La sécurité informatique des données patient en officine

François Bettega

AVERTISSEMENT

LIENS

UNIVERSITÉ GRENOBLE ALPES

UFR DE PHARMACIE DE GRENOBLE

Année : 2018 2019

LA SÉCURITÉ INFORMATIQUE DES DONNÉES PATIENT EN OFFICINE

THÈSE
PRÉSENTÉE POUR L'OBTENTION DU TITRE DE DOCTEUR EN PHARMACIE

DIPLÔME D'ÉTAT

François BETTEGA

[Données à caractère personnel]

THÈSE SOUTENUE PUBLIQUEMENT À LA FACULTÉ DE PHARMACIE DE GRENOBLE

Le : 12/11/2018

DEVANT LE JURY COMPOSÉ DE

Président du jury :

Pr. Pascal Mossuz (directeur de thèse)

Membres :

Pr. Pierrick Bedouch

Dr. Christian Lenne

Dr. Béatrice Bellet

Dr. Sébastien Chanoine

UFR de Pharmacie

UNIVERSITÉ Grenoble Alpes

Doyen de la Faculté : **M. le Pr. Michel SEVE**

Vice-doyen et Directrice des Etudes : **Mme Christine DEMEILLIERS**

Année 2017-2018

ENSEIGNANTS -CHERCHEURS

STATUT	NOM	PRENOM	LABORATOIRE
MCF	ALDEBERT	DELPHINE	LAPM-UMR CNRS 5163
PU-PH	ALLENET	BENOIT	THEMAS TIMC-IMAG UMR CNRS 5525
PU	BAKRI	ABDELAZIZ	TIMC-IMAG CNRS UMR 5525
MAST	BARDET	JEAN-DIDIER	-
MCF	BATANDIER	CECILE	LBFA – INSERM U1055
PU-PH	BEDOUCH	PIERRICK	THEMAS TIMC-IMAG – UMR CNRS 5525
MCF	BELAIDI-CORSAT	ELISE	HP2 – INSERM U1042
MAST	BELLET	BEATRICE	-
MCF	BOUCHERLE	BENJAMIN	DPM
DCE	BOULADE	MARINE	SyMMES
PU	BOUMENDJEL	AHCENE	DPM – UMR 5063 CNRS
MCF	BOURGOIN	SANDRINE	IAB – CRI INSERM U823
DCE	BOUVET	RAPHAEL	HP2
MCF	BRETON	JEAN	LCIB – UMR E3 CEA
MCF	BRIANCON-MARJOLLET	ANNE	HP2 – INSERM U1042
PU	BURMEISTER	WILHEM	UVHCI- UMI 3265 EMBL CNRS
MCU-PH	BUSSER	BENOIT	IAB – CRI INSERM U823
MCF	CAVAILLES	PIERRE	LAPM – UMR 5163 CNRS
AHU	CHANOINE	SEBASTIEN	THEMAS TIMC-IMAG UMR CNRS 5525
MCF	CHOISNARD	LUC	DPM – UMR 5063 CNRS
AHU	CHOVELON	BENOIT	DPM – UMR 5063 CNRS
PU-PH	CORNET	MURIEL	THEREX TIMC-IMAG UMR 5525 CNRS
DCE	COUCHET	MORGANE	LBFA
Professeur Emérite	DANEL	VINCENT	-
PU	DECOUT	JEAN-LUC	DPM UMR 5063 CNRS
MCF	DEMEILLERS	CHRISTINE	TIMC-IMAG INSERM U1055
PU-PH	DROUET	CHRISTIAN	GREPI
PU	DROUET	EMMANUEL	UVHCI UMI 3265 EMBL CNRS
MCF	DURMORT	CLAIRE	IBS – UMR 5075 CEA CNRS
PU-PH	FAURE	PATRICE	HP2 – INSERM U1042
MCF	FAURE-JOYEUX	MARIE	HP2- INSERM U1042
PRCE	FITE	ANDREE	-

Mise à jour le 09/01/2018

STATUT	NOM	PRENOM	LABORATOIRE
AHU	GARNAUD	CECILE	THEREX TIMC-IMAG UMR 5525 CNRS
PRAG	GAUCHARD	PIERRE-ALEXIS	-
MCU-PH	GERMI	RAPHAELE	IBP-IBS UMI 3265 EMBL-CNRS
MCF	GEZE	ANNABELLE	DPM – UMR 5063 CNRS
MCF	GILLY	CATHERINE	DPM – UMR 5063 CNRS
PU	GODIN-RIBUOT	DIANE	HP2 INSERM U1042
Professeure Emérite	GRILLOT	Renée	-
MCF	GROSSET	CATHERINE	DPM UMR 5063 CNRS
MCF	GUIEU	VALERIE	DPM UMR 5063 CNRS
AHU	HENNEBIQUE	AURELIE	TIMC-IMAG
MCF	HININGER-FAVIER	ISABELLE	LBFA
MCF	KHALEF	NAWEL	TIMC-IMAG CNRS UMR 5525
MCF	KRIVOBOC	SERGE	LCBM IRTSV CEA
DCE	LE	CONG ANH KHANH	CERMA V
PU	LENORMAND	JEAN-LUC	THEREX TIMC-IMAG
PU	MARTIN	DONALD	TIMC-IMAG UMR 5525 CNRS
PRCE	MATTHYS	LAURENCE	-
AHU	MAZET	ROSELINE	DPM – UMR 5063 CNRS
MCF	MELO DI LIMA	CHRISTELLE	LECA – UMR CNRS 5553
AHU	MINOVES	MELANIE	
PU	MOINARD	CHRISTOPHE	BFA INSERM U1055
DCE	MONTEMAGNO	CHRISTOPHER	LRB
DCE	MOULIN	SOPHIE	HP2
PU-PH	MOSSUZ	PASCAL	
MCF	MOUHAMADOU	BELLO	LECA – UMR CNRS 5553
MCF	NICOLLE	EDWIGE	DPM – UMR 5063 CNRS
MCF	OUKACINE	FARID	DPM – UMR 5063 CNRS
MCF	PERES	BASILE	DPM – UMR 5063 CNRS
MCF	PEUCHMAUR	MARINE	DPM – UMR 5063 CNRS
PU	PEYRIN	ERIC	DPM – UMR 5063 CNRS
AHU	PLUCHART	HELENE	
MCF	RACHIDI	WALID	LCIB – UMR E3 CEA
MCF	RAVELET	CORINNE	DPM – UMR 5063 CNRS
PU	RIBUOT	CHRISTOPHE	HP2 – INSERM U1042
PAST	RIEU	ISABELLE	-
Professeure Emérite	ROUSSEL	ANNE-MARIE	-
PU-PH	SEVE	MICHEL	IAB-CR INSERM – U823 IAB
MCF	SOUARD	FLORENCE	DPM – UMR 5063 CNRS
MCF	SPANO	MONIQUE	IBS – UMR 5075 CEA CNRS
DCE	TAHER	RALEB	IBS

Mise à jour le 09/01/2018

STATUT	NOM	PRENOM	LABORATOIRE
MCF	TARBOURIECH	NICOLAS	UVHCI – UMR 3265 EMBL CNRS
MCF	VANHAVERBEKE	CECILE	DPM – UMR 5063 CNRS
DCE	VERNET	CELINE	CRI-IAB
DCE	VRAGNIAU	CHARLES	UVHCI
PU	WOUESSIDDJEWE	DENIS	DPM – UMR 5063 CNRS

AHU : Assistant Hospitalo-Universitaire
ATER : Attachés Temporaires d'Enseignement et de Recherches
BCI : Biologie du Cancer et de l'Infection
CHU : Centre Hospitalier Universitaire
CIB : Centre d'Innovation en Biologie
CRI : Centre de Recherche INSERM
CNRS : Centre National de Recherche Scientifique
DCE : Doctorants Contractuels Enseignement
DPM : Département de Pharmacochimie Moléculaire et de Cognition et Ontogenèse »
HP2 : Hypoxie Physiopathologie Respiratoire et Cardiovasculaire
IAB : Institut Albert Bonniot,
IBS : Institut de Biologie Structurale
LAPM : Laboratoire Adaptation et Pathogenèse des Microorganismes
LBFA : Laboratoire Bioénergétique Fondamentale et Appliquée
LCBM : Laboratoire Chimie et Biologie des Métaux
LCIB : Laboratoire de Chimie Inorganique et Biologie
LECA : Laboratoire d'Ecologie Alpine
LR : Laboratoire des Radio pharmaceutiques
MAST : Maitre de Conférences Associé à Temps Partiel
MCF : Maitre de Conférences des Universités
MCU-PH : Maître de Conférences des Universités et Praticiens Hospitaliers
PAST : Professeur Associé à Temps Partiel
PRAG : Professeur Agrégé
PRCE : Professeur certifié affecté dans l'enseignement
PU : Professeur des Universités
PU-PH : Professeur des Universités et Praticiens Hospitaliers
SyMMES : Systèmes Moléculaires et nanoMatériaux pour l'Energie et la Santé
TIMC-IMAG : Laboratoire Technique de l'Imagerie, de la Modélisation
UMR: Unité Mixte de Recherche
UVHCI: Unit of Virus Host Cell Interactions

Mise à jour le 09/01/2018

Table des matières

Table des tableaux

Tables des figures

Remerciement

Pr. Pascal Mossuz directeur de thèse
Je vous remercie d'avoir accepté de m'encadrer et d'avoir accompagné la réalisation de ce travail

Aux Pr Pierrick Bedouch,Dr. Béatrice Bellet , Dr.Sébastien Chanoine et au Dr Christian Lenne d'avoir accepté d'être membre de mon jury et d'évaluer mon travail.

Au Docteur Jean-Luc Cracowski pour son aide et son avis éclairé dans l'élaboration du questionnaire.

A Nicolas Harrand pour nos intéressants débats sur la sécurité informatique et pour sa relecture éclairée.

A Tiffanie GUETAT pour avoir transmis mon questionnaire aux préparateurs en pharmacie

Ainsi qu'à tous les pharmaciens, préparateurs et étudiants ayant accepté de répondre à mon questionnaire

J'aimerais aussi remercier mes parents ainsi que toutes les personnes qui m'ont accompagné et supporté pendant la réalisation de ce travail.

1 Lexique

Adresse mac : au sein d'un réseau informatique, l'adresse MAC (Media Access Control) identifie de manière unique l'interface réseau de l'ordinateur. Cette unicité permet de garantir le bon routage des informations échangées entre deux ordinateurs. C'est un numéro stocké physiquement dans l'interface réseau de chaque ordinateur, unique au monde pour chaque interface réseau(1)

Attaque par « brute force » : attaque informatique qui consiste à tester successivement de nombreux mots de passe (2)

Cheval de Troie : un cheval de Troie, qui peut également transiter par courrier électronique, se comporte comme un programme de commande à distance : installé à l'insu de l'utilisateur, il se lance automatiquement au démarrage du système d'exploitation de l'ordinateur et pénètre ainsi dans la totalité du système – de la configuration au registre, en passant par les mots de passe –, dont il permet de prendre le contrôle à distance. Le code supplémentaire introduit dans un programme réputé sain se déroule lors de l'exécution du programme sain. Il peut par exemple recenser les fichiers d'un ordinateur, puis les effacer.

Chiffrement : système de protection informatique destiné à garantir l'intégrité et l'inviolabilité de données pendant leur transmission ou leur stockage. Les méthodes de sécurisation adoptées garantissent un niveau de confidentialité plus ou moins élevé et sont fondées sur l'emploi d'une ou deux clefs de cryptage sous la forme de suites de chiffres, utilisées lors de l'envoi et de la réception.(3)

Fork : fourche en français, logiciel développé en réutilisant le code source d'un logiciel existant. Pour développer une fourche, un programmeur doit disposer des droits de modification et de distribution du code source original. C'est pour cette raison que les fourches sont souvent produites dans le domaine des logiciels libres. (4)

Formater : mettre en forme un disque dur en vue de l'organisation de ses secteurs pour une utilisation par le système d'exploitation, le formatage efface toutes les informations contenues sur le disque. (5)

Horodatage : l'horodatage est un procédé utilisé pour attester de l'existence d'une donnée à un instant, ou de la date de réalisation d'un acte par voie électronique. qui permet d'assurer la traçabilité des accès et des modifications sur les données personnelles.

Logiciel freeware : un logiciel gratuit, gratuiciel ou freeware est un logiciel propriétaire distribué gratuitement sans toutefois conférer à l'utilisateur certaines libertés d'usage(6)

Logiciel libre : un logiciel libre est un logiciel distribué selon une licence libre et le définissant comme tel. Plus concrètement et de manière un peu simplifiée, un logiciel libre est un logiciel qui peut être utilisé, modifié et redistribué sans restriction par la personne à qui il a été distribué. Un tel logiciel est ainsi susceptible d'être soumis à étude, critique et correction. Cette caractéristique confère aux logiciels libres une certaine fiabilité et réactivité.(7)

Non-répudiation : la non-répudiation consiste à prouver qu'un message a bien été émis par son expéditeur ou reçu par son destinataire. Plus généralement, la non-répudiation consiste à garantir que l'auteur d'un message ou d'un document ne peut pas nier l'avoir écrit ou transmis(8).

Robustesse : la robustesse d'un mot de passe est sa capacité à résister à une attaque par « brute force ».

Système d'exploitation : un système d'exploitation (*Operating System* ou OS) est un ensemble de programmes spécialisés qui permet l'utilisation des ressources matérielles d'un ou plusieurs ordinateurs. Il assure le démarrage (*Boot*) de l'ordinateur et l'exécution des logiciels applicatifs. Il remplit deux fonctions majeures : d'une part, la gestion des ressources matérielles (la mémoire, le processeur et les périphériques), en répartissant leur utilisation entre les différents logiciels ; d'autre part, la fourniture de services aux applications, en offrant une interface de plus haut niveau que celle de la machine physique. Cette interface présente la vision d'une « machine virtuelle », fournissant un ensemble de fonctions de base (appels système) pour l'écriture des applications.(9)

Ordinateur « zombie » : les criminels distribuent des logiciels malveillants (également appelés programmes malveillants) capables de transformer votre ordinateur en « bot » (diminutif de robot), également appelé zombie. Le cas échéant, votre ordinateur peut réaliser des tâches automatisées sur internet sans que vous le sachiez.

En général, les criminels utilisent les zombies pour infecter un grand nombre d'ordinateurs. Ces ordinateurs forment un réseau de zombies, qui permet de

diffuser des messages indésirables, des virus, d'attaquer des ordinateurs et des serveurs et de commettre d'autres types de crime et de fraude. Si votre ordinateur entre dans un réseau de zombies, il risque d'une part de ralentir et vous pourriez aider des criminels sans le savoir.(10)

Pare-feu : un pare-feu est un logiciel dont l'objectif est de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent internet (une zone où la confiance est nulle) et au moins un réseau interne (une zone où la confiance est plus importante). Le pare-feu doit protéger contre plusieurs types de menaces : contre les intrusions sur l'ordinateur depuis l'internet, contre certains virus et certains vers (infection et propagation), contre l'effet de chevaux de Troie en stoppant l'envoi d'informations vers l'internet ou en privant un intrus de l'accès à un ordinateur par une porte dérobée. Il est configuré de telle manière à reconnaître les attaques et les repousser. Il isole ainsi les données non autorisées à circuler sur un réseau protégé et les fait disparaître. Il transmet simultanément des alertes à l'administrateur réseau l'informant des tentatives d'accès et des éventuelles failles de sécurité.(11)

Routeur : un routeur est un appareil capable de gérer un petit réseau comme le réseau de votre domicile et de distribuer une connexion internet à tous les ordinateurs de votre réseau domestique, soit par câble, soit sans-fil. Les "Box" comme la Freebox ou la Livebox intègrent déjà un routeur.(12)

Spam : courrier électronique non sollicité envoyé en grand nombre à des boîtes aux lettres électroniques ou à des forums, dans un but publicitaire ou commercial.(13)

Virus : instruction parasite ou suite d'instructions parasites introduite dans un programme informatique et susceptible d'entraîner diverses perturbations dans le fonctionnement de l'ordinateur. Les virus informatiques sont capables de résister à certaines tentatives de destruction en se dupliquant.(14)

Wifi : réseau local hertzien (sans fil) à haut débit destiné aux liaisons d'équipements informatiques dans un cadre domestique ou professionnel. (15)

WEP / WPA / WPS : ceux sont des mécanismes d'authentification utilisés afin d'identifier les utilisateurs du réseau de manière univoque et sûre, ainsi que des mécanismes cryptographiques mis en œuvre afin de protéger les communications sans-fil : i) le WEP, dont la clef (mot de passe d'accès) est cassable en moins d'une minute ; ii) le WPA2 particulièrement robuste ; iii) et le WPS qui simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple), mais réintroduit une vulnérabilité importante qui en réduit fortement le niveau de sécurité.(16)

Abréviation

ANSM : Agence Nationale de Sécurité du Médicament et des Produits de Santé

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

ASIP Santé : Agence Nationale des Systèmes d'Information Partagés de Santé

CERT-FR : Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

CIL : Correspondant Informatique et Libertés

CNIL : Commission Nationale de l'Informatique et des Libertés

CNAMTS : Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés

CPS : Carte de Professionnel de Santé

DM : Dossier Médical

DMP : Dossier Médical Partagé, avant 2015 c'était le Dossier Médical Personnel

DP : Dossier Pharmaceutique

DPO : Délégué à la Protection des Données (Data Protection Officer)

ESN : Entreprise de Services du Numérique (anciennement SSII)

FSE : Feuilles de Soins Electroniques

FSPF : Fédération des Syndicats Pharmaceutique de France

G29 : Groupe des "CNIL" européennes

InVS : Institut de Veille Sanitaire

LGO : Logiciel de Gestion d'Officine

MAC : Media Access Control

OS : Operating System (système d'exploitation)

PUI : Pharmacie à Usage Intérieur

RGPD : Règlement Général sur la Protection des Données

RPPS : Répertoire partagé des professionnels de santé

VPN : Virtual Protocol Network

WEP : Wired Equivalent Privacy

WPA : Wi-Fi Protected Access

WPS : Wi-Fi Protected Setup

2 Introduction

Depuis 20 ans, le monde de la santé, comme beaucoup d'autres, opère une transition du papier vers le numérique. Cette évolution progresse sous l'impulsion des pouvoirs publics et des utilisateurs parce qu'elle apporte de nombreux bénéfices en matière de stockage, de recherche et communication des informations. L'évolution se fait également sous la pression des « fournisseurs de solutions » commerciaux qui trouvent dans la santé un marché en pleine expansion.

Cette transformation conduit les professionnels de santé, comme la majorité de la population, à utiliser dans leur travail et leur vie privée des outils plus ou moins complexes et pas toujours bien maîtrisés. Ainsi, une très grande majorité des données de santé sont aujourd'hui sous forme numérique. Elles sont généralement stockées chez les divers professionnels de santé, qui ont la charge de leur protection. De par leur nature, ces informations qui concernent la vie privée des patients, doivent être soumis à des règles de confidentialité et de sécurité de haut niveau. Cependant la diversité des outils utilisés, la relative information/formation des professionnels sur les risques inhérents à l'utilisation des techniques d'information et de communication sont des éléments qui peuvent affecter ce niveau de protection. La divulgation éventuelle d'informations confidentielles relève de la seule responsabilité des professionnels de santé utilisateurs, qui n'ont pas toujours les outils et processus adaptés à ce niveau d'exigence. Par exemple, des médecins anglais utilisent, faute d'alternative sécurisée, une application mobile Snapchat, permettant l'affichage de message temporaire (quelques secondes à une minute), pour transmettre des demandes d'avis médicaux (17). Or Snapchat n'est pas un hébergeur de données de santé, de ce fait il n'a pas l'obligation de protéger ces données, ces médecins rendent donc les données de leur patient

vulnérables, à chaque utilisation de l'application.

Parmi les professionnels, les pharmaciens d'officine sont détenteurs d'informations particulièrement sensibles puisque directement informatives sur l'état de santé du patient, informations qui en cas de diffusion malhonnête seraient susceptibles d'avoir un impact sur la vie privée, professionnelle et sociétale des patients.

Dans ce contexte, mon travail s'est intéressé aux moyens mis en œuvre pour protéger les données de santé stockées en pharmacie d'officine.

Après avoir retracé l'historique, l'évolution du dossier patient et son encadrement législatif en France, nous décrirons les recommandations proposées pour assurer la confidentialité des données de santé. Un retour sur les pratiques de terrain est illustré par les résultats d'un questionnaire portant sur l'application des recommandations par les pharmaciens d'officine et leurs employés. Nous évoquerons pour finir les améliorations procédurales envisageables compte tenu des évolutions.

3 Cadre législatif et supports de l’information

3.1 Cadre législatif

3.1.1 Données personnelles

Le cadre législatif des données personnelles en santé est étroitement lié à la notion de vie privée puisque c’est elle qui définit le caractère personnel des données.

La vie privée est une notion juridique en constante évolution et sans cesse précisée par la jurisprudence. Elle inclut entre autres : le domicile, l'image, la voix, la grossesse, l'état de santé, la vie sentimentale, la correspondance.

