appliquer, comme par exemple, le fait d'avoir des systèmes à jour. On peut remarquer que la GIE SESAM-Vitale utilise toujours des certificats TLS en version 1.0, malgré le fait que cette norme a été créé en 1993 et qu'une version 1.3 est sortie en 2017. Comme les officines ne sont pas les seuls acteurs de la sécurité des données, il est nécessaire que des grandes instances françaises ou européennes puissent être en adéquation avec les nouveautés en termes de sécurité informatique. En effet, personne ne voudrait appliquer une recommandation ou même une loi si les grandes instances ne l'appliquent pas.

Une autre piste disponible envisageable est la loi. En effet, les lois actuelles étant assez vagues, certaines failles peuvent y persister. Certaines personnes peuvent utiliser ces failles pour contourner la loi. Il y a donc un flou législatif sur certains points comme le fax, pour traiter des ordonnances, qui n'est ni autorisé ni clairement interdit. De plus, on peut remarquer que les différentes instances de santé ne font que des recommandations ce qui est complètement différent d'une loi. Ces recommandations ne sont malheureusement que peu suivies puisqu'elles sont non obligatoires. Il faut imposer certains points afin que les mentalités puissent changer. On voit encore trop d'utilisations de mails classiques, de fax ou de mots de passe possiblement connus de tout le monde. Donc, si une loi était votée, avec écrits

noir sur blanc tous les interdits, cela en simplifierait la compréhension et cela serait donc plus facilement applicable.

On pourrait aussi beaucoup plus sensibiliser les pharmaciens et les préparateurs sur la sécurité des données surtout que l'on remarque un manque de connaissance vis-à-vis du monde de l'informatique. Le monde évolue, le numérique prend de plus en plus de place. Il faut donc sensibiliser dès le début, pendant les études, plus encore que ce qui est fait actuellement. Des cours obligatoires de sécurités de données en entreprise, simples et facilement compréhensibles par tout le monde pourraient être mis en place dans les écoles et les facultés. À la vue de la place prise par le numérique dans le quotidien, on peut même penser avoir des cours de confidentialité au collège et au lycée pour mieux sensibiliser la population et de potentiels futurs étudiants en pharmacie.

Les solutions fournies par les prestataires de LGO sont assez complètes, mais n'obligent pas à sécuriser entièrement les actes et les données, puisque c'est aux utilisateurs de définir ce qu'ils veulent. Ces prestataires ont un large éventail de logiciels allant de l'antivirus à la gestion de l'authentification par badge. Ils sont au service des officines, il est donc difficile d'imposer des solutions de sécurité. Cependant, s'ils obligeaient d'avoir au moins un mot de passe à chaque code opérateur, cela serait déjà une grande avancée.

Une autre possibilité serait d'imposer la certification ISO 9001 de façon progressive aux officines. L'élément principal de cette certification est l'amélioration continue. Donc même en partant de très bas, en s'améliorant, on peut arriver assez haut. Ce faisant, cette technique peut être appliqué au numérique surtout que cette certification inclut un volet sécurité informatique, ce qui permettrait donc de sécuriser un peu plus les officines. De plus, l'approche de

l'amélioration continue colle assez bien avec le numérique puisque ce dernier évolue très rapidement. Donc une amélioration continue de la sécurité des données au sein d'officines permettrait une sécurité beaucoup plus optimale des données.

On remarque que sans imposer cette sécurité, il n'y a que très peu d'actions concernant la sécurité numérique de la part des officines.

7 Conclusion

En quelques décennies la collecte de données officinales a fortement évolué avec l'arrivée de l'informatique dans les officines. En effet, l'arrivée de la Carte Vitale a engagé un tournant dans la collecte des données de la patientèle. Depuis cette innovation phare, l'officine doit gérer de plus en plus de données-patients. En effet, au fur et à mesure que les missions officinales évoluent, la quantité de données à traiter augmente. Ainsi, l'État ajoute de plus en plus de mesures afin garantir la sécurité des données, notamment depuis la prise de conscience collective de la vie privée informatique. Ce tournant a donc provoqué l'apparition de notion de protection des données.

Contrairement aux entreprises du numérique qui en ont pris conscience assez rapidement et aux grandes entreprises qui ont plus récemment pris conscience de la nécessité de protéger les données stockées, les officines ont quant à elles un peu plus de difficultés. Malgré la possibilité d'avoir des poursuites engagées en cas de fuite de données, les officinaux n'ont toujours pas pris conscience de l'importance de cette sécurité. Cependant, la mise en place du RGPD, a tout de même un peu fait réagir les officines, surtout celles qui disposent d'un site internet. Cependant, au final, la tempête s'est vite calmée. Même si la plupart des outils manipulés au quotidien sont des outils communs ou se rapprochent d'outils connus, leur réelle utilisation est souvent mal faite. Cela est dû au fait qu'un grand nombre de personne travaillant en officine ne possède pas toutes les compétences liées au numérique et sont pas ou peu informées des nouvelles évolutions du numérique.

En officine, le développement professionnel continu a été mis en place, suite à la création de nouvelles prises en charge, et provoque donc une évolution

constante du cœur du métier. Le numérique subit lui aussi une évolution constante, et cette évolution numérique va même plus vite que celle des traitements médicamenteux. Une formation continue du numérique officinale devrait être mise en place afin de comprendre l'intérêt de la sécurisation des données et de suivre l'évolution des différents outils disponibles en plus d'une formation initiale plus approfondie de la sécurité des données.

Même si l'informatique a de beaux jours devant elle, l'officine a encore un long chemin devant elle, avant d'enfin pouvoir garantir une sécurité des données d'une façon la plus optimale possible. Cependant, le numérique évoluant vraiment vite, il faut rattraper rapidement ce retard afin d'anticiper les futures techniques de vols de données. Ce faisant, l'enjeu de protection des données en officine serait enfin compris.

8 Bibliographie

1. Dourgnon P, Grignon M. Le tiers-payant est-il inflationniste ? CREDES; 2000 avr. Report No.: 490.

2. Le Dossier Pharmaceutique (DP) | CNIL [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.cnil.fr/fr/le-dossier-pharmaceutique-dp

3. Dossier médical partagé (DMP) : questions-réponses | CNIL [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.cnil.fr/fr/dossier-medical-partage-dmp-questions-reponses

4. Vente de médicaments sur Internet en France - Les patients - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Les-patients/Vente-de-medicaments-sur-Internet-en-France

5. La télémédecine [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://solidarites-sante.gouv.fr/soins-et-maladies/prises-en-charge-specialisees/telemedecine/article/la-telemedecine

6. HEALTH DATA HUB [Internet]. Disponible sur : https://drees.solidarites-sante.gouv.fr/IMG/pdf/hdh-aap.pdf

7. Respect de la confidentialité des données de patients dans l'usage de l'informatique - Recommandations de Janvier 2013 - Ordre National des Pharmaciens [Internet]. (page consultée le 11 janv 2020). Disponible sur : http://www.ordre.pharmacien.fr/Communications/Publications-ordinales/Respect-de-la-confidentialite-des-donnees-de-patients

8. Guitard E-H. Les serments professionnels de la pharmacie de l'antiquité à nos jours (suite et fin). Revue d'Histoire de la Pharmacie. 1947;35(117):122-32.

9. Code pénal [Internet]. Code pénal. Disponible sur : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719

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

11. Formulaire de demande d'intervention sur le compte d'accès au DMP [Internet]. Disponible sur : https://www.dmp.fr/documents/formulaire-demande-intervention

12. Hébergement des données de santé [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante

13. HDS Hébergeur de données de santé - AFNOR Certification [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://certification.afnor.org/numerique/certification-hds-hebergement-des-donnees-de-sante

14. MSSanté [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://mailiz.mssante.fr/ps/decouvrir

15. Les missions de la CNIL | CNIL [Internet]. (page consultée le 20 févr 2020). Disponible sur : https://www.cnil.fr/fr/les-missions-de-la-cnil

16. Outil PIA : téléchargez et installez le logiciel de la CNIL | CNIL [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

17. Certificats SSL/SMIME de l'agence du numérique en santé | Intégrateurs CPS [Internet]. (page consultée le 4 sept 2020). Disponible sur : https://integrateurs-cps.asipsante.fr/pages/Certificats-SSLSMIME-de-lASIP-Sant%C3%A9

18. Créer son compte MSSANTE [Internet]. Disponible sur : https://www.ameli.fr/sites/default/files/creer_sa_mss.pdf

19. BETTEGA, François. La sécurité informatique des données patient en officine [Internet]. Université Granoble Alpes; 2018. Disponible sur : https://dumas.ccsd.cnrs.fr/dumas-01922819/document

20. Dossier pharmaceutique : quels droits pour les personnes ? | CNIL [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.cnil.fr/fr/dossier-pharmaceutique-quels-droits-pour-les-personnes

21. Assemblée générale Health Data Hub. Convention constitutive plateforme des données de santé. 2019 nov.

22. Guide de la sécurité des données personnelles | CNIL [Internet]. (page consultée le 22 déc 2019). Disponible sur : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

23. CNIL. Guide pratique de sensibilisation au RGPD [Internet]. Disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf

24. Hackathon pharmacie | Congrès des pharmaciens [Internet]. (page consultée le 28 mars 2020). Disponible sur : http://www.congresdespharmaciens.org/actu-congres/hackathon-pharmacie

25. Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine. 2010-1229 oct 19, 2010.