Aujourd’hui, le droit à la vie privée est protégé au niveau international par l’article 12 de la déclaration universelle des droits de l’homme de 1948 : "Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

En Europe le droit à la vie privée relève de l’article 8 de la convention européenne des droits de l’homme du 4 novembre 1950 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ». Cet article prévoit donc que ce droit à la vie privée ne peut faire obstacle à la santé et donc aux soins. Les échanges d’informations

confidentielles sont parfaitement légaux entre professionnels de santé tant qu'ils sont nécessaires aux soins.

En droit français, les dispositions relatives à la vie privée sont composées de l'article 9 du Code civil français, issu de la loi du 17 juillet 1970 : « Chacun a droit au respect de sa vie privée » et les articles 226-1 et suivants du Code pénal, pour les peines prévues.

Le cadre de la vie privée et la protection des données revêtent aujourd'hui une importance capitale dans l'évolution des pratiques de communication. L'existence de réseaux informatiques, particulièrement internet, permet un transit presque instantané des informations. Il permet par exemple d'héberger des données dans un autre pays sans que cela soit une gêne pour leur consultation ou leur édition. De plus si des données personnelles venaient à être récupérées par une personne malveillante il est important qu'elle ne puisse pas en tirer profit légalement dans un autre pays, d'où la nécessité d'une protection nationale et internationale.

Le secret professionnel est un outil de protection de la vie privée des patients, c'est lui qui rend le pharmacien responsable de la protection de toutes les données qu'il recueille et héberge dans le cadre de son activité professionnelle. Il permet de solliciter l'aide d'une profession sans risquer que les informations confiées soient rendues publiques. Les pharmaciens sont soumis au secret professionnel encadré par l'article L1110-4 code santé publique modifié par l'ordonnance n°2017-31 du 12 janvier 2017 - art. 5 : « toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur

médicosocial ou social ou un établissement ou service social et médicosocial mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant. »

Ce cadre législatif montre que toutes les données de santé relèvent de la vie privée au regard de la loi. Il montre aussi que la très large majorité des données recueillies par le pharmacien d'officine comme l'adresse ou les liens de parenté relèvent aussi de la vie privée. Qu'elles soient conservées sous forme informatique ou non, qu'elles concernent un patient nominativement ou permettent de le reconnaître, elles relèvent de sa vie privée et leur protection est, en vertu du secret professionnel, sous la responsabilité du pharmacien les détenant.

3.1.2 Loi informatique et liberté

La France a été en 1978 le 3eme pays d'Europe après l'Allemagne en 1971 et la Suède en 1973 à se doter d'une loi « informatique et liberté » « Loi 78-17 du 6 janvier 1978 modifiée 31 janvier 2017, qui encadre l'utilisation des données numériques.

Dans l'article 1er elle affirme que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

Cette loi offre à chaque citoyen des droits vis-à-vis des données collectées le concernant et a créé un organisme la CNIL (Commission Nationale de

l'Informatique et des Libertés) ayant entre autres des missions d'information et de contrôle (annexe 1).

Ces droits peuvent être regroupés en 4 grands principes : un droit de regard, un droit d'opposition sauf obligation légale, un droit de correction et un droit de suppression ; respectivement les articles 39, 38 et 40 (annexe 2).

Chaque professionnel de santé, à partir du moment où il possède un fichier nominatif de ses patients, est un organisme de traitement de données. Il est responsable de la sécurité de ces informations et doit satisfaire aux demandes des patients. Les professionnels de santé sont en plus responsables du respect des volontés du patient lors du traitement de certaines bases de données nationales. Par exemple, ceux sont les pharmaciens qui ouvrent les dossiers patients (DP), mais ils doivent aussi effectuer les demandes de clôture en cas d'opposition du patient ou encore en permettre la consultation.

Pour le pharmacien, les données personnelles de santé sont donc des données critiques protégées par la loi et la déontologie puisqu'il est organisme de traitement des données et soumis au secret professionnel. Leur protection est sous la responsabilité de chaque professionnel et engage leur responsabilité. Ces données sont en principe colligées dans un document spécifique et partagé entre professionnels : le dossier patient ou dossier médical. Lui aussi a fait l'objet d'évolutions en rapport avec les avancées technologiques.

La CNIL a rendu des avis sur de nombreux outils comme le DP (Dossier Pharmaceutique) ou le DMP (Dossier Médical Partagé) et a œuvré pour s'assurer que les droits fondamentaux des personnes à l'information, l'accès, la rectification/radiation, l'opposition et l'accès indirect soient respectés. De plus elle veille à ce que les délais de conservation des documents ne dépassent pas leur utilité.

La CNIL est un acteur du monde de la protection des données, mais ses moyens n'étant pas illimitée elle n'agit auprès de petites entreprises comme les pharmacies d'officine qu'en cas de plainte ou d'une demande de conseil. Le CIL (Correspondant Informatique et Libertés), nommé parmi les collaborateurs ou en dehors, facilite les échanges avec la CNIL. Il est chargé de conseiller et d'assurer l'application de la réglementation. Sa nomination est facultative, mais facilite les formalités de déclarations de traitement auprès de la CNIL. Il assure aussi en portant une attention particulière aux traitements effectués sur les données que ceux-ci ne portent pas atteinte à la vie privée.

Le RGPD (Règlement Général sur la Protection des Données) entré vigueur le 25 mai 2018 remplace le CIL (Correspondant Informatique et Libertés) par le DPO (Délégué à la Protection des Données) (18)

3.1.3 Règlement général sur la protection des données

Le RGPD, adopté par l'Union européenne le 14 avril 2016, vise à apporter un niveau élevé et cohérent de protection pour les données, il modifie substantiellement la réglementation en matière de protection des données à caractère personnel, dans l'Union européenne. Ce règlement s'applique à tous les pays membres et permet de diminuer les disparités entre règlements nationaux sur la protection des données. Il s'applique aussi aux entreprises non européennes traitant des données de citoyens européens (article 3). Ces premières modifications n'affectent pas directement les pharmacies d'officine, même si elles pourraient ouvrir des possibilités de délocalisation de leurs informations vers des hébergeurs de données de santé.

Le règlement prévoit aussi une notion de sécurité par défaut et la nécessité d'un consentement positif et explicite aux stockages des données patients. Mais ces

nouvelles notions ne devraient pas modifier les pratiques en officine où elles devraient déjà être mises en œuvre compte tenu de la nature sensible des données recueillies.

Le RGPD crée un nouveau droit à la portabilité, il permet à un citoyen de demander le transfert dans un format structuré et couramment utilisé, des données personnelles le concernant à lui-même ou à un autre organisme responsable du traitement. Cette nouvelle réglementation, si elle est couramment appliquée, pourrait conduire à des difficultés en officines : la portabilité des données d'un LGO (Logiciel de Gestion d'Officine) à un autre n'étant pas une opération courante.

Le règlement impose également une obligation de notifications en cas de fuite des données à l'autorité nationale de protection (article 33). Ce point est particulièrement important, car il devrait conduire tous les organismes dont les manquements en matière de sécurité informatique ont conduit à compromettre des données confidentielles, à être repérés et déclarés. Ceci devrait participer à un processus global de sensibilisation sur l'importance de bien garantir la sécurité des données.

Enfin, ce règlement introduit la possibilité de nommer un DPO dans les pharmacies d'officine. L'article 39 prévoit les missions que le DPO devra remplir à minima :

«a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données,

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la

répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;

d) coopérer avec l'autorité de contrôle ;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet. »

La CNIL à la demande de la Fédération des Syndicats Pharmaceutiques de France (FSPF) a confirmé qu'il n'y avait aucune obligation à nommer un DPO en pharmacie d'officine car même si elles traitent des données sensibles, ce traitement n'est pas à grande échelle(19). Cependant il y a un intérêt à nommer un DPO en pharmacie d'officine étant donnée la nature sensible des données stockées et la plus-value qu'il peut apporter en matière de sécurité informatique.

3.1.4 Certification des hébergeurs de données de santé

Pour garantir une sécurité maximum aux données de santé les plus vulnérables, c'est-à-dire celles accessibles à distance, le gouvernement français exige la certification des hébergeurs de données de santé. Ils doivent passer un audit documentaire réalisé par l'ASIP santé (Agence Nationale des Systèmes d'Information Partagés de Santé) et la CNIL. Au premier janvier 2019 de nouvelles contraintes viendront s'ajouter à cette certification, une évaluation de conformité technique et organisationnelle réalisée sur place ainsi que les exigences de la norme ISO 27001 « système de gestion de la sécurité des systèmes

d'information », ISO 20000 « système de gestion de la qualité des services », ISO 27018 « protection des données à caractère personnel » ainsi que des exigences spécifiques à l'hébergement de données de santé. Deux certificats différents seront délivrés selon que l'organisme assure l'hébergement d'infrastructure physique ou des prestations d'hébergeur infogéreur. Ce certificat sera délivré pour une durée de 3 ans, avec un audit de « surveillance » annuelle. Ce changement permettra d'apporter une reconnaissance internationale à cette certification.

Pour une pharmacie d'officine cela signifie qu'il n'est possible de stocker des données de santé à distance que chez un hébergeur de donnée de santé certifié dont la liste est publique [1]. Il est également important de vérifier que cet agrément est obtenu par l'hébergeur du site internet de vente en ligne des médicaments. Un exemple de données stockées à distance en pharmacie est le DP, qui est chez un hébergeur agréé.

3.2 Supports et sécurité

Nous allons nous intéresser aux différents supports utilisés au cours de l'histoire pour conserver les informations relatives à la prise en charge des patients en évoquant l'impact du choix du support sur les mesures à mettre en œuvre pour garantir la confidentialité.

Nous devons traiter la problématique en utilisant l'histoire du dossier médical, parce que le dossier pharmaceutique et les informations détenues par les pharmaciens actuellement n'ont pas d'équivalents historiques, leur apparition étant relativement récente, mais elles sont les descendantes du dossier médical.

---

[1] http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

3.2.1 De l’oral au papier

Historiquement les échanges entre patient et professionnel de santé étaient oraux et le suivi du patient reposait sur la mémoire du praticien. La nature de cet « archivage » conditionnait la confidentialité des échanges à la seule éthique du praticien, mais assurait une protection contre la négligence : ils ne pouvaient être égarés ou volés et ne pouvaient être divulgués sans une action expresse du dépositaire, ou sous la contrainte...

Des traces de recueils écrits répertoriant certains cas intéressants et leur prise en charge apparaissent à partir du 9e siècle. Ces recueils étaient constitués par des médecins arabes. Ils sont plus proches de nos actuels « cas cliniques » que du dossier médical personnel proprement dit.

Au 18e siècle, à l’hôtel-Dieu à Paris, un registre est créé pour répertorier des informations propres à chaque patient, mais son contenu reste succinct. En ville, l’oralité reste le mode dominant de transmission des données de santé.

Le passage de l’oralité au papier a été lent, car il nécessitait des évolutions technologiques impliquant une diminution du coût du papier. Le choix de l’écrit se fait, car il est un support plus fiable que la mémoire humaine et il facilite classement et transmission des informations. Il est plus facile d’envoyer un dossier que de se déplacer pour parler d’un patient à un confrère. De plus dans de grandes structures accueillant de nombreux patients, l’écrit permet à chaque médecin participant à la prise en charge d’être au courant des éléments majeurs de celle-ci.

À partir de la deuxième moitié du 20e siècle, le dossier médical commence à être encadré par des textes de loi. La réglementation impose un premier modèle de dossier médical par l’arrêté du 24 juin 1970.

Le décret du 30 mars 1992 (20) définit la composition du DM (Dossier Médical) hospitalier : il contient les informations nécessaires à l'identification du patient, les actes réalisés et les conclusions des professionnels de santé. On y intègre aussi le dossier de soins infirmiers. Cette réglementation représente le premier pas vers la fusion des dossiers patients détenus par les différents professionnels de santé.

Il faudra attendre 1995 pour offrir un cadre réglementaire au dossier médical en ville et rendre sa tenue obligatoire. L'article 45 du code de déontologie médicale précise : « Indépendamment du dossier de suivi médical prévu par la loi, le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques. Dans tous les cas, ces documents sont conservés sous la responsabilité du médecin. Tout médecin doit, à la demande du patient ou avec son consentement, transmettre aux médecins qui participent à sa prise en charge ou à ceux qu'il entend consulter, les informations et documents utiles à la continuité des soins. »

L'article 45 du code de déontologie rend aussi le médecin responsable de la conservation du dossier médical.

Aujourd'hui le DM et son accès sont encadrés par les articles L1111-7, L1111-8 et L1112-1 du code de la santé publique. En particulier il donne aux patients un droit de regard sur les informations recueillies dans l'article L1111-7 **« T**oute personne a accès à l'ensemble des informations concernant sa santé détenue par des professionnels et établissements de santé, qui sont formalisés et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment des résultats d'examens, comptes rendus de consultations, d'interventions, d'explorations ou d'hospitalisations, des protocoles et prescriptions thérapeutiques

mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers. »

Le dossier médical étant devenu une archive précise et obligatoire des différents événements de santé au cours de la vie d'une personne, il est aussi devenu un outil d'information. La loi autorise tout patient à accéder directement aux informations le concernant détenues par un professionnel de santé. Comme nous le verrons dans le chapitre suivant ce principe a été appliqué largement au-delà du dossier médical, chaque personne ayant le droit d'accéder aux informations personnelles la concernant, peu importe par qui elles sont détenues, mais le dossier médical a été précurseur dans ce domaine.

Le choix du support informatique pour le dossier médical n'est pas imposé par la réglementation, mais l'informatisation massive de notre système de santé et les avantages offerts par le numérique en ont fait un support de choix pour le dossier médical.

3.2.2 Informatisation du système de santé

L'informatisation de notre système de santé a des raisons techniques : moins d'espace de stockage, une facilité de recherche par des algorithmes, une duplication et une édition des documents moins coûteuse, et enfin une capacité de transmission des documents instantanée et à moindre coût. Mais le moteur de cette informatisation a été avant tout un intérêt économique. À la fin des années 1970, l'idée de confier la saisie informatique des feuilles de soins à chaque professionnel

de santé permettait à la sécurité sociale de faire des économies. De plus l'informatisation limitait les erreurs liées au traitement manuel des feuilles de soin.

Le fil de cette informatisation peut être suivi via un de ces moteurs : la mise en place du réseau SESAM-Vitale. En 1983 est créé le Groupe d'intérêt économique de Système Electronique de Saisie de l'Assurance Maladie associé à la carte Vitale (GIE SESAM-Vitale). De nombreuses expérimentations sont lancées pour relever les défis tant techniques de la dématérialisation des feuilles de soins que pour tester ces méthodes d'application pratique. On ne citera ici qu'un petit nombre. L'idée d'une carte à puce de santé naît d'une expérimentation menée à Blois en 1986 alors qu'elle avait été imaginée dès 1983. Le concept était de proposer une carte à puce contenant leurs informations de santé aux jeunes enfants et aux femmes enceintes. Ces données comprenaient : antécédents, groupe sanguin, allergies et traitements. Le but de cette expérimentation était la prévention et le suivi des examens obligatoires au cours de la grossesse.

De 1992 à 1998 des cartes vitales ont été distribuées à de nombreux usagers, des terminaux pour les mises à jour ont été mis à disposition et des lecteurs de cartes ont été distribués à de nombreux professionnels de santé pour expérimenter une nouvelle organisation.

L'article 8 de l'ordonnance 96-345 du 24 avril 1996 officialise la dématérialisation des feuilles de soins. Cet article prévoit que « le 31 décembre 1998 au plus tard, les professionnels, organismes ou établissements dispensant des actes ou des prestations remboursables par l'assurance maladie et les organismes d'assurance maladie doivent être en mesure, chacun pour ce qui le concerne, d'émettre, de signer, de recevoir et de traiter des feuilles de soins électroniques ou documents assimilés conformes à la réglementation. À la même date, chaque professionnel concerné doit avoir reçu une carte électronique professionnelle (la carte CPS (Carte

de Professionnel de Santé)) mentionnée à l'article L. 161-33 du code de la sécurité sociale. Tout bénéficiaire de l'assurance maladie doit avoir reçu la carte électronique individuelle visée au I de l'article L. 161-31 du code de la sécurité sociale ou, par dérogation, figurer en qualité d'ayant droit sur la carte électronique d'un assuré. »

En réalité, à la suite de nombreux problèmes techniques et compte tenu du coût de l'informatisation de chaque professionnel de santé, un délai a été accordé jusqu'au premier juin 2000 notamment pour permettre aux pharmaciens de transmettre les feuilles de soins électroniques (FSE).

Avec l'informatisation, le codage des actes, des prestations et des pathologies sont devenus indispensables. Ce codage univoque, compréhensible par tous est propice à un traitement automatique des données.

La pharmacie n'y a pas échappé avec :

- l'arrêté du 31 décembre 1996 imposant et normalisant la présence d'un code-barre sur les boites de médicaments
- le décret du 13 mai 1997 dispensant le pharmacien de coller les vignettes sur les feuilles de soins si elles sont télétransmises. Cela permet de compléter les informations collectées par la sécurité sociale sur ses assurés ; le traitement manuel des vignettes ne permettait pas auparavant de connaître le traitement de l'assuré en dehors des contrôles.
- la circulaire CNAMTS (Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés) du 22/09/1997 relative au codage des médicaments remboursables

La mise en place de SESAM Vital a conduit à 2 points clefs pour l'informatisation du système de santé : i) doter chaque usager d'une carte à puce personnelle permettant de l'identifier et d'accéder à ses données personnelles et ii) obliger

chaque professionnel de santé à se doter de matériel informatique et de réseau. Cet équipement, même s'il était initialement installé pour la facturation, permet l'utilisation de l'informatique pour une multitude d'autres tâches telle que la gestion de stock en pharmacie.

La multitude de ces applications informatiques a également permis l'émergence de plusieurs outils permettant une meilleure prise en charge des patients, posant les bases conceptuelles de l'usage de l'intelligence artificielle (IA) dans la santé.

3.2.3 Dossier pharmaceutique

Le dossier pharmaceutique est une base de données accessible à distance créée par l'ordre des pharmaciens, pour les pharmaciens. C'est un excellent exemple des avancées que peut permettre l'informatique en matière de suivi thérapeutique.

« Le DP est né d'une évidence : mettre les technologies au service de la sécurité sanitaire des patients en donnant au pharmacien une vue globale des traitements pour améliorer les performances de son exercice. Il découle de l'inscription du dossier médical personnel (DMP) dans la loi du 13 août 2004, et d'une ambition de l'ensemble de la profession qui a eu la conviction qu'il fallait créer un dossier électronique adapté à l'exercice des pharmaciens : le dossier pharmaceutique était né. Le projet porté par l'ordre des pharmaciens en 2006 comprend tous les traitements délivrés au cours des 4 derniers mois qu'ils soient prescrits par le médecin ou conseillés par le pharmacien. La durée est étendue à 21 ans pour les vaccins et à 3 ans pour les médicaments biologiques. Ces objectifs sont : d'éviter les traitements redondants, de détecter les risques d'interaction médicamenteuse, de mieux coordonner les soins entre la ville et l'hôpital (depuis octobre 2012, les pharmaciens des pharmacies à usage intérieur (PUI) peuvent accéder au DP dans

les mêmes conditions que les pharmaciens d'officine), de contribuer au bon usage du médicament, d'améliorer la couverture vaccinale et de disposer de l'information la plus récente possible.

Le DP est aujourd'hui dans 99,9 % des officines soit 21916 pharmacies ce qui lui a permis de se développer comme un outil de communication entre l'ANSM, les laboratoires et les pharmacies d'officine grâce à plusieurs fonctionnalités : « DP-Alertes », « DP-Rappels », « DP-Rupture » ou « DP-Suivi sanitaire ». »(21)

Le DP représente un des premiers spécimens de dossier exclusivement informatisé et mobile avec ses usagers. Il a fait l'objet de nombreux débats pour assurer la confidentialité des données sans pour autant altérer son utilité pratique et son utilisation à des fins de recherche. Les patients, même s'ils en font rarement usage, ont un droit de regard et de contrôle sur chaque information présente dans leur DP et peuvent à tout moment choisir de le clore(22). Le droit à l'oubli est assuré par une procédure automatique de fermeture de tout DP inactifs depuis plus de 3 ans.

Le DP est une grande avancée dans l'application de l'informatique pour la sécurité des patients. Mais ce n'est pas un outil de communication interprofessionnelle, car il n'est utilisé que par les pharmaciens d'officine ou presque et il ne résoud pas la problématique des données redondantes ou incohérentes entre les différentes professions. Ce passage du dossier personnel au dossier partagé implique de nouvelles adaptations juridiques.

3.2.4 Fichier patients

En pharmacie la principale base de données de santé est le fichier des patients. Cette base de données regroupe et remplace peu à peu différents documents anciennement au format papier comme l'ordonnancier ou les registres permettant

la gestion de stock. Il est généralement automatiquement complété par le LGO à chaque opération. Il contient pour chaque patient : les nom, prénom, adresse, numéro de téléphone et un lien vers les autres affiliés du point de vue de la sécurité sociale. Il contient les informations nécessaires à la facturation : la durée et le type de droit lors de la dernière présentation de la carte vitale, la durée des droits de la complémentaire santé et souvent une copie numérisée de la carte de complémentaire en cours. De plus, il regroupe pour chaque patient l'historique de tous les médicaments et dispositifs médicaux délivrés dans la pharmacie. Si la délivrance est sur prescription il contient des duplicatas numérisés de chacune des ordonnances délivrées et un lien avec la base de données des médecins du LGO. Cette dernière contient pour chaque médecin ayant eu une ordonnance délivrée : les nom, prénom, spécialité, adresse et numéro RPPS. La protection de ce fichier est la problématique centrale de cette thèse, car contrairement au DP aucune mesure « publique » n'est proposée par défaut pour garantir sa sécurité et la conservation des informations pour une durée approprié, les mesures mises en place ne dépendant que du pharmacien d'officine et de son équipe.