26. Ce qu'il faut retenir pour se mettre en conformité avec le RGPD - Qui sommes nous - Ordre National des Pharmaciens [Internet]. (page consultée le 22 déc 2019). Disponible sur : http://www.ordre.pharmacien.fr/Qui-sommes-nous/Protection-

des-donnees-personnelles2/Ce-qu-il-faut-retenir-pour-se-mettre-en-conformite-avec-le-RGPD

27. Donnée sensible | CNIL [Internet]. (page consultée le 11 janv 2020). Disponible sur : https://www.cnil.fr/fr/definition/donnee-sensible

28. L'usage des données de santé dématérialisées conforté - Communications - Ordre National des Pharmaciens [Internet]. (page consultée le 22 déc 2019). Disponible sur : http://www.ordre.pharmacien.fr/Communications/Les-actualites/L-usage-des-donnees-de-sante-dematerialisees-conforte

29. Ordre national des pharmaciens. La messagerie sécurisée proposée par les Ordres de santé [Internet]. Disponible sur : http://www.ordre.pharmacien.fr/content/download/389731/1857426/version/1/file/MAILIZ_Publiredac.pdf

30. Arrêté du 28 novembre 2016 relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies d'officine, les pharmacies mutualistes et les pharmacies de secours minières, mentionnées à l'article L. 5121-5 du code de la santé publique.

31. Ordre national des pharmaciens. Bonnes pratiques de dispensation des médicaments. 9 mai 2018; Disponible sur : http://www.ordre.pharmacien.fr/content/download/307371/1558583/version/2/file/Bonnes+pratiques+de+dispensation-Vweb.pdf

32. Activité d'une pharmacie : que faire ? | Besoin d'aide | CNIL [Internet]. (page consultée le 22 déc 2019). Disponible sur : https://www.cnil.fr/cnil-direct/question/activite-dune-pharmacie-que-faire?visiteur=pro

33. Le RGPD : ce qu'il faut retenir ! - Communications - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Communications/Les-actualites/Le-RGPD-ce-qu-il-faut-retenir

34. Durand-Tornare F. 20 ans du label Villes Internet [Internet]. Cités en réseaux; Disponible sur : http://www.villes-internet.net/site/wp-content/uploads/2019/01/00-CER-2019-HD-1.pdf

35. Les apports du RGPD - Qui sommes nous - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Qui-sommes-nous/Protection-des-donnees-personnelles2/Les-apports-du-RGPD

36. BRISSET, Charles. Les logiciels de gestion d'officine : fonctionnalités et acteurs [Internet]. 2014. Disponible sur : http://nuxeo.edel.univ-poitiers.fr/nuxeo/site/esupversions/638717d0-d202-4dc0-acdb-d613454d559e

37. Les mesures mises en place par le CNOP pour se conformer au RGPD - Qui sommes nous - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Qui-sommes-nous/Protection-des-donnees-personnelles2/Les-mesures-mises-en-place-par-le-CNOP-pour-se-conformer-au-RGPD

38. Délibération de la Commission Nationale de l'Informatique et des Libertés. 2018-289 sept 12, 2018.

39. Directive 2011/62/UE du Parlement européen et du Conseil du 8 juin 2011 modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain, en ce qui concerne la prévention de l'introduction

dans la chaîne d'approvisionnement légale de médicaments falsifiés Texte présentant de l'intérêt pour l'EEE [Internet]. 174, 32011L0062 juill 1, 2011. Disponible sur : http://data.europa.eu/eli/dir/2011/62/oj/fr

40. Code de la santé publique [Internet]. Code de la santé publique. Disponible sur : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072665

41. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

42. Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique (Titre résultant de la décision du Conseil constitutionnel n° 2007-546 DC du 25 janvier 2007).

43. Messageries de santé : espace de confiance MSSanté [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://esante.gouv.fr/securite/messageries-de-sante-mssante

44. Décret n°91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 91-1051 oct 14, 1991.

45. Ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins - Article 8.