3.2.5 Du dossier médical personnel vers le dossier médical partagé

Le projet d'un dossier médical personnel exhaustif suivant le patient dans ces déplacements et au cours de sa vie est envisagé depuis le début de l'informatisation du système de santé. Le DMP pourrait en assurant l'interopérabilité entre toutes les bases de données des différentes professions, régler les problèmes d'incohérence et de redondance des informations.

La loi no 2004-810 du 13 août 2004 relative à l'assurance maladie initie réellement le projet. Après une première expérimentation en 2006 le dossier médical personnel est mis en suspens. Il sera relancé en 2008, mais ne sera réellement déployé qu'à partir de décembre 2010 et les patients ne pourront consulter leur DMP qu'à partir d'avril 2011. Il recevra un accueil très mitigé entre 2011 et 2013, date à laquelle seulement 418 011 DMP ont été ouverts pour un coût de plus de 500 millions(23). Parmi les explications, mises en avant pour expliquer les difficultés de mise en place, sont mentionnées : la définition imprécise de son contenu et de ses champs d'applications, la création repose sur le médecin généraliste sans intérêt pour lui et sans rémunération particulière, les modalités d'utilisation du numéro d'identification de la sécurité sociale (NIR), les modalités de consentement du patient, la grande difficulté de suppression par les patients qui le souhaitent et des problèmes de compatibilité entre le DMP et les logiciels de gestion de cabinet médical. Certains médecins se plaignaient aussi d'une ergonomie « médiocre » rendant la complétion du dossier difficile(24).

Le 13 avril 2015, une deuxième relance du DMP est présentée dans l'article 25 de la loi de santé ; elle le renomme dossier médical partagé et prévoit un déploiement dans 9 départements tests en 2016 puis une extension progressive. Le DMP peut contenir les documents suivants :

- Comptes rendus hospitaliers et radiologiques
- Résultats d'analyses biologiques
- Antécédents et allergies
- Actes importants réalisés
- Médicaments prescrits et délivrés

À tout moment, le patient peut supprimer certains documents qu'il contient où empêcher l'accès à certains professionnels. L'accès au DMP ne nécessite pas de

consentement signé du patient, mais une déclaration sur l'honneur par le professionnel souhaitant y accéder que le patient l'y autorise. Chacun peut s'il le désire créer son DMP, ou demander sa création dans un établissement de santé ou lors d'une consultation médicale.

Actuellement les dossiers numériques colligent une énorme quantité de données éparpillées dans des bases de plus en plus nombreuses. Ces bases sont très utiles pour assurer un suivi de chaque patient, mais elles posent des problèmes de sécurité des données personnelles à une échelle très différente de celle qui s'appliquait au dossier papier : ouvrir un accès distant à ces bases de données sensibles crée de nouvelles vulnérabilités propres aux réseaux informatiques.

3.2.6 Du papier à l'informatique : comment préserver la confidentialité

Quand les informations des patients n'étaient qu'orales, leur divulgation ne pouvait relever que d'un acte délibéré du professionnel de santé et le secret était garanti par la seule éthique du professionnel. Avec le passage à l'écrit et la présence d'un objet physique, des problèmes de stockages se sont posés. Il a fallu mettre au point des systèmes de classement, réfléchir à leur durée de conservation et à leurs modalités de destruction. De même la question de la protection de ces informations contre la négligence et la malveillance s'est posée. Dès lors que des documents ont une existence physique il est possible de les perdre, de les voler, de les dupliquer, de les falsifier ou d'y introduire des erreurs pour les diffuser. Le problème est de s'assurer que seules des personnes autorisées puissent avoir des accès en lecture et en écriture. Néanmoins la réalité du support physique du DM papier lui assure un certain niveau de sécurité et limite de fait sa diffusion et son accès à l'échelle du

support. Inversement le passage au numérique et la disparition de l'objet physique anéantit cette sécurité primaire.

Pour accéder à un document papier, il faut s'introduire dans son lieu de stockage, donc se déplacer jusqu'à lui et on ne peut explorer qu'un lieu de stockage à la fois. Il faut ensuite copier le document, procédure assez longue et coûteuse si l'on veut copier par exemple tous les dossiers médicaux d'un hôpital.

La collecte de ces données n'est à la portée que de rares acteurs comme les états par exemple et uniquement contre des personnes désignées. La collecte de masse de telles informations est impossible en pratique.

A l'inverse, conserver un dossier médical, même chiffré dans un ordinateur, revient à l'enfermer dans un coffre que n'importe qui dans le monde peut tenter d'ouvrir à n'importe quel moment et pour un coût par essai dérisoire. Une fois ouvert, les informations contenues dans ce coffre peuvent être divulguées et dupliquées dans le monde entier en seulement quelques secondes.

De même lors de la transmission d'informations « physiques », il est difficile d'imiter l'écriture et la signature de son auteur. En revanche numériquement l'identification des parties et l'authenticité du contenu doivent être assurées par des outils de chiffrement.

Par exemple une adresse e-mail non sécurisée, facilement usurpable, conduit de nombreux internautes à se faire voler, chaque année, leurs informations bancaires via de faux mails imitant leur banque.

Il est difficile d'intercepter un courrier postal, il est complexe d'espionner une conversation et une mise sur écoute permanente coûte très cher. En informatique il est possible pour n'importe qui, connecté à internet, d'écouter tout ou partie des informations envoyées, ce qui revient à suivre et noter chacun des échanges privés ou non. Le chiffrement, même s'il est indispensable, ne change pas cet état de fait,

il vous fait juste communiquer dans une langue incompréhensible, mais il n'empêche pas l'écoute. Une fois circulante sur la toile, cette information même chiffrée est difficile à effacer complètement. Il n'y a aucun moyen de savoir combien de fois cette information a été dupliquée ou encore de connaître le nombre et la localisation des serveurs physiques assurant son stockage. Par exemple Wikipédia conserve une copie des pages web citées. Cette copie est consultable même si la page web initiale est supprimée ou modifiée. Il est donc impossible d'assurer qu'une information ayant circulé sur internet ait été complètement effacée.

En informatique la recherche et la manipulation de grande quantité d'informations sont aisées. Par exemple en disposant d'une source d'informations nominatives ne contenant pas d'information confidentielle et d'une source d'informations anonymisées contenant des informations critiques, il est possible de fusionner ces deux sources et de rendre tout ou partie des données confidentielles, initialement anonymisées, nominatives.

Prenons l'exemple d'un groupe Facebook regroupant des pharmaciens qui partagent de nombreuses photos d'ordonnance ou des histoires sur leurs patients. Elles sont évidemment toutes anonymisées, mais le pharmacien les postant ne l'étant pas il est aisé de retrouver son lieu de travail et de reconnaître un patient mentionné. De plus Facebook connaissant la localisation de chacun de ses utilisateurs mobiles, réglages par défaut conservés, et connaissant l'heure et le lieu de la photo via les métadonnées, peut en regroupant ces informations « dés-anonymiser » cette ordonnance. Cet exemple ne vise pas à discréditer ce type de groupe Facebook, mais plus à mettre en avant les dangers de la communication d'informations de santé via des vecteurs non conçus dans ce but. Il illustre la réelle difficulté à préserver l'anonymat par simple « pseudonymisation » à

l'ère des big data et de la facilité (relative) de ré-identification de patients par le croisement de bases de données.

Tout cela justifie la mise en œuvre de procédures de sécurisation que nous allons développer au chapitre suivant.

4 La protection des données de santé en officine

4.1 Recommandations

En matière de sécurité informatique, il existe des référentiels applicables à la pharmacie d'officine dans :

- le guide de la sécurité des données personnelles proposé par la CNIL

- le guide de la CNIL à destination des professionnels de santé

- les recommandations de l'ordre des pharmaciens [2] « Respect de la confidentialité des données de patients dans l'usage de l'informatique ».

Nous ne les détaillerons pas, mais en reprendrons les principaux points dans l'analyse des risques qui va suivre.

4.1.1 Analyse des risques

Les référentiels en sécurité informatique conseillent de pratiquer une analyse des risques. Elle consiste à identifier les événements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels puis de décider des actions à mettre en œuvre pour réduire le risque à un niveau acceptable.

- [2] le guide de la sécurité des données personnelles proposé par la CNIL https://www.cnil.fr/sites/default/files/typo/document/Guide_securite-VD.pdf

- Le guide de la CNIL à destination des Professionnels de santé https://www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_professionnels_de_sante.pdf

- Respect de la confidentialité des données de patients dans l'usage de l'informatique proposé par l'ordre des pharmaciens http://www.ordre.pharmacien.fr/content/download/75069/480084/version/6/file/Guide+Confidentialit%C3%A9+-+janvier+2013.pdf

-

L'objectif est de recenser systématiquement tous les fichiers contenant des données à caractère personnel, les traitements associés et les supports matériels, logiciels, ainsi que les canaux de communications et les éventuels supports-papier associés (documents imprimés et photocopies). Il faut ensuite déterminer les atteintes possibles accidentelle ou intentionnelle à la confidentialité, à la disponibilité et à l'intégrité des données. Il faut également étudier les menaces propres à chaque support avec leur fréquence. Il faut voir s'il existe des moyens de les détecter, combiner ces 2 paramètres et hiérarchiser ces menaces selon leur gravité, leur échelle (de l'accès aux données d'une personne à leur collecte de masse) et leur vraisemblance. Il faut ensuite mettre en œuvre des mesures de sécurité pour réduire ces risques.

Dans cette analyse des risques, il est rarement possible d'apparier un risque et une mesure : une mesure protégeant souvent contre plusieurs risques et la prévention d'un risque nécessitant souvent plusieurs mesures.

On déclinera donc les principaux risques mis en avant par les recommandations pour chacun des items, puis les mesures proposées par les recommandations pour répondre à ces différents risques.

4.1.2 Sécurisations des locaux et du matériel

En tant qu'acteur du circuit du médicament, les pharmacies ont déjà mise en place des mesures dans le but de garantir la sécurité physique des locaux. On ne s'étendra donc pas sur ce point.

Les risques

Les risques principaux sont : l'intrusion, l'accès par un personnel non autorisé, un sinistre majeur (incendie, inondation), une surtension ou une augmentation de température (panne de climatisation).

Les mesures

Les mesures à mettre en œuvre sont : la mise en place d'une alarme, l'interdiction d'accès à tout personnel non autorisé, des dispositifs anti-incendie, des panneaux anti-inondations, la surélévation du matériel, des détecteurs de température, d'onduleurs et autres sécurités électriques.

4.1.3 Sécurisations des postes de travail et des logiciels associés

Les risques

La sécurisation des postes de travail vise à se prémunir contre : les tentatives d'accès frauduleux qu'ils soient effectués depuis la pharmacie ou via une prise de contrôle à distance, notamment via internet, l'exécution d'un virus volontairement par une personne mal intentionnée dans la pharmacie ou par erreur via un message infecté ou une clef USB, les failles de sécurité du système d'information dues à l'interfaçage entre les différents logiciels métier et la panne matérielle.

Les mesures

Il est recommandé de ne pas utiliser un système exploitation obsolète, une liste de ces systèmes est disponible sur le site internet du CERT-FR [3] (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

Il faut aussi s'assurer qu'un pare-feu est installé sur le routeur et sur chacun des postes de travail. En plus du pare-feu un antivirus doit être installé sur chacun des

[3] https://www.cert.ssi.gouv.fr/information/CERTFR-2005-INF-003/

postes de la pharmacie, il est parfois nécessaire de modifier la configuration de ces deux logiciels selon l'activité de la pharmacie, par exemple il faut créer une exception dans l'antivirus si un script détecté comme un virus est couramment utilisé.

Il est recommandé d'effectuer régulièrement les mises à jour des logiciels et des systèmes d'exploitation pour se protéger des failles connues et corrigées. En effet des failles de sécurité sont régulièrement découvertes, et notamment les plus critiques se situant dans le système exploitation, dans les logiciels de sécurité (pare-feu et antivirus) et dans le navigateur internet. Notamment pour le système d'exploitation il peut être important de programmer ces mises à jour et de les systématiser, car elles peuvent être longues et geler le parc informatique. Par exemple, les mises à jour Windows étant disponible le mercredi il peut être utile d'en programmer une le mercredi matin avant le début du travail.

Il faut autant que possible harmoniser les logiciels, même logiciel et même version sur chacun des postes, pour faciliter les interfaces et les mises à jour.

L'installation et l'utilisation d'applications nécessitant des droits de niveau administrateur pour leur exécution doivent être limitées au maximum.

Les serveurs en tant qu'ordinateur accessible à distance doivent être particulièrement protégés, il faut donc constamment renforcer les mesures de sécurité et faire appel à des outils de détection des vulnérabilités.

Les actions sur chaque poste de travail doivent être limitées uniquement à celles strictement nécessaires à l'activité à partir de ce poste, par exemple un poste servant à la vente au comptoir ne devrait pas servir à la navigation internet.

Il est aussi recommandé de limiter le nombre et les permissions de chaque application au strict nécessaire, par exemple le personnel vendant exclusivement

des cosmétiques a besoin d'un accès au LGO pour effectuer des ventes, mais ne devrait pas pouvoir accéder à l'historique des traitements.

Il faut documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur le système, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans des documents auxquels les utilisateurs peuvent se référer. Chaque utilisateur doit être conscient des enjeux concernant la protection des données à caractère personnel.

La rédaction d'une charte informatique rappelant les règles élémentaires de protection des données peut également aider à la bonne application de la politique de sécurité de l'information appliquée dans la pharmacie.

La formation des utilisateurs est la meilleure méthode de sensibilisation à la sécurité du système d'information et permet de les faire adhérer à ces mesures de base.

4.1.4 Contrôle de l'accès aux données

Les risques

En matière de contrôle d'accès aux données, il faut se prémunir de l'accès aux données de santé par une personne non autorisée (y compris au sein des structures extérieures en cas d'externalisation d'activités), de l'accès à des données sensibles sans rapport avec l'activité de l'utilisateur et de la connexion avec le code d'un autre utilisateur.

Les mesures

Elles reposent essentiellement sur l'authentification et l'habilitation des utilisateurs.

L’authentification des utilisateurs doit assurer que chaque utilisateur du système n’accède qu’aux données dont il a besoin pour l’exercice de sa mission. Les mécanismes permettant de réaliser l’authentification des personnes sont catégorisés en trois familles selon qu’ils font intervenir :

- ce que l’on sait, par exemple un mot de passe,
- ce que l’on a, par exemple une carte à puce comme la CPS, moyen d’authentification des professionnels de santé,
- ce qui nous caractérise, par exemple une empreinte digitale ou encore une signature manuscrite.

L’authentification d’un utilisateur est qualifiée de forte lorsqu’elle a recours à une combinaison d’au moins deux de ces méthodes.

En pratique, l’authentification est souvent construite sur le couple login - mot de passe. L’authentification est toujours précédée par l’identification, permise par la saisie d’identifiant ou login parmi ceux associés à un compte. Il ne faut ni utiliser ni laisser actifs les comptes fournis par défaut par l’éditeur des logiciels.

L’authentification apporte la preuve de son identité. Quand elle est réalisée via un mot de passe, il doit être confidentiel. Il ne faut jamais révéler son mot de passe, ou le laisser accessible à tous, il doit être unique c’est-à-dire qu’un même mot de passe ne doit pas servir pour plusieurs logiciels et il faut choisir un mot de passe robuste. La robustesse d’un mot de passe est sa capacité à résister à une attaque par « brute force ». Il est déconseillé d’utiliser comme mot de passe un mot courant dans les langues les plus utilisées ou un des mots de passe utilisés très couramment comme « azertyuiop ». La CNIL recommande d’utiliser un mot de passe de minimum 8 caractères, d’en changer régulièrement, au moins tous les 3 mois, et de ne jamais utiliser 2 fois les mêmes mots de passe.

Pour garantir l'authentification des utilisateurs, il est recommandé de définir des règles de connexions et de déconnexions. Les principales sont :

- l'impossibilité de se connecter avec le même code utilisateur sur plusieurs postes en même temps ;
- la limitation du nombre de tentatives d'accès : en général, trois essais erronés bloquent l'accès ;
- la déconnexion automatique en fin de traitement par un utilisateur ;
- la déconnexion automatique après une période d'inactivité définie ;
- la possibilité d'une « mise en confidentialité » par un mode d'interruption volontaire déclenché par l'utilisateur ;
- le redémarrage conduit à la page d'identification ;
- un système d'horodatage participant à la sécurité des comptes en affichant la date et l'heure de la dernière connexion.

Il est nécessaire de formaliser par une procédure la création des comptes informatiques pour tout nouvel utilisateur dans les plus brefs délais, et la désactivation immédiate de l'accès dès qu'un utilisateur n'est plus habilité (changement d'activité, de mission ou départ).

Les habilitations définissent des niveaux d'accès aux données par les utilisateurs. Elles sont justifiées par leur métier ou dans les limites des besoins de leurs activités et en fonction de leur qualité. Chaque utilisateur ne doit accéder qu'aux données nécessaires à son activité.

La notion d'habilitation implique d'établir une hiérarchie des comptes dont le compte administrateur. Il doit posséder les droits lui permettant de modifier les paramètres de sécurité, d'installer des logiciels et du matériel et d'accéder à tous les fichiers de

l'ordinateur. Il est également habilité à créer et modifier les comptes d'utilisateurs. L'utilisation du compte administrateur doit être strictement limitée au nécessaire.

Un engagement de confidentialité doit être signé par tous les employés et particulièrement les non-professionnels de santé, qui n'ont pas toujours été sensibilisés durant leur formation au secret professionnel. Une autre possibilité est de prévoir une clause de confidentialité dans le contrat de travail.

Le contrôle de l'accès aux données est particulièrement important en pharmacie, car tout établissement pharmaceutique doit tenir à la disposition des patients la liste des personnes habilitées à saisir, conserver, archiver et transmettre par voie électronique des données personnelles de santé. Les personnes concernées par le traitement des fichiers de données à caractère personnel doivent connaître, entre autres, la finalité de ce traitement, les destinataires et les transmissions envisagées.(25)

4.1.5 Archivage et sauvegarde des données

La préservation de la confidentialité passe obligatoirement par la disponibilité et l'intégrité des données à caractère personnel d'où l'importance des notions de stockage, archivage et sauvegarde.

L'objectif d'une solution de sauvegarde est la récupération des données en cas d'événement indésirable. Les sauvegardes dupliquent les données du système informatique à un moment donné afin de les mettre en sécurité. C'est une copie de sûreté qui assure une reproduction exacte des données informatiques à un instant précis.

L'archivage, tout comme la sauvegarde, est une copie des données à un moment déterminé, mais il concerne uniquement les données anciennes ou dormantes et

vise leur conservation sur une longue durée. Ce recueil d'informations doit donc garantir la conformité des données sur le long terme.

Les risques

En matière de sauvegarde et d'archivage les risques sont : une non-disponibilité temporaire des données, une perte d'une partie ou de la totalité des informations, une rupture de la continuité de l'activité, une restitution non fidèle des données stockées ou un accès non autorisé à des données à caractère personnel via le stockage.

Les mesures

Que ce soit pour les sauvegardes ou les archivages, il est nécessaire de les sécuriser par une méthode de chiffrement (chiffrer les sauvegardes ou chiffrer les données à la source) et en les stockant dans un lieu sécurisé, distant du lieu d'exercice.

Les sauvegardes régulières permettent de restaurer le système avec un minimum de perte de données et assurent ainsi la continuité de l'activité en cas de panne. Elles doivent garantir l'intégrité des données, qui comprend aussi l'intégrité des historiques. C'est pour cette raison qu'elles doivent être testées régulièrement. On doit pouvoir, à tout moment, exécuter une restauration de sauvegarde.

Le plus important dans le stockage est de réunir les conditions de restitution des données. Pour cela, il est indispensable de stocker sur un support externe les données et de sauvegarder le logiciel. Il est nécessaire de garantir l'interopérabilité des systèmes dans le cas d'un transfert ou d'un partage des données sur plusieurs systèmes ou entre différents systèmes. Lors d'un changement du logiciel professionnel, il est courant que les sauvegardes ou les archivages ne soient plus lisibles et que les données à caractère personnel ne soient plus disponibles. Il est donc impératif que les ESN (Entreprise de Services du Numérique) garantissent au

pharmacien la possibilité de récupérer l'intégralité des archivages ou sauvegardes, quel que soit le logiciel. À ce titre, il peut être utile de sauvegarder au moins une fois l'ensemble des données, avec le logiciel et le système d'exploitation (restauration de l'environnement complet).

Il faut également être capable de différencier les types d'archivages selon les types de données, par exemple il serait impensable de stocker un registre des médicaments dérivés du sang devant être conservé 40 ans sur un DVD/CD dont la longévité dépasse rarement 4/5 années. Les supports doivent être sélectionnés selon de nombreux critères : leur durée de vie, leur capacité de stockage, leur taille physique, les potentiels transferts. Le stockage est également possible chez un hébergeur à condition qu'il soit agréé.

Il est aussi nécessaire de déterminer les dossiers actifs, constitués par l'ensemble des éléments de ces dossiers accessibles aux traitements automatisés. Ils doivent avoir des chemins d'accès valides.

Sauvegardes et archivages sont donc des copies des informations à un moment donné. Il ne s'agit donc plus des données « originales » au sens juridique du terme. Pour faire office de preuve, ces copies doivent :

- associer fond et forme de manière indissociable,
- être accompagnées de la traçabilité de toutes les modifications effectuées depuis la date de la copie,
- être enregistrées dans un format non modifiable,
- être dissociées de l'éditeur.

L'accès aux sauvegardes doit répondre aux mêmes règles que l'accès aux données à caractère personnel, par le biais des habilitations. Mais avec des

modalités d'accès spécifiques aux données archivées parce que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle.

Il est important de stocker les sauvegardes et les archives dans un lieu distinct de celui des machines hébergeant les données, pour assurer qu'elles ne soient pas perdues simultanément en cas de sinistre majeur.

La politique d'archivage doit intégrer la notion de cycle de vie des données. La durée de stockage est déterminée par les durées de conservation imposées par la CNIL et le code de la santé publique.

4.1.6 Comment sécuriser l'informatique mobile

Les risques

Les risques sont similaires à ceux des postes de travail, mais amplifiés par le caractère transportable et la possibilité de connexion en itinérance.

Les mesures

Il est recommandé d'utiliser des mesures d'authentification fortes pour les périphériques mobiles. Pour se faire de plus en plus d'ordinateurs portables, smartphones et tablettes sont équipés d'un dispositif de lecture d'empreinte digitale. Mais la mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL.

Encore plus que pour les postes de travail il est recommandé de limiter les logiciels installés au strict minimum.

Il est également recommandé de ne connecter les périphériques à un réseau que si cela est nécessaire à son utilisation.

Tous les périphériques mobiles de stockages de données : ordinateur portable, smartphones, périphérique de stockage amovible doivent être chiffrés.

Lorsque des appareils mobiles servent à la collecte de données, il faut prévoir un verrouillage de l'appareil au bout de quelques minutes d'inactivité et des purges sitôt que les données ont été introduites dans le système d'information de l'organisme.

4.1.7 Destruction

Lors d'un changement de matériel informatique, le pharmacien est responsable de la destruction totale des données stockées. Les supports de stockage sont en général mis au rebut ou recyclés. Un formatage simple est insuffisant pour rendre les données irrécupérables.

Les risques

Les risques liés à la destruction de matériels informatiques sont la persistance de données à caractère personnel sur les supports de stockage mis au rebut et la destruction ou élimination de données devant être conservées.

Les mesures

Il faut assurer la destruction totale des données à caractère personnel stockées sur les supports mis au rebut ou remplacés. Pour cela on peut utiliser plusieurs méthodes : la destruction physique (par écrasement, incinération ou torsion des disques durs, broyage des CD ou DVD) ou une démagnétisation pour certaines unités de stockage, ou l'effacement par réécriture avec un logiciel dédié et agréé. Dans le cas où le pharmacien souhaiterait faire sous-traiter cette destruction il doit être informé et son autorisation est requise selon une procédure préétablie et vérifiée avant toute destruction afin de s'assurer qu'aucune donnée ou logiciel devant être conservés ne soient présents sur le support à détruire. Il est important

de vérifier que le contrat contient bien une clause de confidentialité et qu'à chaque opération un document attestant de la méthode et de l'effacement des données soit remis au pharmacien.

Une attention particulière doit être portée au matériel de location ou de secours lorsqu'il est restitué pour assurer qu'aucune donnée sensible ne demeure stockée.

4.1.8 Maintenance

Tous les fournisseurs de LGO assurent une activité de maintenance et de hotline. Beaucoup utilisent la télémaintenance. Les éditeurs de logiciels effectuent des recueils d'informations sans l'accord du pharmacien et sans même qu'il en soit informé (26).

Dans les contrats avec les ESN, les responsabilités respectives doivent être clairement fixées et identifiées. Il serait aussi intéressant que les ESN développent des outils logiciels qui, par exemple, produiraient automatiquement des rapports d'intervention détaillés.

Les risques

Ils sont divers comme une intervention sur le système informatique effectuée sans que le pharmacien soit informé (au préalable ou a posteriori), un recueil de données et une transmission à des tiers effectués (de façon fortuite ou volontaire) sans l'accord du pharmacien ou l'accès d'une personne non habilitée aux données à caractère personnel durant une opération de maintenance.

Les mesures

Le pharmacien (ou le responsable de la sécurité informatique) doit vérifier que le contrat contient des clauses prévoyant : des normes de sécurité garantissant l'authentification des parties, l'intégrité et la disponibilité des données, l'accord

préalable du pharmacien à tout intervention, la signature d'une clause de confidentialité pour tous les employés de maintenance et l'assurance que toute donnée transmise est chiffrée.

Le logiciel de télémaintenance choisi doit être configuré pour qu'aucune intervention distante ne soit possible sur un poste de travail sans une intervention de l'utilisateur par exemple en cliquant sur une icône. L'utilisateur doit aussi pouvoir savoir quand une opération de télémaintenance débute et finit. Chaque intervention doit faire l'objet d'un rapport détaillé intégré au système de journalisation.

Les logiciels de télémaintenance constituent toujours une vulnérabilité dans un système, cela revient à percer une porte dans un mur. Il est donc important que le logiciel de télémaintenance n'ait pas de vulnérabilité connue, ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) accorde des certifications de premier niveau à des logiciels pour réaliser cet objectif.[4]

Il faut aussi vérifier que l'accès physique et logique aux ports de diagnostic et de configuration à distance est contrôlé.

4.1.9 Traçabilité

Les risques

Les risques sont principalement qu'une des actions suivantes soit effectuée sans que le système en conserve une trace : un accès non autorisé à des données à caractère personnel, une utilisation abusive de données à caractère personnel, un

[4] http://www.ssi.gouv.fr/archive/fr/confiance/ certif-cspn.html.

détournement d'information, une altération des données (changées ou détruites), l'exploitation d'un défaut de sécurité.

Les mesures

La traçabilité fait partie des critères de sécurité des systèmes d'information. Elle consiste à suivre le cheminement de l'information, avec la possibilité de mener des analyses. Il est recommandé d'y associer la non-répudiation. La traçabilité peut permettre d'identifier un accès frauduleux à des données personnelles ou une utilisation abusive de ces données.

On parle de « journal des traces », qui doit être consulté régulièrement. Il doit au minimum contenir la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion.

Il est donc important que l'horloge des différents systèmes de traitement de l'information soit synchronisée (routeurs, PC, serveurs, etc.). Il est recommandé d'y ajouter poste par poste les actions réalisées (ajout, modification, suppression) par les utilisateurs, les événements liés à la sécurité et les tentatives de connexions.

La durée d'archivage de ces informations n'est pas bien définie. La CNIL parle d'une « durée non excessive ». On peut considérer que leur conservation doit s'aligner à minima sur celle des fichiers à caractère personnel.

Lorsqu'un système de traçabilité est mis en place, les utilisateurs doivent en être informés et doivent connaître la nature des traces qui sont journalisées et archivées.

Il est important que ce système ne serve qu'à garantir le bon usage du système d'information pour éviter que les utilisateurs tentent volontairement de le contourner.

La traçabilité est souvent associée une gestion des incidents.

4.1.10 Réseaux locaux et internet

Les risques

En matière de réseau informatique les risques sont : un réseau non sécurisé, un réseau non fiable (coupures), l'infection par des virus, des malwares ou des chevaux de Troie, les spams, un accès illicite aux données à caractère personnel, le vol ou détournement de données, l'usurpation d'identité.

Les mesures

Pour les réseaux locaux, il faut cloisonner au maximum les différents réseaux informatiques. Un système d'information en réseau est un système de partage. Ce partage concerne les dossiers, mais aussi le matériel notamment les périphériques comme les imprimantes, etc. La sécurisation d'un système en réseau passe par la segmentation du réseau local en réseaux virtuels (VLAN). On peut, par exemple, séparer le service administratif du service médical. La segmentation peut aussi permettre des mesures de sécurité différentes.

À noter : le secret partagé n'exonère pas chacun de sa responsabilité en matière de secret professionnel.

Il est aussi recommandé de changer les identifiants par défaut permettant de se connecter via le réseau au routeur et aux différents périphériques : fax, imprimante ou caméra.

La connexion internet doit être restreinte au strict nécessaire ou prévoir la séparation physique entre internet et le réseau local. Les flux réseau doivent être limité au strict nécessaire, un compte administrateur ne doit jamais être utilisé pour naviguer sur internet, un système de détection d'intrusion doit être installé. Des solutions logicielles doivent assurer que toutes les informations qui transitent sont rendues illisibles par des moyens de chiffrement.

Les connexions wifi doivent être sécurisées par le protocole WPA2 et le wifi doit être désactivé s'il n’est pas nécessaire au fonctionnement de la pharmacie.

4.1.11 E-commerce

Les risques

Le E-commerce en pharmacie cumule tous les risques évoqués précédemment et surtout ceux liés aux connexions réseau en y ajoutant le grand nombre de nouvelles vulnérabilités liées au maintien d’un serveur web, que nous ne pourrons détailler ici. Quand une pharmacie ouvre un site internet de vente en ligne de médicament, le pharmacien devient responsable de données bancaires en plus des données de santé.

Les mesures

Il n’existe pas de recommandation propre au E-commerce, en pharmacie. D’autant plus que celui-ci est encore encadré de manière relativement floue par la loi française. Mais on peut supposer qu’on exigera à minima les mêmes attentes que pour la vente physique des médicaments. Il est aussi obligatoire de faire appel à un hébergeur de données de santé agréé pour le site de vente en ligne de médicaments. Le pharmacien devra être très attentif aux clauses dans le contrat de sous-traitance, car il reste responsable des données à caractère personnel de ces patients même en utilisant un hébergeur agréé.

4.1.12 L’anonymisation

Il est interdit pour une pharmacie d’utiliser les données-patient à des fins commerciales, cela inclut par exemple la publicité ciblée ou le démarchage. Mais une pharmacie peut utiliser les données issues des ventes pour faire des

statistiques. Dans le cas où elle voudrait faire appel à un prestataire extérieur, ces données doivent être anonymisées. Il existe une problématique inhérente à l'anonymisation de données qui est la ré-identification de patients depuis les données anonymisées. Cette problématique est majorée en pharmacie, car les données de consommations de médicaments sont des données très discriminantes, rendant donc la ré-identification plus aisée même à partir de données « pseudonymisées ». De plus la pharmacie fournissant ces données n'étant pas anonyme, elle délimite un périmètre géographique permettant de grossièrement localiser ces patients. Pour parer à ce risque, le pharmacien doit s'assurer que le procédé qu'il utilise pour anonymiser ses données est non réversible. Le G29 (groupe des "CNIL" européennes) qui a publié un document sur les différentes procédures d'anonymisation met en avant la difficulté d'anonymiser des données en conservant l'intérêt de leur exploitation et évalue l'efficacité de différentes techniques, le choix de chaque technique dépendant du jeu de données.

4.1.13 Transmissions

Il faut différencier les transmissions à caractère obligatoire comme les télétransmissions aux caisses ou l'alimentation du dossier pharmaceutique (DP), de celles à caractère volontaire comme l'externalisation du tiers payant ou la transmission des rapports d'observance par les prestataires de services de santé à domicile aux prescripteurs.

Dans le 1er cas, la sécurisation, donc la confidentialité des données à caractère personnel est garantie, car très encadrée par la législation. Par exemple les FSE en mode sécurisé sont chiffrées à l'aide de l'algorithme triple DES considérés comme sûr.

Dans le 2e cas, le « transmetteur » doit s'assurer du respect de la réglementation. Pour la transmission des données de santé il est obligatoire que les interlocuteurs soient identifiés et que les données transitent de façon confidentielle donc chiffrées, pour ce faire il est conseillé d'avoir recours à un VPN (Virtual Protocol Network) : réseau logique privé et dédié, car seuls les ordinateurs des réseaux locaux, de part et d'autre du VPN, peuvent accéder aux données en clair.

Dans tous les cas, l'utilisation du réseau internet pour transmettre des données personnelles de santé nécessite la mise en œuvre d'un système de chiffrement « fort » de la transmission.

De nombreuses recommandations proposent des mesures à mettre en place pour garantir la sécurité des données de santé. La question est de savoir si les professionnels de santé travaillant en officines les mettent en œuvre. La suite de ce travail va explorer, via un questionnaire, la réalité de cette mise en œuvre, en cherchant à évaluer le niveau de sécurité informatique dans les pharmacies d'officine.

4.2 Evaluation des pratiques en officine

4.2.1 Matériel et méthode

Questionnaire

Les données sur le suivi pratique des recommandations en matière de sécurité informatique manquent. Cet état des lieux a été réalisé grâce à un questionnaire proposé aux professionnels travaillant en officines.

L'objectif était de préciser les recommandations suivies en pratique, d'évaluer le niveau de connaissance en matière de sécurité informatique des professionnels de santé en officine et de les interroger sur leur responsabilité dans la prise en charge de cette protection.

Le questionnaire proprement dit est présenté en annexe. Il a été soumis numériquement aux sondés. Il se composait de 3 questions préliminaires visant à situer les caractéristiques sociodémographiques des habitants de la zone d'exercice de leur officine.

Le questionnaire était organisé en 36 questions obligatoires et 20 questions conditionnelles présentées en fonction des réponses données précédemment. Cette modalité visait à réduire le temps de réponse moyen pour augmenter la participation. Les questions étaient à choix unique ou multiple. Lorsque l'item « autre » était la réponse choisie, un champ libre était proposé pour plus de développement. Lors de l'analyse des résultats, quand cela était possible, le champ "autre" a été regroupé avec la modalité proposée équivalente, sinon une nouvelle modalité a été créée.

Le questionnaire a été distribué via Facebook sur différents groupes professionnels « tu sais que tu es pharmacien » pour les pharmaciens d'officines, « Tu sais que tu es préparateur/préparatrice en pharmacie quand... » pour les préparateurs et « 6A officine 2016-2017 » pour les étudiants en 6ème année d'officine de Grenoble.

Ce questionnaire a été largement ouvert, le pharmacien titulaire pouvant déléguer à n'importe qui la mise en place de la sécurité des données patient. De plus, chacun des utilisateurs étant en mesure de compromettre la sécurité des données, il me semblait intéressant d'évaluer le niveau de connaissance de chacune des professions. Pour obtenir des données sur les connaissances des futurs employés en officines, ce questionnaire a été ouvert aux étudiants.

Il n'y a pas eu de plan de sondage pour ce questionnaire, les réponses ne peuvent donc pas être considérées comme provenant d'un échantillon représentatif des pharmacies d'officines françaises. Les résultats ne sont représentatifs que du niveau de sécurité informatique pour les personnes travaillant en pharmacie ayant participé à cette enquête.

Le questionnaire a été élaboré avec le logiciel « sphinx déclic 2 ». Les résultats ont été analysés à l'aide du logiciel et langage de programmation R. version 3.4.3 "Kite-Eating Tree".

4.2.2 Résultats

Données générales

Au total il y a eu 142 réponses. Le taux de réponse moyen aux questions a été de 95%, intervalle de confiance à 95% [91%,99%], minimum 60% et maximum 100%. Le tableau 1 résume les principales données socio-démographiques en fonction de la profession exercée.

Tableau 1 données sociodémographiques

	Répondants	Âge moyen	Âge max	Âge min	Sexe H	Sexe F	Rurale	Quartier	Centre-ville
Apprenti préparateur	5	23	27	20	0 %	100 %	40 %	60 %	0 %
Étudiant en pharmacie	15	23	26	20	33 %	67 %	13 %	47 %	40 %

Pharmacien adjoint	31	27	47	24	19 %	81 %	29 %	58 %	13 %
Pharmacien titulaire	18	40	66	27	67 %	33 %	44 %	39 %	17 %
Préparateur	73	30	60	20	0 %	100 %	36 %	38 %	26 %
Total	142	30	66	20	16 %	84 %	33 %	44 %	23 %

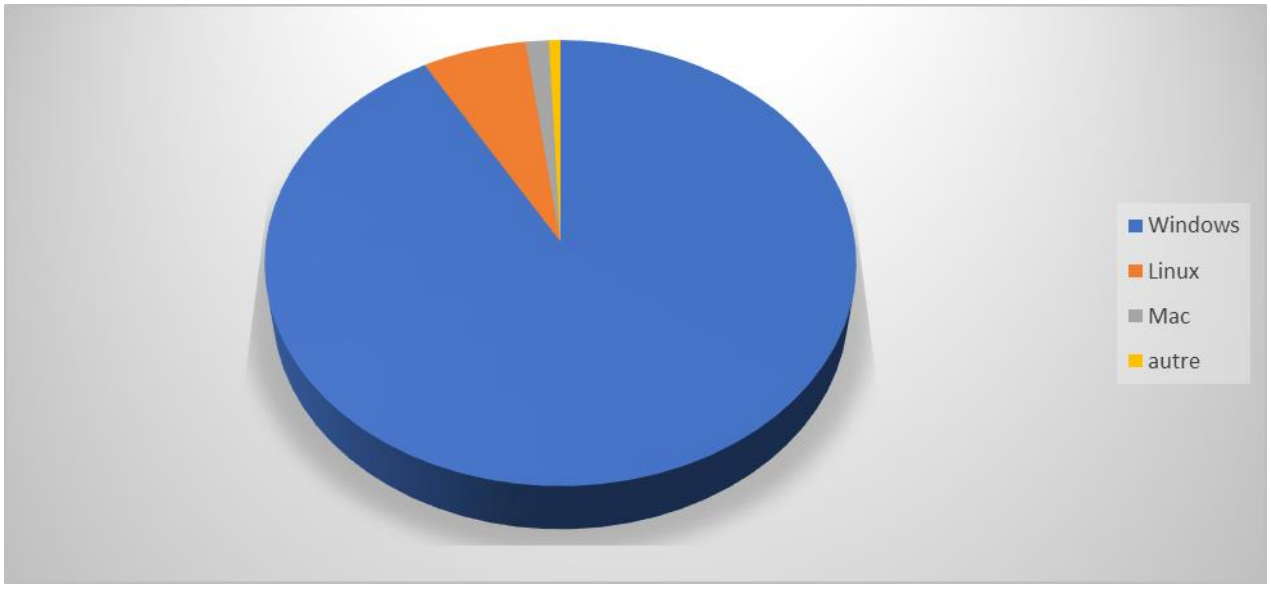
Les participants définissaient eux même si la localisation géographique de leur pharmacie était rurale, de quartier ou de centre-ville. Une hypothèse était que la situation géographique de la pharmacie pouvait avoir une influence sur le niveau de sécurité informatique des pharmacies interrogées. Mais il n'y a pas de différence statistiquement significative P- value 0.87 dans les réponses selon la localisation géographique de la pharmacie.

Les répondants au questionnaire étaient plus jeunes que la population travaillant en officine, l'âge moyen des pharmaciens titulaires répondants était de 40 contre 50 ans en moyenne dans la population générale (test de Student P value 0,002), la différence pour les pharmaciens adjoints 27 ans contre 43 ans (test de Student P value $2{,}2 \times 10^{-16}$).

Les résultats sont présentés en pourcentage avec entre parenthèse le nombre de répondant en valeur absolue.

Système d'exploitation

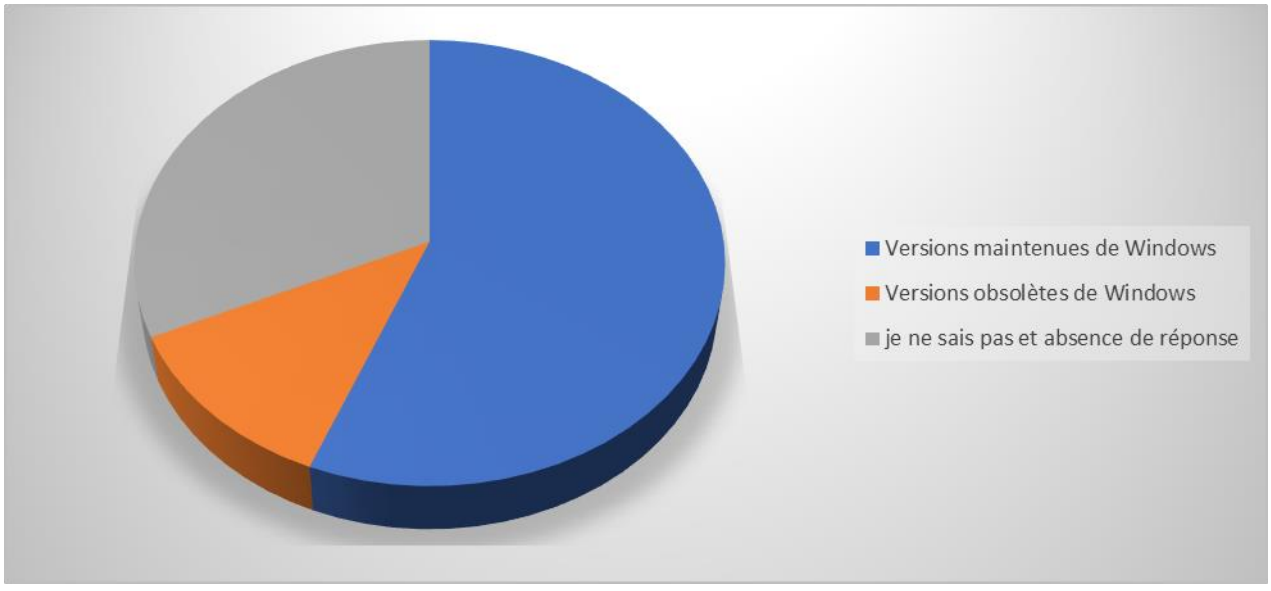
Figure 1 Répartition des systèmes d'exploitation



93 % (132) des répondants utilisaient le système d'exploitation Windows.