46. Ordonnance n° 2012-1427 du 19 décembre 2012 relative au renforcement de la sécurité de la chaîne d'approvisionnement des médicaments, à l'encadrement de la vente de médicaments sur internet et à la lutte contre la falsification de médicaments.

47. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [Internet]. 281, 31995L0046 nov 23, 1995. Disponible sur : http://data.europa.eu/eli/dir/1995/46/oj/fra

48. Pharmacies Norme simplifiée NS-052 | CNIL [Internet]. (page consultée le 22 déc 2019). Disponible sur : https://www.cnil.fr/fr/declaration/ns-052-pharmacies

49. Quelles obligations pour les titulaires d'officine ? - Qui sommes nous - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Qui-sommes-nous/Protection-des-donnees-personnelles2/Quelles-obligations-pour-les-titulaires-d-officine

50. Cuggia M, Polton D, Wainrib G, Combes S. Rapport Health Data Hub [Internet]. Disponible sur : https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf

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

52. Règlement intérieur de la plateforme des données de santé [Internet]. déc 2, 2019. Disponible sur : https://fee494fb-072e-49c6-a5ed-00cfc497e5db.filesusr.com/ugd/8b518a_5adc79af603d4cbbaf904cd2e7ecabcb.pdf

53. Ordre national des pharmaciens. Règles techniques applicables aux sites internet de commerce électronique de médicaments [Internet]. 2018. Disponible sur : http://www.ordre.pharmacien.fr/content/download/307372/1558586/version/2/file/Commerce+électronique+de+médicaments-Vweb.pdf

54. Certification des hébergeurs de données de santé [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante

55. RGPD et professionnels de santé libéraux : ce que vous devez savoir | CNIL [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir

56. Se prémunir des pratiques abusives « Mise en conformité RGPD » avec la CNIL et la DGCCRF - Communications - Ordre National des Pharmaciens [Internet]. (page consultée le 21 mars 2020). Disponible sur : http://www.ordre.pharmacien.fr/Communications/Les-actualites/Se-premunir-des-pratiques-abusives-Mise-en-conformite-RGPD-avec-la-CNIL-et-la-DGCCRF

57. Téléexpertise [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.ameli.fr/medecin/exercice-liberal/telemedecine/teleexpertise

58. Télémédecine [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://esante.gouv.fr/projets-nationaux/telemedecine

59. Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé ».

60. DICOM_Lisa.C, DICOM_Lisa.C. Vente en ligne de médicaments [Internet]. Ministère des Solidarités et de la Santé. 2020 (page consultée le 21 mars 2020). Disponible sur : http://solidarites-sante.gouv.fr/soins-et-maladies/medicaments/le-bon-usage-des-medicaments/article/vente-en-ligne-de-medicaments

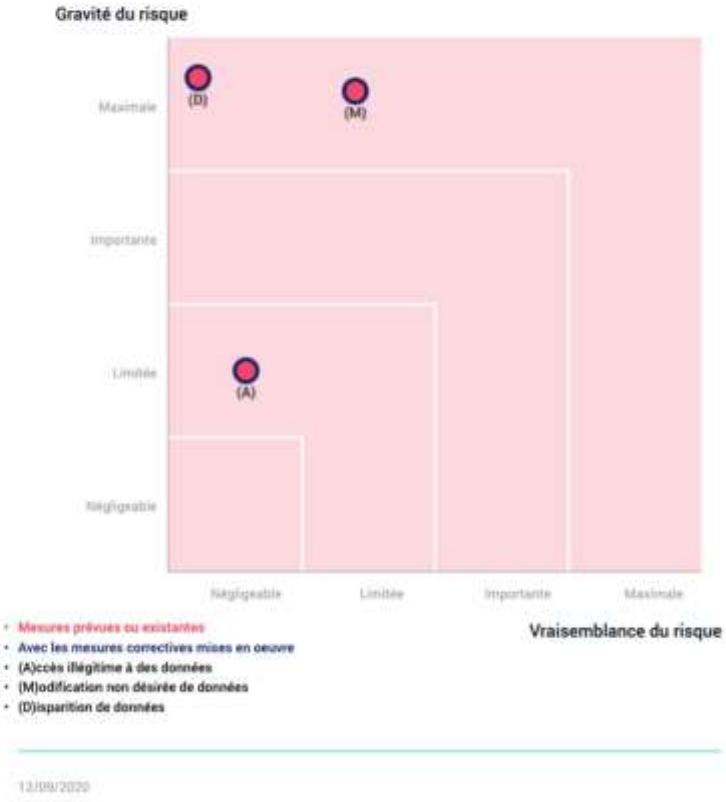
61. Vente en ligne de médicaments - ANSM : Agence nationale de sécurité du médicament et des produits de santé [Internet]. (page consultée le 21 mars 2020). Disponible sur : https://www.ansm.sante.fr/Activites/Vente-en-ligne-de-medicaments/Vente-en-ligne-de-medicaments/(offset)/0