1,4 % (2) des répondants utilisaient plus d'un système d'exploitation

Figure 2 Version de Windows



30 % (40) des répondants ne connaissent pas leur version de Windows dont 23 %

(11) de pharmaciens incluant 6 % (1) de titulaire, il faut ajouter à ce chiffre les 13 %

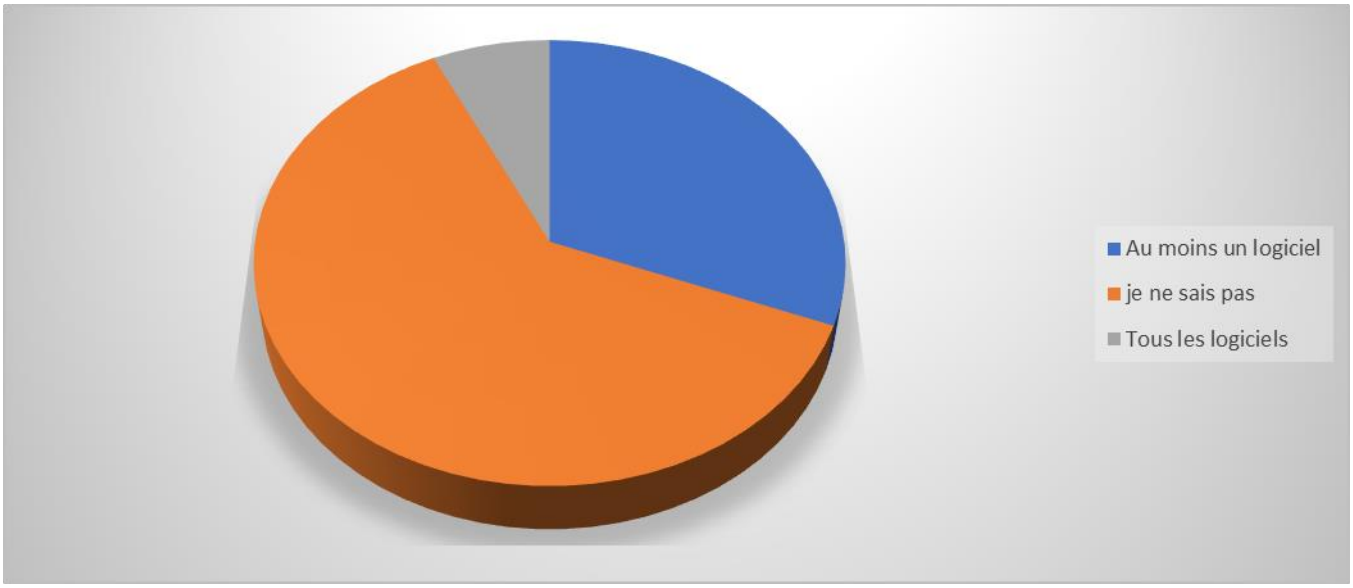
(2) des pharmaciens titulaires utilisant Windows qui n'ont pas répondu à cette question.

12 % des utilisateurs utilisaient un système exploitation obsolète avec 1,5 % (2) Windows XPsp1, 6 % (8) Windows XP sp2 et 4,5 % (6) Windows 8.

17 % (23) des utilisateurs utilisaient Windows 7.

Mise à jour logiciels

Figure 3 Mise à jour des logiciels



62 % (88) des répondants ne savaient pas si les logiciels de la pharmacie étaient mis à jour, dont 41 % (20) des pharmaciens incluant 17% (3) de titulaires.

11% (15) des répondants faisaient la vérification de mise à jour pour le système d'exploitation.

Pour 81 % (115) des répondants il n'y avait pas de contrôle des mises à jour des logiciels.

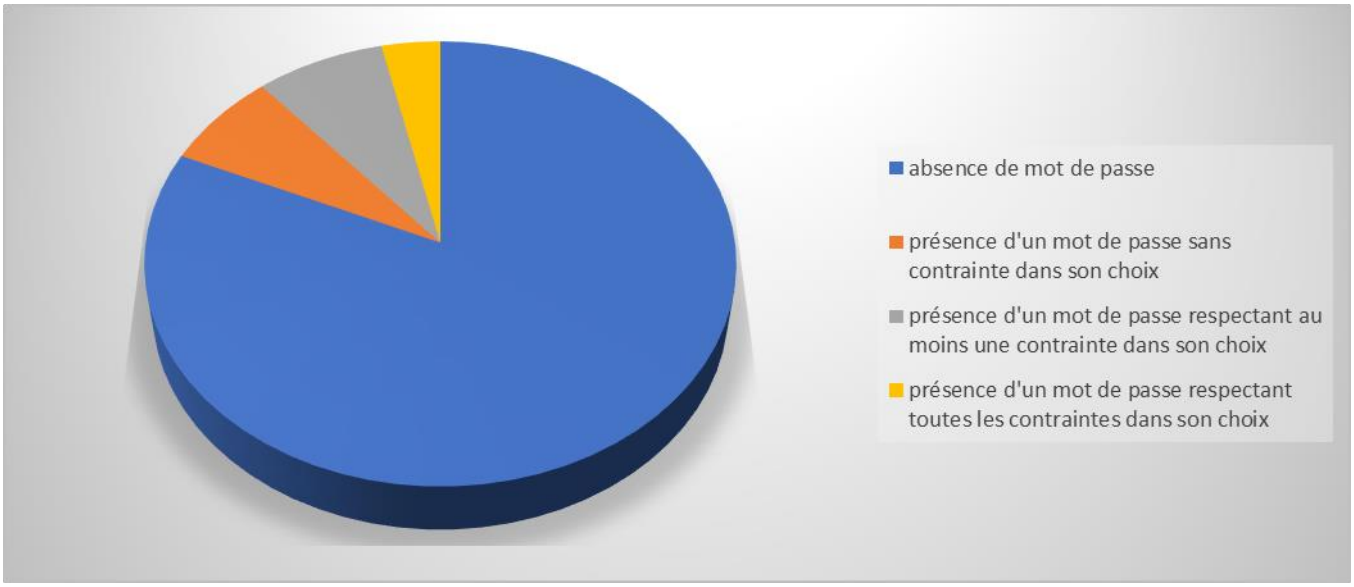
Mesure de sécurité

Login et mots de passe

Accès au poste : 55% (78) des répondants n'avaient pas de mot de passe et 15% (21) ne savaient pas. Seul 2,1% (3) des répondants avaient un mot de passe à l'allumage et en sortie de veille.

Accès au LGO

Figure 4 Utilisation d'un mot de passe pour accès au LGO

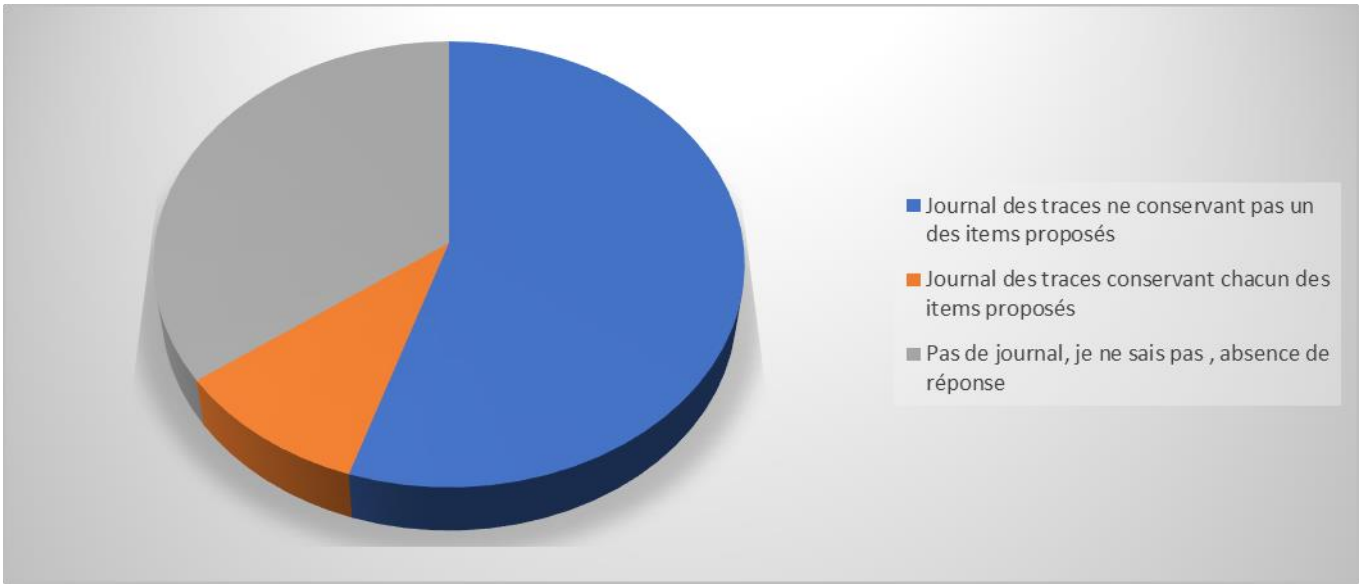


7 % (10) des personnes interrogées n'utilisaient aucun login

91% (129) utilisaient un login avant chaque opération. 18% (26) utilisaient un mot de passe dont 16,9% (24) avant chaque opération. Parmi les utilisateurs de mot de passe, 38% (10) n'avaient aucune contrainte dans le choix de ce dernier. 19% (5) des possesseurs de mot de passe, soit 3,5% (5) de la population totale, respectaient toutes les contraintes inhérentes à celui-ci.

Journal des traces

Figure 5 Journal des traces



64% (91) des répondants avaient un journal des traces, 30% (42) ne savaient pas, dont 33% (16) des pharmaciens incluant 22% (4) de titulaires. 15% (14) des personnes ayant un journal des traces soit 10% (14) de la population totale avaient un journal conservant les six items proposés « le journal des traces conserve une trace des consultations » , « le journal des traces conserve une trace des modifications », « le journal des traces conserve une trace des suppressions », « le journal des traces conserve une trace des connections », « le journal des traces conserve une trace des opérations de maintenance » et « le journal des traces contient les dates et heures des actions effectuées ».

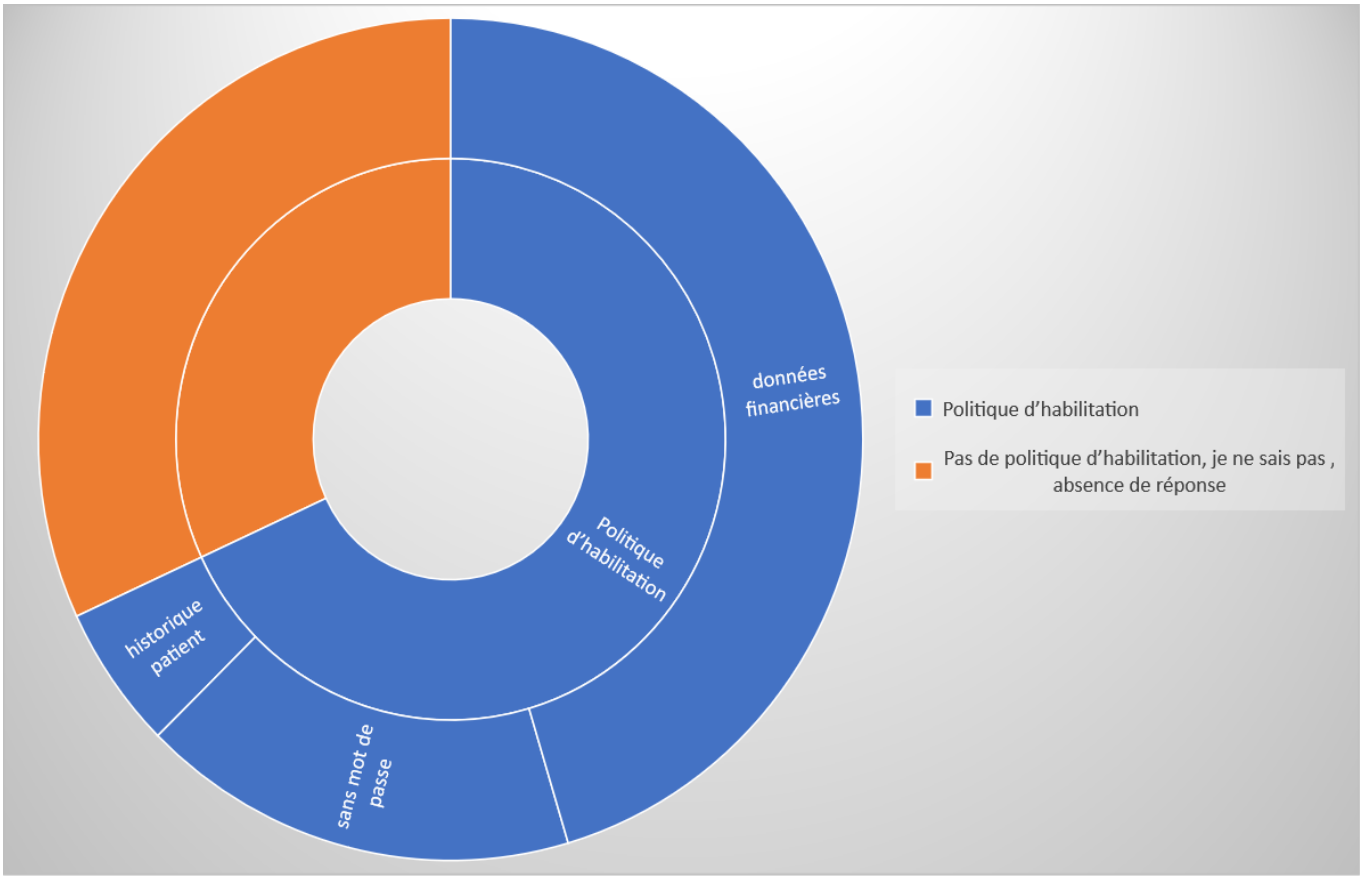
Politique d'habilitation

Dans 29% (41) des réponses, il n'y avait pas de politique d'habilitation, 6% (9) des répondants ne savaient pas, dont 6% (3) de pharmaciens n'incluant aucun titulaire. 20% (28) des répondants déclaraient avoir une politique d'habilitation sans utiliser de mot de passe.

Dans 80% (74) des cas, les politiques d'habilitation concernaient la caisse ou les transmissions.

Dans 10% (9) des cas soit 6% (9) de la population totale, les politiques d'habilitation concernaient l'historique patient.

Figure 6 Fonctionnalité protégé par une politique d'habilitation

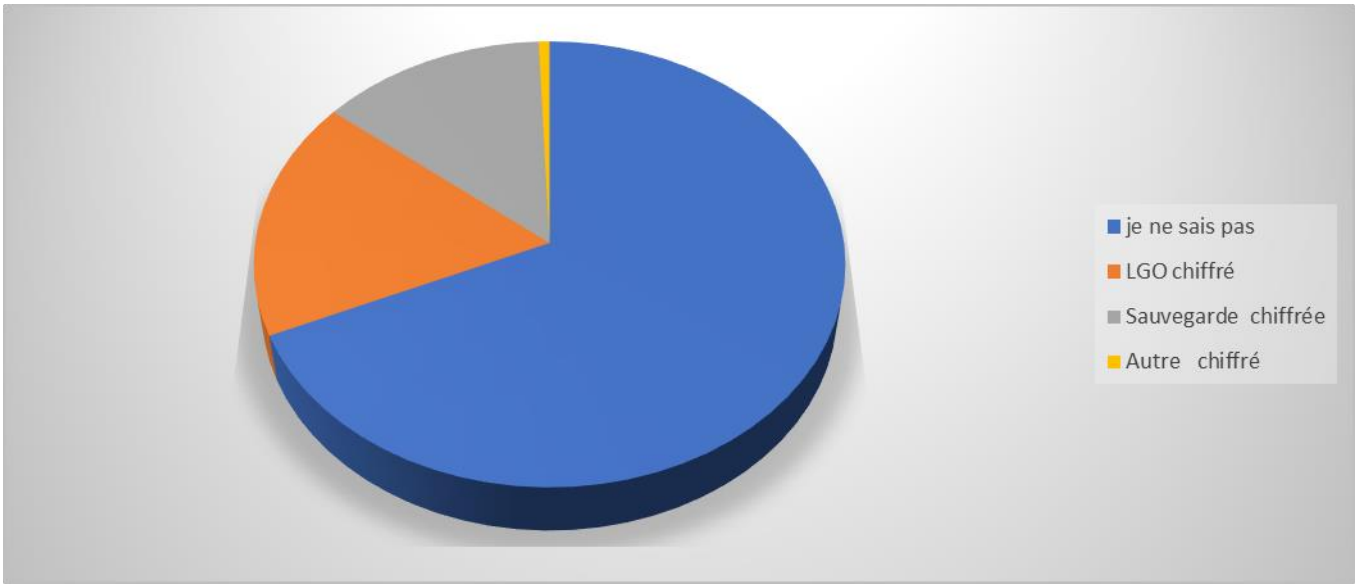


Contrat et formation

Contrat et formation : 72 % (102) des répondants ne pratiquaient aucune mesure relative aux contrats et formations. Aucun des répondants n'avait concomitamment de charte informatique, au moins un employé ayant suivi une formation en rapport avec l'informatique ni de contrat de confidentialité signé par les employés non professionnels de santé.

Chiffrement

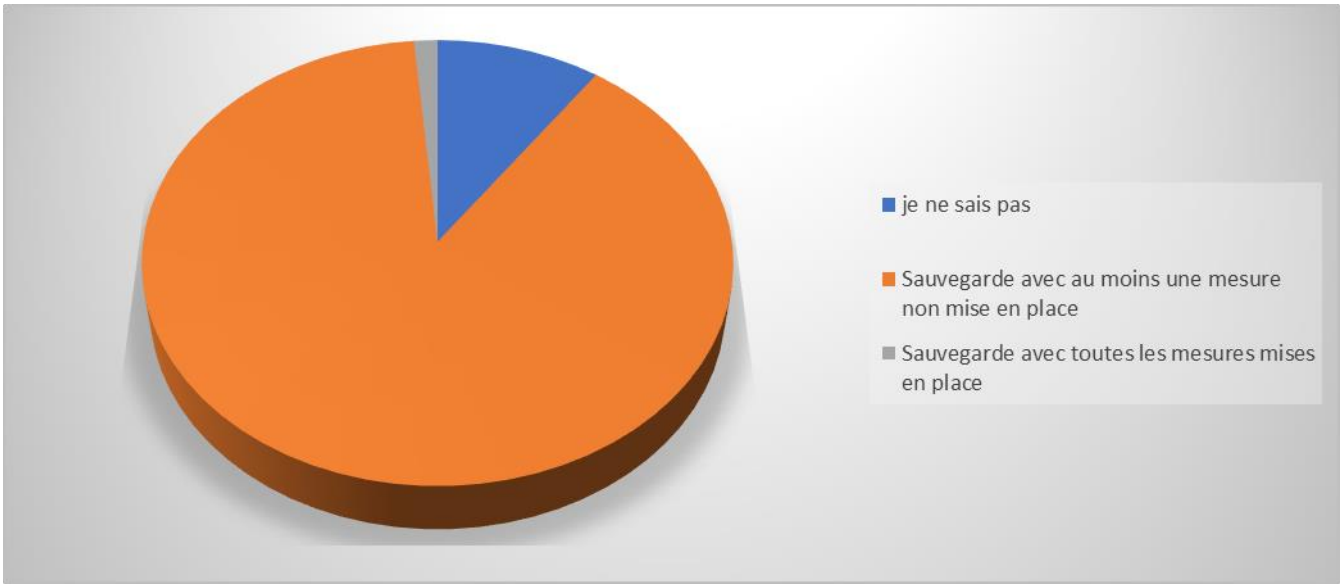
Figure 7 Chiffrement



74% (105) des répondants n'avaient pas de notion d'une méthode de chiffrement dans la pharmacie, dont 76% (37) de pharmaciens incluant 70% (10) de titulaires. 9% (13) des répondants avaient leurs sauvegardes et leur LGO chiffrés. Aucun des répondants ne connaissait le logiciel ou l'algorithme.

Sauvegardes

Figure 8 Sauvegardes



90% (128) des interrogés effectuaient des sauvegardes. 1,5% (2) des répondants avaient mis en place toutes les mesures de sauvegarde préconisées (périphériques, multiples sauvegardes du LGO, test des sauvegardes…). 10% (13) des sondés effectuaient des purges de leur sauvegarde.

Changement matériel informatique

15% (22) des répondants faisaient appel à un sous-traitant pour la destruction du matériel. 20% (28) n'avaient aucune procédure prévue, dont 24% (11) des pharmaciens incluant 44% (8) de titulaires.

61% (86) des répondants ne savaient pas.

16% (23) des personnes n'avaient pas de procédure valide de destruction du matériel.

Périphérique mobile

12% (17) des répondants utilisaient des périphériques mobiles dans leur pratique courante. Parmi eux 52% (9) ne savaient pas s'ils étaient protégés.

Télémaintenance

50% (9) des titulaires interrogés avaient répondu « je ne sais pas » à la question relative au contrat de maintenance.

39% (7) savaient que l'accord du pharmacien était nécessaire pour la mettre en œuvre.

22% (4) disposaient d'un rapport de maintenance.

6% (1) des titulaires interrogés avaient un contrat contenant une clause de confidentialité pour les employés en charge de la maintenance et une clause imposant que toutes les données transmises soient chiffrées.

Aucun des titulaires sondés n'appliquaient l'ensemble de ces 4 modalités

L'opération de télémaintenance était visible pour 44% (62) de l'ensemble des personnes interrogées. Une action était nécessaire à sa mise en place pour 60% (85) des répondants, mais ces 2 mesures étaient appliquées de façon concomitante pour 18% (32) des sondés.

Le logiciel de télémaintenance était agréé dans 1,4% (2) des réponses.

Changement de configuration

75% (107) des personnes interrogées ne savaient pas si la configuration de base des fax/imprimantes, caméras, et box internet avait été changée dont 69% (34) de pharmaciens incluant 56% (10) des pharmaciens titulaires. Dans 9% (13) des cas la

configuration n'avait été changée sur aucun des périphériques évoqués dans le questionnaire (fax/imprimante, box internet et caméra).

8% (12) des répondants avaient changé la configuration de la box internet

1,4% (2) des sondés avaient changé la configuration sur tous ses périphériques.

Le wifi

Le wifi était activé pour 64% (91) des sondés, mais il était nécessaire pour 39% (30) des répondants ; 5% (2) ne savaient pas s'il était nécessaire. Parmi les réponses ayant le wifi 15% (5) se connectaient par WPS (Wi-Fi Protected Setup) et 10% (9) ne connaissaient pas la procédure de connexion. Parmi les répondants utilisant une clef de connexion, 28% (20) utilisaient une clef WPA, 20% (14) une WEP (Wired Equivalent Privacy) et 52% (37) ne savaient pas.

Mail

Le mail était utilisé comme moyen de communication professionnelle pour 84% (119) des sondés. 74% (88) des personnes interrogées, utilisaient uniquement une boîte mail conventionnelle pour leur communication professionnelle.

25% (30) utilisaient une messagerie sécurisée. 53% (16) des sondés utilisaient une messagerie sécurisée spécialisée pour la communication entre professionnels de santé.

Fax

Le fax était utilisé comme moyen de communication professionnelle dans 70% (100) des réponses.

57% (57) des interrogés utilisant le fax ne mettaient en place aucune des mesures recommandées. Les mesures mise en place par les répondants utilisateurs de fax

étaient : préenregistrer tous les numéros pour 20% (20), envoyer une copie papier pour 15% (15) et les 2 mesures préconisées pour 2% (2).

Responsabilité du pharmacien

Le tableau 2 présente les réponses en pourcentages aux questions « Vous considérez que la sécurité informatique des données-patient est de la responsabilité des pharmaciens », et « Vous pensez que la sécurité informatique des données de santé devrait être assurée par les fournisseurs de logiciels à destination des officines ».

Tableau 2 Perception de la responsabilité de différents acteurs selon la profession

	Responsabilité pharmacien	Responsabilité LGO
Apprenti préparateur	60 % (3)	80 % (4)
Étudiant en pharmacie	80 % (12)	40 % (6)
Pharmacien adjoint	58 % (18)	65 % (20)
Pharmacien titulaire	67 % (12)	50 % (9)
Préparateur	53 % (39)	42 % (31)
Total	59 % (84)	49 % (70)

Pour 3% (4) des personnes interrogées un CIL avait été nommé dans leur pharmacie.

3% (4) des personnes interrogées pensaient être suffisamment formées en sécurité informatique.

8% (12) avaient lu les recommandations en matière de sécurité des données personnelles de santé.

4.2.3 Discussion

Les résultats ont été analysés selon les vulnérabilités aux scénarios d'attaque suivants :

- scénario 1, une personne tente d'obtenir les données d'une personne ciblée,
- scénario 2, une ou plusieurs personnes essayent d'obtenir des données de santé au hasard parmi les pharmacies ayant un faible niveau de sécurité (pêche),
- scénario 3, accès aux données sensibles par un membre du personnel non autorisé ou ayant une activité sans rapport avec ces données ou incapacité à identifier qui a eu accès aux données,
- scénario 4, attaque ou aléa conduisant à une cessation d'activité de la pharmacie
- scénario 5, une personne obtenant par erreur les données de santé d'un patient.

Une attention particulière a été portée au niveau de connaissance chez les titulaires qui en tant que chef d'entreprise sont légalement responsables de l'organisation de l'officine.

Biais

Le questionnaire ayant été exclusivement distribué par voie informatique, on peut s'attendre à ce que les répondants maîtrisent mieux l'outil informatique que la population générale.

Les réponses au questionnaire étant uniquement sur la base du volontariat, on peut attendre des résultats légèrement surestimés par rapport à la réalité.

Pour ne pas compromettre l'anonymat des répondants, les pharmacies où ils travaillaient n'étaient pas identifiées. Il n'est donc pas possible de savoir si plusieurs employés d'une même pharmacie ont répondu, mais parmi tous les répondants aucun ne mettait en place les mêmes modalités.

Données sociodémographiques

Les répondants au questionnaire étaient majoritairement des femmes, plus que la population générale des travailleurs en officine. Les pharmaciens adjoints respectaient exactement le sex-ratio de la population, en revanche les pharmaciens titulaires et préparateurs ayant répondu au questionnaire étaient plus souvent des femmes. (27,28)

Le fait que la population répondant au questionnaire soit plus jeune que la population générale s'explique par le mode de diffusion du questionnaire et devrait conduire à surestimer la maîtrise de l'informatique comparée à la population générale.

Système d'exploitation

Comme Windows était le système utilisé par 93% des répondants, les questions, visant à savoir si le système exploitation des pharmacies interrogées était obsolète, ne peuvent être présentées que pour ce système.

L'utilisation d'un système d'exploitation obsolète est particulièrement critique dans le scénario d'attaque 2, car ces systèmes d'exploitation ont des failles de sécurité connue qui ne seront jamais corrigées. L'utilisation dans un réseau local d'un seul poste utilisant un système d'exploitation obsolète rend tout le réseau local vulnérable, ce poste servant de porte d'entrée. L'utilisation d'un système exploitation obsolète rend également vulnérable au scénario 4, la compatibilité avec les autres programmes n'étant plus assurée.

On peut aussi noter que 17% des répondants utilisaient Windows 7 qui ne sera plus supporté dans 2 ans, une migration vers un autre OS devra donc être envisagée rapidement.

Ces risques sont majorés par le fait que 30% des répondants dont 23% des pharmaciens ne connaissaient pas leur version de Windows, ils sont donc potentiellement vulnérables ignorant quand leur système d'exploitation arrivera en fin de support.

Mesure de sécurité

Les mesures de sécurité proposées dans cette question visaient surtout à prévenir le scénario d'attaque 2.

50% des pharmacies utilisaient un antivirus, mais 13% seulement avaient un antivirus sur chaque poste, cela constitue une vulnérabilité, car un poste infecté peut compromettre toutes les données de santé d'une pharmacie. D'autant plus que les 11% de répondants ayant des sessions de travail en mode administrateur n'avaient pas d'antivirus sur chaque poste ce qui rend une infection plus critique puisque l'éventuel logiciel malveillant aurait les pleins pouvoirs sur la machine.

De nos jours toutes les box internet, ainsi que Windows sont équipés de pare-feu, on peut donc supposer que, malgré les 21% de réponses positives, toutes les pharmacies interrogées en sont équipées. Le faible nombre de personnes ayant répondu positivement à cette question souligne le manque de connaissance sur les outils à mettre en place pour garantir la sécurité des données. Quand, comme le pare-feu, ces outils sont mis en place par défaut cela ne constitue pas une faille de sécurité. Mais cela révèle une vulnérabilité puisque les répondants ne connaissaient pas son existence et n'étaient donc pas persuadés de l'utilité d'un tel dispositif.

Dans 12% des pharmacies, ces mesures étaient mises en œuvre simultanément. Il existe plusieurs antivirus gratuits et la plupart des systèmes exploitation dont

Windows intègrent un pare-feu, il est donc relativement aisé de mettre ces mesures en place.

Mise à jour.

Cette question a suscité le plus de réponse « je ne sais pas » (62%). Cela montre la faible importance accordée aux mises à jour dans les pharmacies où exercent les interrogés. Ce chiffre est à nuancer par le fait que, chez les pharmaciens titulaires, la modalité « je ne sais pas » a été moins souvent choisi que dans le reste de l'échantillon (17%).

Pour 81% des répondants il n'y avait pas de mise à jour systématique des logiciels clefs ce qui expose à des vulnérabilités dans le scénario 2. Des logiciels contenant des failles de sécurité révélées et qui auraient pu être corrigées par un patch peuvent être utilisés pendant une durée indéfinie.

Le fait qu'aucune procédure ne soit prévue peut occasionner des mises à jour inopinées et rendre la pharmacie vulnérable au scénario 4, d'autant plus que parmi les 3 logiciels proposés le moins vérifié est l'OS (11%) et qu'une mise à jour du système d'exploitation peut paralyser l'informatique d'une pharmacie pendant plus d'une dizaine de minutes.

La vérification et la mise à jour automatique à date et heure fixe est très facilement automatisable, la majorité des logiciels, dont Windows, le permettent en quelques clics.

Login et mots de passe

Pour 55% des répondants il n'y avait pas de mot de passe pour l'ouverture des postes de travail, ce qui rend vulnérable dans le scénario 1, en cas d'intrusion dans

les locaux de la pharmacie, et dans le scénario 3, les postes de travail étant accessibles à n'importe quel employé.

Ce nombre doit être majoré par les 15% répondants « je ne sais pas » ce qui peut laisser supposer qu'il n'y a pas de mot de passe.

Au total 2,1% des professionnels en pharmacie avaient un mot de passe à l'allumage et en sortie de veille. Tous les systèmes d'exploitation prévoient nativement qu'on puisse mettre un mot de passe à l'allumage et en cas d'inactivité. Ce mot de passe n'étant entré que peu de fois par jour il est peu contraignant.

Opération et accès aux données personnelles.

7% des professionnels interrogés n'utilisaient pas de système de login ce qui les rend incapable de savoir qui a accédé aux données patientes. Cela rend vulnérable aux scénarii 1, 2 et 3.

Dans 82% des cas il n'y avait pas de mot de passe ce qui représente une vulnérabilité dans le scénario 1 et 3 puisqu'il suffit de disposer d'un poste de travail pour accéder aux données.

La faible proportion de professionnels en pharmacie ayant un mot de passe (18%) peut s'expliquer par la contrainte qu'il représente. Dans une pharmacie un employé peut effectuer plus de 100 opérations en une journée et doit s'éloigner de son poste de travail pendant chaque opération. Entrer un mot de passe, même si celui-ci ne prend que quelques secondes, finit par être une contrainte importante pour chaque employé.

Il est intéressant de voir que malgré le peu de pharmacie ayant un mot de passe quand celui-ci est mis en place il est dans 93% des cas nécessaire avant chaque opération.

Parmi les personnes utilisant un mot de passe, nous avons cherché à savoir si des contraintes étaient imposées dans son choix et son fonctionnement. La question

relative à la « contrainte dans le choix des mots de passe » a eu un taux de réponse de 61%. Un item "aucune de ces propositions" aurait dû être prévu, mais n'explique probablement pas ce faible taux de réponse.

Concernant la déconnexion automatique en cas d'inactivité, principalement destinée à protéger les comptes dans le scénario 1 et 3, des contraintes dans le nombre et le type de caractère pour protéger contre une attaque par dictionnaire dans le scénario 1 et 2, un nombre d'essais limité contre une attaque par force brute dans le scénario 1 et 2 et l'affichage de la date et de l'heure de la dernière connexion pour permettre d'alerter en cas d'activités anormales sur le compte, 19% des interrogés utilisant un mot de passe avaient mis en place ces mesures (3% de toutes les professionnels interrogés). Cela limite l'intérêt d'avoir mis en place un mot de passe surtout au vu de la contrainte qu'il engendre.

Journal des traces

Les réponses mentionnant l'absence de login et/ou mot de passe montrent déjà une impossibilité à mettre en place un système de traçabilité efficace chez 88% des professionnels interrogés puisque sans même parler d'intention malveillante un employé peut être identifié à la place d'un autre sur une simple erreur de login.

Tous les LGO conservent une traçabilité des opérations, donc sauf si une des personnes ayant répondu au questionnaire est un cas très particulier n'utilisant pas de LGO par exemple, toutes les pharmacies ont un journal des traces. Cette question avait pour but de cerner l'utilisation du journal des traces. 64% des personnes interrogées utilisaient leur journal des traces mais pour 85% d'entre elles le journal des traces ne conservait pas toutes les modalités attendues : la date et l'heure des opérations, une trace des opérations de maintenance, de la connexion,

ou d'opération sur les données comme la consultation, la modification, la suppression.

Il est important de noter que 22% des pharmaciens titulaires interrogés ne savaient pas s'ils avaient un journal des traces, ce qui signifie qu'ils n'ont pas de moyen de vérifier si dans un des 3 premiers scénarios une ou plusieurs personnes ont consulté ou altéré des données sensibles. Il leur était de plus impossible de constater un défaut de sécurité ce qui rend impossible la mise en place de mesures de sécurité suite à un incident.

Politique d'habilitation

65% des personnes interrogées avaient des politiques d'habilitations. Mais dans 80% des cas, cette politique a été mise en place pour protéger l'accès aux données financières de la pharmacie comme la caisse ou les transmissions. Seulement pour 10% des professionnels la politique d'habilitation protégeait les données-patient. 90% des personnes travaillaient dans des pharmacies vulnérables au scénario 3, n'importe quel employé ayant accès à toutes les fonctions de tous les logiciels de la pharmacie.

20% des répondants déclarant avoir une politique d'habilitation n'avaient pas de mot de passe pour les connexions aux sessions. Le questionnaire ne prévoyait pas d'interroger sur la manière d'accéder aux fonctions protégées par la politique d'habilitation dans leur cas.

Contrat et formation

72% des pharmacies n'appliquaient aucune de ces mesures (une charte informatique, au moins un employé ayant suivi une formation en rapport avec l'informatique ou des contrats de confidentialité pour les employés non

professionnels de santé) et aucune des personnes interrogées ne les appliquait toutes. Ces résultats ne montrent pas une vulnérabilité directe en matière de sécurité des données de santé, mais pointent le manque à la fois dans la formation et l'organisation en matière de sécurité informatique dans les pharmacies. Le fait de ne pas faire signer de contrat de confidentialité à l'employé non professionnel peut le conduire à divulguer certaines des données par ignorance de leur caractère critique. Ce faible niveau de sécurité organisationnel pourrait être reproché au pharmacien titulaire en cas d'incident.

Sauvegarde

90% des personnes interrogées effectuaient des sauvegardes pluri-hebdomadaires, mais seulement 1,5% d'entre elles le faisaient en respectant toutes les recommandations (sur plusieurs périphériques, stockés dans des lieux différents des postes de travail, avec une sauvegarde du LGO et avec un test de sauvegarde préalable). Très peu effectuaient un test de leur sauvegarde (3%) probablement parce qu'elles n'ont jamais été confrontées à une restauration rendue impossible par une sauvegarde défectueuse. Ces résultats montrent que de nombreuses données pourraient être perdues dans le scénario 4.

10% des répondants effectuaient des purges de leur sauvegarde quand celles-ci dépassaient le délai légal de conservation. L'absence de purge multiplie les lieux de stockages des données et accroît la vulnérabilité notamment dans le scénario 3.

Chiffrements.

Le chiffrement est un point crucial dans la protection de données sensibles, il assure que, dans les scenarii 1, 2, 3 et 5, même si une personne obtenait des données provenant d'une pharmacie celles-ci seraient illisibles. Seulement 9% des

répondants avaient à la fois un LGO et leurs sauvegardes chiffrées. Aucun des répondants ne connaissait son logiciel de cryptage ou l'algorithme utilisé ce qui nous empêche de vérifier si le logiciel est agréé ou l'algorithme sûr. Dans une très grande majorité des cas (74%), les personnes interrogées sur le chiffrement ont répondu « je ne sais pas ». Il existe de nombreux logiciels libres et gratuits de chiffrement sur internet. Ils permettent de crypter de manière sûre les données de santé. Il pourrait être intéressant de sensibiliser les pharmaciens d'officine à leur existence et leur utilisation.

Changement matériel informatique

La destruction du matériel informatique endommagé ou obsolète n'est pas courant en pharmacie d'officine ce qui peut expliquer le nombre très important de « je ne sais pas » (61%). Pour une meilleure lisibilité les résultats sont présentés en % des personnes ayant répondu à une des modalités (procédures, sous-traitantes ou non) soit 55 répondants.

Pour 40% des répondants, la destruction était confiée à un sous-traitant et pour 9% une procédure interne était prévue dans la pharmacie. Parmi les professionnels ayant une procédure interne pour la destruction du matériel informatique, un seul travaillait dans une pharmacie ayant une procédure agréée pour les données de santé.

51% des répondants ont déclaré n'avoir aucune procédure pour la destruction du matériel informatique.

Dans 58% des cas les données personnelles contenues dans le matériel informatique mis au rebut, n'étaient pas ou pas complètement rendues inutilisables exposant ces données à une vulnérabilité aux scénarii 3 ou 5.

Il existe de nombreux logiciels libres et gratuits sur internet permettant d'effacer de manière sûre les données personnelles, contenues dans un disque dur ou une clef USB. Là encore une sensibilisation des pharmaciens d'officine pourrait être utile.

Périphérique mobile

Pour le moment les professionnels utilisant des périphériques mobiles (tablette, smartphone, ordinateur portable) dans leur pratique courante étaient rares (17 répondants). Ce qui rend les pourcentages sur les mesures de protection qui leur sont appliquées peu significatifs, sauf pour la modalité « je ne sais pas » choisie par 52%.

Mais on peut supposer que leur utilisation va aller en augmentant, il est donc important que les recommandations continuent bien à insister sur le caractère critique, car plus vulnérable de ces périphériques.

Contrat de maintenance et télémaintenance

Contrat de maintenance

La question sur le contrat de maintenance n'était présentée qu'au pharmacien titulaire, le nombre important de « je ne sais pas » (50%) peut être expliqué par l'oubli des modalités exactes du contrat. Cette hypothèse est confirmée par le fait que les modalités ayant reçu le plus de réponses positives étaient celles visibles depuis la pharmacie « accord du pharmacien nécessaire » (39%) et « rapport de maintenance » (22%), comparées aux modalités concernant le prestataire de

maintenance « contrat de confidentialité pour les employés en charge de la maintenance » (6%) et "toutes les données transmises sont chiffrées » (6%).

Aucun des répondants n'appliquait toutes les modalités recommandées.

Un questionnaire envoyé n'est probablement pas la bonne manière d'évaluer la conformité aux recommandations de sécurité des données de santé de contrats signés il y a des années.

Télémaintenance

La possibilité de prise de contrôle à distance d'un poste constitue une vulnérabilité, c'est comme ouvrir une porte dans un mur. Il est donc particulièrement important que cette action soit visible et nécessite une action depuis l'intérieur de la pharmacie.

1,4% des répondants, savaient que leur logiciel était agréé. Utiliser un logiciel qui ne l'est pas, représente une vulnérabilité notamment dans le scénario 2. La responsabilité du pharmacien serait engagée dans le cas d'une intrusion suite à l'utilisation pour la télémaintenance d'un logiciel non-agréé. Ce nombre doit être nuancé par le fait que la vérification de l'agrément du logiciel de télémaintenance peut avoir été faite il y a longtemps ou par une autre personne que le répondant.

L'opération de télémaintenance était visible pour 44% des personnes interrogées et une action était nécessaire à sa mise en place pour 60% des professionnels, mais ces 2 mesures étaient appliquées de façon concomitante pour 18% des personnes, ouvrant une vulnérabilité dans les scénarios 1 et 3, par exemple dans le cas où un membre de la société de maintenance souhaiterait accéder à des données de santé.

Changement de configuration

L’absence de changement des paramètres par défaut sur les périphériques connectés en réseaux avec le reste de la pharmacie constitue une vulnérabilité, majorée pour les périphériques accessibles depuis l’extérieur comme certaines caméras de surveillance. Il s’agit tout particulièrement des login et mot de passe fournis par le constructeur et donc écrits sur le mode d’emploi.

Une très grande majorité des répondants ne savaient pas (75%). Ce résultat s’explique par le fait que cette opération n’a était réalisée qu’une fois par périphérique, mais 55% des pharmaciens titulaires ne savaient pas, or il devrait être les garants de ces mots de passe. On peut donc supposer que pour au moins 16% des professionnels ce changement n’avait pas été fait (somme des répondants déclarant qu’aucune configuration n’a été changée et des pharmaciens titulaires qui ont répondu « je ne sais pas »). Quand les configurations pour tous ces périphériques sont restées celles fournies par défaut ceci rend les pharmacies vulnérables au scénario 2 et rend de plus une partie du parc informatique des pharmacies susceptibles de devenir des « zombies ».