9 Annexes

PIA :

Validation

Cartographie des risques



12/09/2020

Validation

Plan d'action

Vue d'ensemble

Principes fondamentaux

Recueil du consentement
Plan d'action / mesures correctives :
A affiche à la pharmacie
Commentaire d'évaluation :
même s'il n'y pas besoin du consentement, prévenir les patient c'est mieux

Sous-traitance
Plan d'action / mesures correctives :
demander une copie à pharmagest
Commentaire d'évaluation :
Un descriptif de tous ce que récupère pharmagest et accessible à tout le monde serait le bienvenu

Mesures existantes ou prévues

Sauvegarde des données
Plan d'action / mesures correctives :
chiffrement complet du NAS
Commentaire d'évaluation :
Sauvegarde sur le NAS non chiffré correctement

Sécurité physique
Plan d'action / mesures correctives :
Mettre une armoire sous clefs pour les serveurs
Commentaire d'évaluation :
Les serveurs ne sont pas sous clef

Gérer les risques
Plan d'action / mesures correctives :
affilié une seconde personne pour vérifier les ordonnances
Commentaire d'évaluation :
seul 30% des ordonnances sont vérifiés à l'année

Risques

Aucun plan d'action enregistré.

Validation

Avis du DPD et des personnes concernées

Nom du DPD

Maxime VDOVYTSYA

Opinion du DPD

Les traitements sont légitimes, il y a une certaine protection mais à améliorer.

Recherche de l'avis des personnes concernées

L'avis des personnes concernées a été demandé.

Noms des personnes concernées

Maxime VDOVYTSYA

Statuts des personnes concernées

Le traitement pourrait être mis en œuvre.

Opinions des personnes concernées

La plupart des données collectés sont conservés de façon obligatoire, le traitement effectué est partiellement anonyme, on peut mettre en place ce traitement.

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

LGPI et **P-Dose** permettent de collecter différentes données (nom, prénom, médicaments vendus, médicaments produits en PDA, etc.)

Finalité :
- Voir quelles références sont les plus vendus, et les quelles sont les moins vendus
- Améliorer le stock de médicaments

Enjeux :
- Éviter la perte d'argent (médicaments non vendus périmés, trop de temps entre l'achat et la vente, etc.)

Quelles sont les responsabilités liées au traitement ?

Responsables : Pharmaciens associés
Sous-traitants : Pharmagest, Pill-dose
Co-responsable : VDOVYTSYA Maxime, Pharmacien

Quels sont les référentiels applicables ?

Aucun référentiel spécifique

Évaluation : Acceptable

Contexte

Données, processus et supports

Quelles sont les données traitées ?

Données collectées : conservé pendants 3 ans (sauf médicaments particuliers)

- Nom, prénom
- Numéro de sécurité social
- Médicaments vendus et la date de vente

Destinataires : Pharmaciens

Personnes pouvant y accéder : Pharmaciens, préparateurs

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Chaque poste client envoie les différentes données sur 2 serveurs locales : 1 de pharamagest (pour LGPI) et 1 de P-Dose

Quels sont les supports des données ?

Postes client : pc sous windows 7 ou 10, logiciel LGPI et P-Dose

Serveurs :

- Pharmagest : sous linux
- P-Dose : sous windows 10

Papiers : liste des médicaments à commander chaque mois

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les données collectées permettent de fournir la liste du stock nécessaire en officine pour la PDA et le comptoir.
Elle permet :

- aux patients de ne pas revenir en officine une seconde fois pour leurs ordonnances (prévision des médicaments vendus)
- pour la PDA : production sans interruption du robot de production de piluliers

Évaluation : Acceptable

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Le traitement est nécessaire à une obligation légale et est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie.
Les contrats sont signées entre les EHPADs ou FAM et l'officine, et entre les patients et les EHPAD ou FAM.