La configuration a été changée sur chacun des périphériques pour 1,4% des personnes interrogées. Le périphérique dont le plus de personnes savaient que la configuration initiale avait été changée était la box internet (8% des répondants). Modifier les login et mot de passe par défaut pour les périphériques est une opération nécessaire une fois par périphérique, elle ne nécessite que peu de compétence et améliore la sécurité.

Le wifi

Le wifi offre une possibilité à toute personne présente physiquement y compris en dehors des locaux de se connecter aux réseaux de la pharmacie, il ouvre donc une vulnérabilité dans le scénario 1 et dans une moindre mesure les scénarii 2 et 4.

Le wifi était activé pour 64% des répondants, il était nécessaire pour 67% de ceux ayant le wifi activé. Au total pour 21% des interrogées le wifi, activé et non nécessaire, crée une vulnérabilité, sans intérêt pour le fonctionnement de la pharmacie.

Les professionnels ont été interrogés sur le mode de sécurisation mis en place pour leur connexion wifi. L'utilisation d'une clef WEP pour 15% des répondants ayant le wifi activé est une vulnérabilité importante. En effet, ce protocole a plusieurs faiblesses et peut aujourd'hui être craqué, avec peu de connaissances en informatique. Le WPS utilisé pour 15% des professionnels ayant le wifi activé possède lui aussi plusieurs vulnérabilités identifiées. Et le WPA (Wi-Fi Protected Access) ou WPA2 utilisé par 22% des répondants ayant le wifi activé est considéré comme sûr à condition que la clef de sécurité soit assez longue. Durant de nombreuses années, les routeurs internet utilisaient par défaut une clef WEP et le passage au WPA nécessite l'intervention d'un utilisateur. On peut donc craindre que dans une majorité des pharmacies où travaillent les personnes ayant répondu « je ne sais pas » (50%) la connexion wifi est sécurisée en WEP.

Mail

La messagerie électronique est le mode de communication utilisé par 84% des personnes interrogées pour communiquer avec les autres professionnels de santé. Parmi ces répondants, 74% utilisaient exclusivement une messagerie conventionnelle, les rendant doublement vulnérables en premier lieu dans le scénario 2, mais donnant potentiellement accès aux données de santé transitant par cette voie à l'hébergeur de leur boîte mail (Orange ou Google…). 25% utilisaient une messagerie sécurisée dont la moitié une messagerie sécurisée spécialisée pour la communication entre professionnels de santé. Ils existent des logiciels de

messagerie sécurisée spécialisée gratuits, ces logiciels offrent des avantages comme l'intégration automatique des données dans les logiciels de gestions. Il serait donc important de communiquer sur leur existence et de mettre en avant leurs avantages pour les pharmaciens.

Fax

Les recommandations en matière de sécurité informatique pour le fax visent à protéger les données des patients transmises dans le scénario 5. 20% des répondants utilisant le fax avaient tous les numéros utilisés préenregistrés et 15% des personnes envoyaient une copie. Ces 2 mesures étaient simultanément mises en place pour 1,4% des professionnels interrogées et 57% ne mettent aucune de ces mesures en place. À l'instar des mails l'utilisation d'une messagerie sécurisée serait préférable à l'utilisation du fax.

Responsabilité du pharmacien

41% des personnes interrogées et 33% des pharmaciens titulaires interrogés pensaient que la sécurité des données de santé n'étaient pas de la responsabilité du pharmacien. Ce résultat donne des éléments d'explication aux réponses précédentes. Si le pharmacien ne se sent pas responsable des données des patients ce n'est pas à lui de s'assurer que les mesures nécessaires pour les protéger sont en place. Les étudiants en pharmacie sont beaucoup plus conscients de leur future responsabilité, cet écart est probablement lié au fait que les étudiants en pharmacie sont nés avec l'informatique et une formation de bases via le C2I leur est donnée durant leurs études. Il serait donc particulièrement important dans un premier temps de sensibiliser les pharmaciens en exercice sur le fait que la sécurité informatique des données de santé est de leur responsabilité.

Le fait que 8% des personnes interrogées aient lu les recommandations sur lesquelles se base ce questionnaire explique aussi le faible nombre de modalités mises en place. Mais le besoin de formation, passant par une évaluation des connaissances, est ressenti puisque 97% des répondants pensent ne pas être suffisamment formés sur la sécurité informatique.

Il est donc intéressant de sensibiliser et proposer des formations sur les recommandations aux responsables et utilisateurs du parc informatique des officines.

Avec la mise en place des RGPD, les CIL déjà existants changeront de nom et seront remplacés par les DPO. 3% des personnes interrogées savaient qu'un CIL avait été nommé, ce qui présage un nombre similaire de nominations de DPO. Ce petit nombre de DPO nommé en pharmacie peut être expliqué par la difficulté d'identifier un DPO par pharmacie au regard de la taille moyenne des officines. Si l'état voulait démocratiser la nomination de DPO en pharmacie d'officine, il faudrait engager une réflexion globale de la profession avec le conseil de l'ordre pour faire émerger des propositions plus adaptées, avec des DPO responsables de plusieurs pharmacies par exemple.

Notons que 49% des répondants pensaient que le fournisseur du LGO devrait, en tant que professionnel de l'informatique, prendre en charge les données patients. Ces fournisseurs sont partiellement responsables aujourd'hui par exemple en cas de failles dans leurs logiciels ou de négligence. Mais le pharmacien est responsable de s'assurer que tout est mis en œuvre par le fournisseur du LGO pour garantir la sécurité des données confidentielles dans leur officine.

4.2.4 Conclusion

L'analyse des données montre que l'absence de connaissance des outils devant être mis en place pour garantir la sécurité de données critique constitue en soi une vulnérabilité. Le pharmacien, étant responsable de ces données, lui ou la personne qu'il a nommée responsable de la sécurité, doit savoir quelles mesures sont mises en place pour garantir leur sécurité. Sur l'ensemble du questionnaire ce sont les pharmaciens titulaires qui ont le moins répondu "je ne sais pas" avec 13% en moyenne, mais ce résultat doit être nuancé par le fait que de nombreuses questions concernaient l'organisation de l'officine et que le chef d'entreprise est la personne la plus à même de pouvoir y répondre.

Avec l'application du RGPD, les pharmaciens seront contraints de déclarer aux institutions concernées toute fuite de données les concernant, mais au vu de la faible sécurité mise en place dans les officines où travaillaient les personnes interrogées il est possible que des fuites de données passent complètement inaperçues.

Globalement le suivi des recommandations est très faible parmi les professionnels interrogés. 80% des recommandations sont suivis à moins de 40%. Deux modalités sont suivies par plus de 80% des professionnels interrogés : effectuer des sauvegardes et un login avant chaque opération. Mais ces 2 modalités ne sont pas suffisantes pour garantir la confidentialité des données personnelles.

Pour assurer une meilleure protection des données personnelles en officine, on peut augmenter le suivi des recommandations par les équipes officinales, ou s'assurer que les outils proposés aux professionnels de santé garantissent par défaut une meilleure sécurité.

5 Pistes d'amélioration de la protection des données de santé en officine

La population est de plus en plus consciente de la valeur et de la vulnérabilité de leurs données personnelles stockées informatiquement, en témoigne le récent scandale impliquant Facebook (29) et l'utilisation qui a été faite des données de leurs utilisateurs. Cela laisse présager que dans un avenir proche la population pourrait demander massivement et régulièrement des comptes aux sociétés hébergeant des données, à plus forte raison si ces données sont aussi sensibles que des données de santé. Des scandales pourraient se multiplier si les mesures mises en place ne sont pas suffisantes, obsolètes ou que la pharmacie manque de transparence.

Même si les résultats du questionnaire (basé sur le volontariat) ne sont pas extrapolables à toutes les pharmacies d'officine, ils donnent néanmoins une image instructive du niveau de sécurité informatique appliqué dans les officines et des difficultés rencontrées par les professionnels pour assumer leur responsabilité dans le domaine. Le caractère local de l'enquête en limite la portée nationale mais on peut penser sans trop de risque d'erreur que ces chiffres sont extrapolables à la population globale des officines.

Au-delà des déficits mis en évidence par l'enquête, elle présente l'intérêt de cibler les points de faiblesse majeur et donc les axes d'amélioration prioritaires à explorer.

5.1 Culture de la sécurité.

Introduire une culture de la sécurité informatique dans une entreprise présente plusieurs intérêts. En premier lieu, il suffit d'une seule personne mal informée pour compromettre la sécurité de tout un système. Deux exemples sont couramment donnés : l'ouverture de mails infectés et l'introduction d'une clef USB inconnue ou non contrôlée. Dans ces deux cas, tout le réseau informatique peut-être compromis, bien que toutes les mesures de sécurité aient été mises en place.

Un deuxième intérêt de la culture de la sécurité informatique est l'acceptation par les utilisateurs des mesures visant à garantir la sécurité des données de santé même si elles sont contraignantes, comme saisir plusieurs centaines de fois par jour un mot de passe d'une certaine complexité et d'un nombre de caractères suffisant par exemple. Il faut donc que les utilisateurs soient convaincus que c'est absolument nécessaire pour qu'ils acceptent de s'y plier. Ceci passe obligatoirement par une sensibilisation aux risques encourus.

On ne peut imposer la sécurité informatique ni à grande échelle (via l'état) en agissant sur les pharmaciens titulaires, ni à l'échelle du pharmacien titulaire sur son équipe. Quand des outils sont proposés ou imposés à des utilisateurs sans qu'ils y adhèrent, le risque est de les voir peu ou mal utilisés ou contournés, pour se soustraire à la contrainte qu'ils représentent. L'exemple le plus courant est le choix d'un mot de passe précaire comme "123" quand un mot de passe est exigé. Il faut donc faire prendre conscience à tous les utilisateurs de leur implication et de l'exposition aux risques liés à un faible niveau de sécurité. Cette adhésion ne pourra être obtenue que par la formation de tous les professionnels de santé.

Mais il est long et coûteux de former une population aussi vaste et hétérogène que l'ensemble des personnes travaillant en pharmacie d'officine. La formation professionnelle continue est un moyen, mais l'éducation des étudiants en

pharmacie et des préparateurs au cours de leur cursus universitaire est la meilleure façon d'augmenter leurs compétences dans ces domaines. La mise en place récente d'une plate-forme en ligne d'évaluation et de certification des compétences numérique (PIX) s'adressant à tous les individus francophones, lycéens, étudiants, professionnels, citoyens pourrait également être un support à cette formation continue.

Une autre étape serait de mettre en avant les recommandations déjà publiées, pour permettre aux pharmaciens sensibilisés de connaître ces mesures. Notamment il faudrait exposer plus les check-lists de l'ordre des pharmaciens (annexe 4) et de la CNIL en matière de sécurité informatique, qui permettent aux pharmaciens d'officine de visualiser une par une les mesures qu'ils n'ont pas encore mises en place.

Cette culture de la sécurité s'acquiert également en informant sur les conséquences potentielles d'attaques de leur entreprise, en prenant des exemples en rapport avec leur activité. Un pharmacien titulaire se sentira probablement moins concerné par des histoires lui semblant éloignées de son entreprise, comme une attaque d'un groupe de hackers sur le service informatique d'une grande entreprise par exemple.

Une de ces situations appliquées à une pharmacie d'officine pourrait être la suivante : un virus ou un incident technique rend le parc informatique indisponible durant plusieurs heures. Pour le pharmacien cela implique :

-d'investir en urgence des ressources pour éliminer le virus ou résoudre l'incident technique ;

- de passer les commandes quotidiennes auprès du grossiste par téléphone et sans l'historique des stocks ;

-de compliquer les ventes, par l'absence d'historique patient et de possibilité de créer des FSE ou d'imprimer des feuilles de soins. De plus dans l'intervalle chaque vente expose à des erreurs de stocks devant par la suite être corrigées potentiellement par un inventaire.

Dans le cadre de la sensibilisation des pharmaciens d'officine, il serait intéressant de chiffrer l'exploitation d'une faille de sécurité à son coût pour la pharmacie en pourcentage de son chiffre d'affaires quotidien. Ces chiffres n'existent pas pour le moment, mais une étude menée par Kaspersky(30) évalue en moyenne pour une PME le coût d'un vol de données à 86 600 dollars. Cette étude a été effectuée dans plusieurs pays, sur des PME, ce qui induit des biais. Ces PME ne payent pas forcément un support informatique permanent ce qui augmente le coût d'un incident. Mais ces PME n'ont probablement pas toutes des données aussi sensibles que les données de santé qui accroît le coût d'un incident. Cette étude situe quand même l'importance du coût d'une faille de sécurité pour une entreprise. Il serait intéressant de transposer ce travail en pharmacie.

Une autre possibilité serait de faire passer cette sensibilisation par les DPO. Les DPO doivent se déclarer et se maintenir informés des problématiques en rapport avec les données et leur traitement. Cela les rend plus faciles à contacter et plus enclins à se former en matière de sécurité informatique. On pourrait donc envisager de leur confier la mission de sensibiliser et de former leur collaborateur pour introduire par ruissellement la culture de la sécurité informatique en officine. Mais la nomination d'un DPO n'étant pas obligatoire en pharmacie (19), il est peu probable que les pharmaciens d'officine n'ayant pas nommé de CIL en nomme un. Une autre possibilité serait d'utiliser les titulaires dans ce même but, mais étant en moyenne plus âgés que le reste de leurs collaborateurs et n'ayant pas forcément d'inclinaison pour l'informatique, les formations risquent d'être plus aléatoires.

5.2 Certification

Une autre approche pour augmenter la sécurité informatique en officines serait de mettre en place une certification en matière de sécurité des données de santé. Cette mesure serait d'autant plus efficace si elle était encadrée par un organisme gouvernemental ou européen la rendant plus uniforme (une seule certification) et moins coûteuse que des certifications vendues par des entreprises privées. Mais la mise en place de normes strictes, uniformes et obligatoires soulève plusieurs problématiques. Qui supporterait le coût de la mise en place du choix des normes et leur mise à jour au fur et à mesure des évolutions technologiques ? Qui créerait la structure ? Qui contrôlerait les dossiers en vue d'obtenir cette certification ? Qui contrôlerait la mise en place en pratique ? De plus si cette certification était obligatoire, elle représenterait un poids qui augmenterait l'écart entre les petites et les grosses officines. Sa mise en œuvre serait quasiment impossible pour les premières à moins de les contraindre à mutualiser la sécurité informatique de leurs données.

5.3 Modalités peu coûteuses à mettre en œuvre.

Une partie importante de la menace en matière de sécurité informatique réside dans des attaques faites au hasard visant les ordinateurs les moins protégés. Les mesures suivantes ne sont pas suffisantes pour assurer la protection des données de santé, mais ne pas être parmi les ordinateurs les moins protégés constitue déjà une première protection importante. L'objectif est de montrer qu'il est possible d'augmenter la sécurité informatique en pharmacie à faibles coûts à la fois financiers et temporels.

Mise à jour des systèmes d'exploitation

Un argument cité fréquemment pour justifier l'utilisation d'un système exploitation obsolète, est le coût induit par le changement de version. Ce coût correspond à l'achat de la licence et au renouvellement du parc informatique s'il est trop vieux. Mais une version, Windows par exemple, est souvent maintenue pendant plusieurs années (13 ans pour Windows XP) ce qui permet d'amortir l'achat des licences. Si le coût semble malgré tout trop important la majorité des LGO fournissent une version compatible avec Ubuntu Linux.

De même il est souhaitable de tenir un registre contenant la liste des systèmes exploitation installés dans la pharmacie, et d'inscrire la date de fin de support lorsqu'elle est annoncée pour anticiper la mise à niveau de ces systèmes.

Aussi l'automatisation des mises à jour est facile à mettre en œuvre, mais elle peut causer un redémarrage intempestif et donc paralyser le parc informatique durant plusieurs minutes. Il est utile de planifier cette action de façon à ce que l'OS procède aux mises à jour en dehors des heures d'ouverture de la pharmacie, par exemple pour Windows [5]. Il est ensuite possible de configurer l'heure de redémarrage automatique.

Pour les autres logiciels, on peut prévoir une vérification des mises à jour une fois par semaine, cette tâche peut être facilitée par un logiciel vérifiant périodiquement pour tous les programmes.

---

[5] https://www.malekal.com/regler-heure-installation-mises-a-jour-windows10/ exemple lien explicatifs

Antivirus

Une des raisons expliquant qu'un antivirus n'est pas présent sur chaque poste de travail d'une pharmacie est que les pharmaciens en ignorent la nécessité et le coût, proportionnel au nombre de postes à équiper. Ce problème peut être résolu en choisissant un antivirus gratuit sur internet. Pour la majorité d'entre eux, ils ne nécessitent pas de configuration particulière et l'installation ne prend que quelques minutes. Microsoft fournit de plus Windows Defender par défaut avec Windows 10. Le choix de l'antivirus n'est pas une décision facile, les articles traitant de la comparaison d'antivirus étant des documents techniques relativement difficiles à lire. De plus les antivirus évoluent constamment au gré des nouvelles versions. Lors du choix de l'antivirus, il est important de se renseigner sur le logiciel que l'on installe, car de nombreux faux antivirus existent sur internet.

Pour les utilisateurs d'Ubuntu, l'utilisation d'un antivirus est discutable. Ils sont naturellement protégés, leur système exploitation étant par défaut très peu permissif, il ne laisse au programme que les droits explicitement donnés par l'utilisateur. De plus seule une minorité des utilisateurs ont choisi ce système ce qui rend le développement de virus ciblés sur Ubuntu moins rentable. Il est cependant recommandé par la CNIL d'installer un antivirus, quel que soit le système d'exploitation.

Les mots de passe Une première étape serait qu'un mot de passe différent soit défini sur chacun des postes de travail de la pharmacie et que ce mot de passe soit nécessaire à l'allumage et après une période d'inactivité. Ces mesures ne nécessitent pas l'installation de logiciel, tous les systèmes d'exploitation ayant nativement cette fonctionnalité. Mais cela implique de retenir un mot de passe par poste pour chaque employé.

Une solution est de créer des sessions utilisateurs, pour chaque employé, sur chacun des postes ; cela permet pour un employé donné de n'avoir que son propre mot de passe à retenir. Cette action contribue à initier le principe des habilitations en limitant les droits en fonction du niveau hiérarchique de l'employé, notamment en ce qui concerne l'accès au serveur. La mise en place de telles sessions assure aussi que la navigation internet sera toujours effectuée en mode utilisateur, la session administrateur étant réservé à l'installation de nouveaux logiciels et à la maintenance.

Pour aller plus loin, il est possible de configurer des sessions partagées permettant à chaque employé de la pharmacie d'avoir ses documents, quel que soit son poste de travail.

Quand le logiciel de gestion d'officine le permet, il est conseillé de configurer un mot de passe par employé au moins lors de leur première connexion et suite à une période d'inactivité pour accéder au LGO.

Dans un second temps, il est important d'introduire dans l'organisation de la pharmacie un agenda des changements de mot de passe, par exemple pour planifier cette action tous les 3 mois. En parallèle, les employés doivent être sensibilisés aux mots de passe sécurisés et à la nécessité de les différencier selon leur compte, par exemple le mot de passe de connexion à leur session ne doit pas être celui pour accéder au LGO. Il peut être intéressant par la suite d'automatiser l'obligation de renouvellement des mots de passe ainsi que les contraintes dans son choix. Il est aussi possible de conserver une trace des différents mots de passe choisis par chaque utilisateur, sans pour autant avoir à les connaître, afin d'éviter qu'un utilisateur alterne tous les 3 mois entre deux mots de passe.

Mots de passe et configuration sur les périphériques.

La connexion au routeur se fait en rentrant l'adresse IP dans son navigateur internet. Lorsqu'on se connecte sur la page d'administration du routeur, il faut introduire un login et un mot de passe. Si aucun changement n'a été effectué ou si le routeur a été remis en mode usine, ce sont le login et le mot de passe fournis par le fabricant. En cas de perte ils sont très faciles à retrouver en cherchant le modèle du routeur sur internet. La première chose à faire est de changer ce couple login-mot de passe par défaut. Ensuite, si le wifi n'est pas nécessaire au bon fonctionnement de la pharmacie il faut le désactiver dans la configuration du routeur. S'il est nécessaire, il faut s'assurer que la connexion par WPS est bien désactivée et que la connexion s'effectue par une clef WPA2. Ces modifications étant différentes pour chaque routeur internet il suffit de rechercher sur un moteur de recherche : clef WPA ainsi que le nom du routeur.

Il est par la suite possible de mettre en place une nouvelle sécurité depuis l'interface de votre routeur.

La création d'une liste blanche pour les adresses mac, permet aux seuls périphériques présents dans cette liste de se connecter au routeur et d'accéder au réseau.

Il est important de noter que le changement des logins et mots de passe par défaut de connexion ne doit pas être limité exclusivement au routeur et qu'il faut l'effectuer pour tout périphérique accessible à distance comme les caméras connectées, les imprimantes/fax … Pour ce faire, il faut rentrer leur adresse IP dans votre navigateur internet à la page de gestions du périphérique et modifier les logins et mots de passe par défaut.

Dans l'organisation du parc informatique, il est conseillé de prévoir une procédure pour l'ajout et le renouvellement de matériel informatique, dans laquelle le

changement des identifiants et mots de passe par défaut est prévu en même temps que la mise en place du nouveau matériel. Il est de plus conseillé de prévoir comme pour tous les mots de passe un calendrier de changement régulier.