Évaluation : Acceptable

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

- **Nom, prénom, numéro de sécurité social** : obligation légale vis à vis de l'état
- **Médicaments vendus** : obligation légale
- **Date de vente** : obligation légale

Seuls les médicaments vendus et leurs dates de ventes sont exploités pour établir la liste à commander

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les données sont fournies par la carte vitale, établit par les caisses d'assurances maladies qui garantissent les données y figurant (pouvant être confirmé par le numéro de sécurité social sur le site d'ameli)

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Obligation légale de conserver les données pour une délivrance de stupéfiants et de médicaments sous liste I et II et de médicaments d'exception de 3 ans

Évaluation : Acceptable

Principes fondamentaux

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

A la demande du patient, les pharmaciens et les préparateurs informent les patients des traitements subis à leurs données

Évaluation : Acceptable
Commentaire d'évaluation :
Affiche à installer dans la pharmacie pour informer les patients
Prévenir les patients sans qu'ils le demandent

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Il n'y a pas besoin de recueillir le consentement des patients pour collecter et conserver les données de santé dans la mesure où leurs collectes et leurs conservations sont nécessaires à la prise en charge du patient.

Évaluation : Améliorable
Plan d'action / mesures correctives :
A affiche à la pharmacie
Commentaire d'évaluation :
même s'il n'y pas besoin du consentement, prévenir les patients c'est mieux

Comment les personnes concernées peuvent-elles exercer leurs droits d'accès et droit à la portabilité ?

Sur simple demande à l'équipe officinale, les patients ont accès à leurs données et peuvent demander une copie papier

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droits de rectification et droit à l'effacement (droit à l'oubli) ?

Sur simple demande à l'équipe officinale, les patients peuvent rectifier leur dossier. L'effacement des données ne peut s'effectuer que si les délais légales de conservations sont dépassés

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droits de limitation et droit d'opposition ?

Conformément à la loi, les patients ne peuvent exercer leurs droits de limitation et d'opposition parce qu'il y a une conservation légale de ces données pendant un durée légale. Seul le traitement effectué peut subir les droits de limitation et d'opposition sur simple demande à l'équipe officinale

Évaluation : Acceptable
Commentaire d'évaluation :
Il faudrait informer les patients que ces droits-là ne peuvent être exercer

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Pharmagest possède une certification fournit par l'état pour l'hébergement des données de santé et leurs traitements le cas échéants.

Évaluation : Améliorable
Plan d'action / mesures correctives :
demander une copie à pharmagest
Commentaire d'évaluation :
Un descriptif de tous ce que récupère pharmagest et accessible à tout le monde serait le bienvenu

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Il ne peut y avoir transfert de données de santé en dehors de l'Union européen sont dans le cas de demande par un autre professionnel de santé. Dans ce cas, il faut une identification claire du professionnel de santé. Les données sont transmises aux patients ou au professionnel de santé sous forme de papier ou support numérique physique.

Évaluation : Acceptable

Risques

Mesures existantes ou prévues

Chiffrement

Les données sont récoltés par le biais de carte vitale ne pouvant être lues qu'avec la présence d'une carte CPS ou CPE, les échanges se font grâce à un certificat SSL (établit par l'état) et grâce à un certificat S/MIME pour l'échange d'objet.
Une bi-clé RSA est généré à chaque demande de 1024bits

Évaluation : Acceptable

Anonymisation

Non applicable

Évaluation : Acceptable

Cloisonnement

Chaque patient possède son propre dossier, accessible qu'avec son nom.

Évaluation : Acceptable

Contrôle des accès logiques

L'accès aux données ne se fait que grâce au mot de passe unique à chaque opérateur. Aucune personne de l'extérieur ne peut y accéder sans un mot de passe

Évaluation : Acceptable

Journalisation

Chaque modification de données est inscrite dans les registres avec le code de l'opérateur

Évaluation : Acceptable

Archivage

Les données sont conservées pendant le temps légale demandé par l'état et l'ordre des pharmaciens.

Évaluation : Acceptable

Sécurisation des documents papier

Toutes données imprimées non utilisées est broyer avant d'être jeter.

Évaluation : Acceptable

Minimisation des données

Les données minimales à avoir : nom, prénom, n° de sécurité social, adresse et n° de téléphone du patient, et nom et n° ameli du prescripteurs.

Évaluation : Acceptable

Sécurisation de l'exploitation

La maintenance des serveurs est couverte par un contrat établit entre l'officine et Pharmagest.

Évaluation : Acceptable

Lutte contre les logiciels malveillants

- Antivirus sur chaque poste client
- Sécurité des serveurs couverte par le contrat entre l'officine et pharmagest

Évaluation : Acceptable

Gestion des postes de travail

- Antivirus sur chaque poste
- Mot de passe session sur chaque poste
- Pare-feu numérique général

Évaluation : Acceptable

Protection des sites web

- La protection des sites web est couvert par le contrat entre l'officine et Pharmagest
- La sécurisation des données se fait par le biais d'une carte vital et d'une carte CPS ou CPE

Évaluation : Acceptable

Sauvegarde des données

- Sauvegarde du serveur LGPI effectué par Pharmagest
- Sauvegarde du serveur P-Dose sur Nas

Évaluation : Améliorable
Plan d'action / mesures correctives :
chiffrement complet du NAS
Commentaire d'évaluation :
Sauvegarde sur le NAS non chiffré correctement

Maintenance

La maintenance des serveurs est couverte par le contrat entre l'officine et Pharmagest.

Évaluation : Acceptable

Contrat de sous-traitance

Le seul sous-traitants est Pharmagest, autorisé par l'état + certification HDS.

Évaluation : Acceptable

Sécurisation des canaux informatiques

- Communication avec les serveurs des assurances maladies et complémentaires à l'aide d'Offisecure fournit par Pharmagest
- Wi-Fi avec mot de passe fort

Évaluation : Acceptable

Sécurité physique

Les portes d'entrée sont sou clefs et une alarme est installée

Évaluation : Améliorable
Plan d'action / mesures correctives :
Mettre une armoire sous clefs pour les serveurs
Commentaire d'évaluation :
Les serveurs ne sont pas sous clef

Traçabilité

Un journal des dysfonctionnements est mis en place et accessible sur chaque poste client.

Évaluation : Acceptable

Gérer les risques

- Double vérification d'ordonnance mise en place à l'officine

Évaluation : Améliorable
Plan d'action / mesures correctives :
affilié une seconde personne pour vérifier les ordonnances
Commentaire d'évaluation :
seul 30% des ordonnances sont vérifiés à l'année

Risques

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Communication des données sensibles (données de santé)

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Usurpation du code opérateur permettant d'avoir un accès aux données

Quelles sources de risques pourraient-elles en être à l'origine ?

Employé(s), Malfaiteur(s)

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Sécurité physique, Contrôle des accès logiques, Lutte contre les logiciels malveillants, Sécurisation de l'exploitation, Gestion des postes de travail, Journalisation, Sécurisation des documents papier, Sécurisation des canaux informatiques, Protection des sites web

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée, Pour accéder aux données, il faut obligatoirement le mot de passe du serveur, le mot de passe du pc client et un code opérateur.
Un passage par internet est possible mais négligeable

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Il faut avoir les 3 mot de passes pour pouvoir avoir les données.

Évaluation : Acceptable

Risques

Modifications non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Mauvais traitement dispensé

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Usurpation du code opérateur permettant d'avoir un accès aux données, Mauvaise entrée de médicaments par l'opérateur

Quelles sources de risques pourraient-elles en être à l'origine ?

Employé(s), Malfaiteur(s)

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Gérer les risques

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Maximale, La délivrance d'un mauvais traitement impact les données mais en plus la vie du patient (peut amener à son décès)

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, Les risques sont limités dû à la double vérification des ordonnances

Évaluation : Acceptable

Risques

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Perte des listes de médication à produire en PDA, avec possibilité de ne pas avoir le bon traitement pour la bonne personne

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Crash du serveur avec perte de données, Suppression intentionnelle

Quelles sources de risques pourraient-elles en être à l'origine ?

Sources physiques (alimentation électrique, problème de pc, ...), Employé(s)

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Journalisation, Archivage, Maintenance, Sécurisation de l'exploitation, Sécurité physique, Sauvegarde des données, Lutte contre les logiciels malveillants

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Maximale, La perte de la liste des médicaments du patient peut engendrer la perte de son traitement donc conduisant à son décès

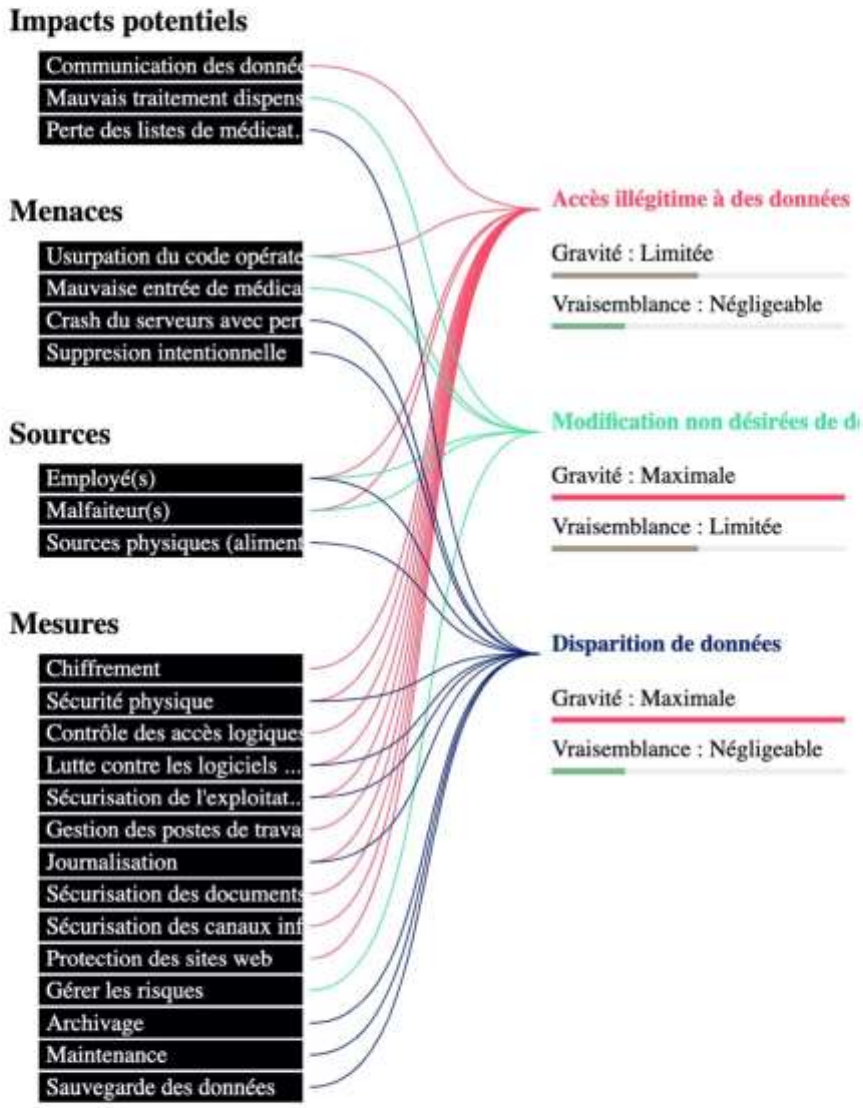
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Il y a plusieurs logiciels qui contiennent la liste des médications. Donc si l'un deux a ses données supprimées, on peut récupérer tout ou une partie de ses données sur un autre logiciel (ex : si perte sur P-Dose, on peut retranscrire les ordonnances depuis LGPI). De plus une sauvegarde quotidienne des données est effectuée sur les différents serveurs.

Évaluation : Acceptable

Risques

Vue d'ensemble des risques



Titre : Organisation du réseau informatique a l'officine : enjeu de la protection des données patients

Résumé :

L'avènement de l'ère informatique a bouleversé le comportement et le quotidien des officines. Après plusieurs décennies, l'informatique est enfin ancrée dans les officines, devenant un outil quasi obligatoire pour exercer correctement le métier de pharmacien. La sécurité du métier étant primordiale, des questions se sont posées concernant l'informatique à l'officine.

Cette thèse a pour but d'explorer la sécurité informatique à l'officine. Elle liste les divers textes de loi encadrant l'informatique à l'officine et la sécurité des données. Ensuite, les différents réseaux disponibles au niveau domestique, des entreprises et des officines sont décrits. Puis, la sécurité des données y est abordée, avec une liste de différents outils disponibles pour les officines et leurs utilisations quotidiennes.

Pour finir, une discussion conclue cet ouvrage.

Mots clés : Informatique, officine, sécurité, données de santé

Title : Organization of computer network in pharmacies : patient data protection issue

Abstract :

The advent of the computer age has changed the behavior and daily life of pharmacies. After several decades, computers are finally implented in pharmacies, becoming an important tool to properly practice the profession of pharmacist. Safety of the profession is important, computers in the pharmacy asked questions about his safety.

This thesis aims to explore computer security in the pharmacy. It lists the various pieces of legislation governing pharmacy computing and data security. Then, the various networks available at domestic, companies and pharmacies level are described. Then, data security is discussed, with a list of different tools available for pharmacies and their daily uses.

Finally, a discussion concludes this work.

Keywords : Computer, pharmacy, security, health data