Effacement des données avant mise au rebut

La destruction de matériels informatiques dans des conditions rendant impossible la récupération des données est une opération qui peut nécessiter des machines et des compétences spécifiques. Il n'est donc pas évident de la mettre en place à l'officine, le rôle du pharmacien est donc de choisir un sous-traitant et de contrôler le contrat. Il est néanmoins possible et peu coûteux d'assurer soi-même la destruction des disques durs et des clefs USB à l'intérieur de la pharmacie à condition que ces supports de données soient fonctionnels. Il suffit de télécharger un utilitaire d'effacement de données par passage multiple. L'ANSSI a certifiée "Blancco Data Cleaner+ version 4.8". Il existe de très nombreux utilitaires freeware, non certifiés pouvant remplir ce rôle, laissant au pharmacien la responsabilité de s'assurer que le logiciel efface correctement les données.

Il est aussi possible de détruire au sein de la pharmacie les CD et DVD à condition que la broyeuse à papier le permette.

Pour organiser la destruction du matériel informatique mis au rebut, il faut établir une procédure. Celle-ci regroupe : pour quel type de matériel la destruction est assurée au sein de l'officine et les moyens mis en œuvre. Pour procéder à la destruction du reste du matériel informatique, la pharmacie doit faire appel à un sous-traitant, certains fournisseurs de LGO assurant la maintenance se chargent de récupérer et de détruire le matériel informatique défectueux. Lors du choix de l'entreprise assurant la destruction du matériel informatique une attention

particulière devra être portée à la présence d'une clause de confidentialité et à la fourniture des preuves de destruction.

Chiffrement

Comme nous l'avons vu dans les parties précédentes, le chiffrement des données assure la dernière ligne de protection des données ; si elles venaient à être récupérées par quelqu'un elles seraient illisibles. Pour réaliser le chiffrement de tout ou une partie d'un disque dur, il ne faut que peu de connaissances techniques. La principale difficulté réside dans le choix du logiciel, il ne doit pas avoir de faille connue, il doit utiliser un algorithme considéré comme sûr et être le plus optimisé possible pour limiter le temps et les ressources consacrées à chiffrer et déchiffrer.

Le choix n'est néanmoins pas facile. Par exemple le logiciel de chiffrement freeware, Truecrypt certifié par l'ANSSI, considéré comme compromis par ses développeurs, qui conseillent à la place l'utilisation de Bitlocker. Pourtant celui-ci est connu pour offrir des portes dérobées au service de renseignements (31), son utilisation est donc déconseillée par certains professionnels de l'informatique.

Ce qui semble donc le plus prudent en matière de solution de chiffrement est d'utiliser un programme open source, le code est public et peut donc être contrôlé par tous, ce qui est la meilleure assurance qualité. Citons par exemple CipherShed qui est un "fork" open source de Truecrypt.

Dans l'idéal, toutes les données de chacun des postes de travail d'une pharmacie devraient être chiffrées. Mais si aucune solution de chiffrement n'était mise en place, il est recommandé de commencer par chiffrer les sauvegardes, car elles sont situées sur des périphériques amovibles et donc plus vulnérables et représentent de petits volumes. Par la suite, quand le personnel sera accoutumé à l'utilisation

des logiciels de chiffrement, il convient de mettre en place le chiffrement de tous les postes de travail.

Messagerie sécurisée

Il n'est pas acceptable, actuellement d'utiliser des moyens de communication non sécurisés pour les données de santé. Les messageries conventionnelles ne garantissent ni l'identité des protagonistes ni l'illisibilité des informations dans le cas où elles seraient interceptées.

Le choix d'une messagerie sécurisée protège aussi de la collecte de données de santé par les géants de l'internet comme Google qui analyse le contenu des mails(32). De plus, ces applications, quand elles sont à destination des professionnels de santé, possèdent des fonctionnalités spécifiques et gratuites. « MonSisra », messagerie sécurisée à destination des professionnels de santé pour la région Auvergne-Rhône Alpes, propose par exemple, un interfaçage à d'autres services de e-santé déployés dans la région sans avoir à ressaisir de mot de passe. Il existe aussi la messagerie sécurisée de santé nationale, la MSSanté.

Une solution pour augmenter le suivi des recommandations par les pharmaciens serait de les rendre opposables, mais cela risque de conduire les pharmaciens à limiter ces communications au strict minimum pour ne pas être sanctionnable.

5.4 Au-delà des recommandations

Les recommandations proposées par la CNIL et l'ordre des pharmaciens ne représentent pas le maximum de ce qui pourrait être fait en matière de sécurité informatique, car les rédacteurs de ces recommandations ont dû se limiter aux mesures les plus importantes.

Par exemple l'ANSSI recommande, dans le cas d'entreprise manipulant des données sensibles comme les pharmacies, de paramétrer Windows pour limiter les données envoyées à Microsoft.

5.5 Pistes de réflexions

En se basant sur les résultats du questionnaire, les pharmaciens d'officine peinent déjà à appliquer les recommandations actuelles. La sécurité informatique est un domaine à part entière en constante évolution. Elle demande temps et compétences à des utilisateurs certes professionnels, mais pour qui l'informatique n'est qu'un support. Il me semble peu réaliste aujourd'hui de demander aux pharmaciens d'officine d'assurer seuls la sécurité informatique des données personnelles des patients. Il faudrait donc réfléchir à des alternatives, permettant que la sécurité informatique des données de santés soit assurée par des professionnels de l'informatique. L'acteur de choix avec des compétences en informatique pour les pharmacies d'officine est le sous-traitant chargé de la maintenance informatique qui est souvent le fournisseur du LGO. On pourrait donc envisager de le rendre coresponsable de la sécurité des données-patients avec une obligation de moyens, la mise en place de ces moyens continuant à relever du pharmacien d'officine.

De manière plus générale, on pourrait envisager de contraindre les pharmacies à souscrire à une assurance sécurité informatique précisant le niveau de sécurité nécessaire et les prestataires agréés à le mettre en œuvre.

Et en dernier lieu, la solution la plus radicale consisterait à déposséder les pharmaciens des données de leurs patients en imposant l'hébergement des données de santé sur des serveurs dédiés et sécurisés en dehors de la pharmacie.

Déchargeant ainsi complètement le pharmacien de la responsabilité de la sécurité informatique des données, mais rendant dépendant de la connexion internet. Cette organisation conduirait à stocker de grande quantité de données de santé au même endroit, rendant les conséquences d'un piratage extrêmement graves.

Il est aussi intéressant de favoriser des outils assurant par défaut la sécurité informatique des données.

Deux exemples déjà en place qui pourraient servir de modèles pour les outils à fournir aux professionnels de santés sont le DP et la facturation sécurisée. Ces outils devraient être mis en avant, car ils remplissent leur fonction en assurant la traçabilité des soins de manière sécurisée et sans être conditionnés par les connaissances des utilisateurs. Les opérations assurant la confidentialité des données leur sont transparentes.

Une autre approche serait de contraindre les éditeurs de logiciels et de matériels informatiques à proposer des solutions matérielles et logicielles avec une configuration par défaut, assurant une sécurité informatique maximum : par exemple une version de Windows ne communiquant pas de donnée à Microsoft. Cette solution est déjà partiellement mise en place : Microsoft proposant par exemple un pare-feu, un antivirus et un logiciel de chiffrement par défaut. Mais la contrainte est limitée sur des entreprises hors France ou Europe.

Actuellement, ces entreprises n'ont pas d'obligation de transparence sur les failles qui sont découvertes dans les solutions qu'elles proposent. Il serait donc très utile d'instaurer une communication rapide, claire et régulière concernant les logiciels pour lesquels des failles pouvant compromettre des données de santé ont été mises à jour, par exemple via la « newsletter » de l'ANSM. Cette solution continue d'impliquer la vigilance du pharmacien ou de son sous-traitant en sécurité informatique.

La problématique commune à toutes ces solutions, au vu du coût que représente la décision de confier la sécurité des données patients à des professionnels de la sécurité informatique, ne peut reposer uniquement sur la bonne volonté des pharmaciens. Il faut leur fournir des incitations supplémentaires, soit en aidant à financer la protection des données, soit en créant des obligations légales sur les mesures à mettre en œuvre, soit une combinaison des deux.

6 Conclusion

THÈSE SOUTENUE PAR : François BETTEGA

TITRE :

LA SÉCURITÉ INFORMATIQUE DES DONNÉES PATIENT EN OFFICINE

CONCLUSION :

L'avènement de l'informatique et des réseaux a permis d'améliorer considérablement le soin en facilitant le partage d'informations entre professionnels de santé, puis en permettant le traitement de quantités de données de plus en plus importantes et provenant de sources différentes. Ainsi les organismes de sécurité sociale peuvent outre les contrôles connaître les consommations des assurés. L'informatique a aussi facilité la vie des patients notamment par exemple via le tiers payant. Ce changement rapide a généré des problématiques nouvelles. Par exemple, le fonctionnement d'un ordinateur ou d'internet est souvent mal connu de la plupart des professionnels de santé même quand ils en sont des utilisateurs quotidiens. Cela rend la mise en place de certains outils de protection difficile, en particulier ceux nécessitant un minimum de compréhension du domaine. L'informatique permet aussi, avec de petits moyens, d'analyser des données, quel que soit leur nombre et d'en retirer un profit substantiel. Il est donc absolument indispensable de mettre en place des moyens de protéger contre l'exploitation non consentie des données personnelles. La protection des données en générale est un sujet d'actualité, les grands géants d'internet se sont construits sur la publicité. Et au fur et à mesure elle est devenue 129 de plus en plus ciblée grâce à la collecte et à l'analyse de grande quantité de données. Depuis peu, les premiers scandales en rapport avec l'utilisation de données personnelles commencent à émerger. Par exemple, Grinder, application de rencontre, fournissait le statut VIH de ses utilisateurs à un de ses sous-traitants, sans que ceux-ci n'en soient informés. Ces scandales laissent présager une prise de conscience par la population de l'importance des données personnelles. Ce qui devrait conduire à une élévation des demandes en matière de protections de leurs données et à plus de transparence de la part des organismes les traitants. Depuis déjà plusieurs années, le gouvernement français et plus récemment l'Europe avec le RGPD construisent un cadre législatif pour garantir la sécurité de ces données personnelles. Les données de santé n'échappent pas à ce cadre et ont le statut particulier de données sensibles ne devant servir qu'à garantir la meilleure prise en charge des patients. Avec leur numérisation, la protection de ces données requiert de plus en plus de compétences qui échappent aux professionnels de santé alors qu'ils restent responsables de leur sécurité. Garantir la sécurité de données numériques nécessite la mise en place de nouveaux moyens, plus complexes comparés au support physique. La protection des données représente donc un coût temporel et financier important pour les pharmaciens d'officine sans qu'ils en retirent de bénéfice direct financier ou 130 d'image de la pharmacie, c'est un frein à la mise en place des mesures pouvant l'assurer. Ce sont ces éléments qui expliquent que malgré un cadre législatif et des recommandations, les mesures visant à assurer la protection des données de santé ne soient mises en place que faiblement en pharmacie d'officine selon le retour d'expérience recueilli par questionnaire. Ces problématiques liées à la protection des données numériques, au-delà de la pharmacie d'officine, s'étendent à l'ensemble du système de santé en ville et plus largement dans toutes les structures n'étant pas suffisamment grandes pour employer des professionnels de l'informatique. Une priorité serait donc d'identifier tous les professionnels stockant des données de santé en ville et de mettre en place des outils pour les former et les sensibiliser à l'absolue nécessité de mettre en pratique les mesures nécessaires à la protection de ces données. Face à l'utopie de croire que tous les professionnels de santé seront en mesure de se former pour garantir durablement et au gré des évolutions technologiques la sécurité des données de santé, une solution plus durable serait de confier leur protection à des professionnels de l'informatique qui pourront assurer un service de qualité dans la durée. Mais la mise en place de ce type de solution est très complexe à l'échelle de toutes les petites entités dont est constitué le système de santé en ville. Notamment une des questions est de savoir qui supportera le coût de 131 la mise en place et du maintien de toutes ces mesures de sécurité. Cette problématique est centrale pour présager de l'adhésion des professionnels impliqués. Il me semble par exemple illusoire de croire que, dans le modèle de rémunération actuel, les petites et moyennes officines seront en mesure de payer pour la sécurité de leur base de données-patient, déléguée à des organismes privés. Même si dans un avenir proche cette solution est mise en place, la sensibilisation et formation des professionnels de santé en matière de sécurité informatique reste primordiale dès l'université puis dans le cadre de la formation professionnelle continue, car un dispositif de sécurité efficace repose sur des utilisateurs conscients des problématiques de sécurité et de l'importance des mesures appliquées. Problématique actuelle, l'importance de la protection des données de santé devrait continuer à grossir à l'avenir, d'autant plus si un scandale sur l'exploitation de données de santé venait à se produire en France. Des outils comme le dossier pharmaceutique ou le DMP pourraient être refusés massivement

par les patients. Cela représenterait une perte majeure pour la santé publique. Il faut donc que les instances administratives continuent à se mobiliser pour trouver les solutions les plus efficaces possible, permettant à la fois à notre système de santé de bénéficier de tous les avantages qu'offre l'informatique sans pour autant prendre le risque de compromettre la vie privée de ses usagers.

VU ET PERMIS D'IMPRIMER
Grenoble, le : 22/10/18

LE DOYEN
DE L'UFR DE PHARMACIE

et par délégation
Le Doyen de Pharmacie
Pr. Michel SÈVE

Pr. Michel SÈVE

LE PRÉSIDENT DE LA THÈSE
JURY DE PHARMACIE

Pr. Pascal MOSSUZ

Faculté de Pharmacie,
Université Grenoble Alpes

Serment de Galien

« Je jure en présence des Maîtres de la Faculté, des Conseillers de l'Ordre des Pharmaciens et de mes condisciples :

D'honorer ceux qui m'ont instruit(e) dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle à leur enseignement.

D'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de l'honneur, de la probité et du désintéressement.

De ne jamais oublier ma responsabilité et mes devoirs envers le malade et sa dignité humaine ; en aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels.

Que les hommes m'accordent leur estime si je suis fidèle à mes promesses. Que je sois couvert(e) d'opprobre et méprisé(e) de mes confrères si j'y manque ».

Références

1. Lexique - Adresse MAC - Guide sécurité [Internet]. [cité 30 mai 2018]. Disponible sur : https://www.credit-agricole.fr/guidesecurite/Adresse-MAC.html

2. Authentification par mot de passe : les mesures de sécurité élémentaires | CNIL [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

3. Définitions : cryptage - Dictionnaire de français Larousse [Internet]. [cité 30 mai 2018]. Disponible sur: http://www.larousse.fr/dictionnaires/francais/cryptage/20841

4. fourche [Internet]. [cité 30 mai 2018]. Disponible sur: http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26529122

5. Larousse É. Définitions : formater - Dictionnaire de français Larousse [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/formater/34639

6. Graham LD. Legal Battles that Shaped the Computer Industry. Greenwood Publishing Group; 1999. 265 p.

7. gnu.org [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.gnu.org/philosophy/free-sw.fr.html

8. pb_cours.pdf [Internet]. [cité 30 mai 2018]. Disponible sur: http://iml.univ-mrs.fr/ati/cimpa/pb_cours.pdf

9. Universalis E. SYSTÈMES D'EXPLOITATION, informatique [Internet]. Encyclopædia Universalis. [cité 30 mai 2018]. Disponible sur: http://www.universalis.fr/encyclopedie/systemes-d-exploitation-informatique/

10. Qu'est-ce qu'un réseau de zombies (botnet en anglais) ? [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.microsoft.com/fr-fr/security/resources/botnet-whatis.aspx

11. Pare-feu [Internet]. [cité 30 mai 2018]. Disponible sur: http://www.berkeley-software.wikibis.com/pare-feu.php

12. Définition Routeur - Dictionnaire informatique [Internet]. Cours Informatique Gratuit. [cité 30 mai 2018]. Disponible sur: https://cours-informatique-gratuit.fr/dictionnaire/routeur/

13. Larousse É. Définitions : spam - Dictionnaire de français Larousse [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/spam/10910104

14. Larousse É. Encyclopédie Larousse en ligne - virus informatique [Internet]. [cité 30 mai 2018]. Disponible sur: http://www.larousse.fr/encyclopedie/divers/virus_informatique/186101

15. Larousse É. Définitions : wi-fi - Dictionnaire de français Larousse [Internet]. [cité 31 mai 2018]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/wi-fi/10910038

16. NP_WIFI_NoteTech.pdf [Internet]. [cité 30 mai 2018]. Disponible sur: https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_WIFI_NoteTech.pdf

17. Ces médecins accros à Snapchat ou Instagram [Internet]. Le Quotidien du Médecin. [cité 29 mai 2018]. Disponible sur: https://www.lequotidiendumedecin.fr/actualites/article/2017/09/23/ces-medecins-accros-snapchat-ou-instagram_850452

18. Devenir délégué à la protection des données | CNIL [Internet]. [cité 29 mai 2018]. Disponible sur: https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

19. RGPD INFO/INTOX [Internet]. FSPF. 2018 [cité 23 août 2018]. Disponible sur: http://www.fspf.fr/fspf-services/breves/rgpd-infointox

20. Décret no 92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés et modifiant le code de la santé publique (deuxième partie: Décrets en Conseil d'Etat).

21. Qu'est-ce que le DP ? - Le Dossier Pharmaceutique - Ordre National des Pharmaciens [Internet]. [cité 30 mai 2018]. Disponible sur: http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Qu-est-ce-que-le-DP

22. 2017-RA2016-+vDEF.pdf [Internet]. [cité 29 mai 2018]. Disponible sur: http://www.ordre.pharmacien.fr/content/download/389795/1858448/version/1/file/2017-RA2016-+vDEF.pdf

23. Dossier médical personnel: 500 millions d'euros pour 418.011 dossiers [Internet]. La Parisienne. 2014 [cité 29 mai 2018]. Disponible sur: http://www.leparisien.fr/laparisienne/sante/dossier-medical-personnel-500-millions-d-euros-pour-418-011-dossiers-04-01-2014-3461813.php

24. Mathieu-Fritz A, Esterle L. Les médecins et le dossier santé informatisé communiquant, Doctors and the electronic health record. Réseaux. 4 juill 2013;(178-179):246.

25. Code de la santé publique - Article R1110-2. Code de la santé publique.

26. Guide+Confidentialité+-+janvier+2013.pdf [Internet]. [cité 8 janv 2018]. Disponible sur: http://www.ordre.pharmacien.fr/content/download/75069/480084/version/6/file/Guide+Confidentialit%C3%A9+-+janvier+2013.pdf

27. brochure-la-demographie-+2018.pdf [Internet]. [cité 31 août 2018]. Disponible sur: http://www.ordre.pharmacien.fr/content/download/399974/1888607/version/1/file/brochure-la-demographie-+2018.pdf

28. Saumon L. Préparateurs, pharmaciens: si proches et pourtant si différents. :148.

29. Cambridge Analytica : 87 millions de comptes Facebook concernés. Le Monde.fr [Internet]. 4 avr 2018 [cité 29 mai 2018]; Disponible sur: https://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_4408996.html

30. Lab K. Étude sur l'impact financier de la sécurité informatique sur les entreprises [Internet]. [cité 3 mai 2018]. Disponible sur: https://www.kaspersky.fr/blog/etude-sur-limpact-financier-de-la-securite-informatique-sur-les-entreprises/6309/

31. Wikiwix's cache [Internet]. [cité 29 mai 2018]. Disponible sur: http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fwww.technewsworld.com%2Fstory%2F62825.html

32. Privacy Policy – Privacy & Terms – Google [Internet]. [cité 29 mai 2018]. Disponible sur: https://policies.google.com/privacy?hl=en

33. grindr-privacy-leaks: Report and raw data about privacy leaks in Grindr [Internet]. SINTEF-9012; 2018 [cité 31 mai 2018]. Disponible sur: https://github.com/SINTEF-9012/grindr-privacy-leaks

7 Annexe 1 Missions de la CNIL

Commission nationale de l'informatique et des libertés et conservation de données personnelles

En 1974, la révélation d'un projet du gouvernement visant à identifier chaque citoyen français par leur numéro d'inscription au répertoire des personnes physiques (numéro de sécurité sociale) et à interconnecter les fichiers administratifs français fit craindre un fichage général de la population. Cette inquiétude a abouti à la création de la commission « informatique et liberté » pour garantir que le développement de l'informatique se faisait dans le respect de la vie privée. La commission « informatique et liberté » proposa la création d'une autorité indépendante visant à poursuivre sa mission. Ce qui sera chose faite le 6 janvier 1978 via la loi relative à l'informatique, aux fichiers et aux libertés» qui créa la Commission Nationale de l'Informatique et des Libertés (CNIL). Ses 4 missions principales sont :

Informer / protéger : la CNIL informe les particuliers et les professionnels et répond à leurs demandes. Elle met à leur disposition des outils pratiques et pédagogiques et intervient très régulièrement pour animer des actions de formation et de sensibilisation, notamment dans le cadre de l'éducation au numérique. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits. Elle a pour mission de promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

Accompagner /conseiller : la régulation des données personnelles passe par différents instruments qui poursuivent tous un objectif de mise en conformité des organismes : avis sur des projets de loi ou de décret, autorisation pour les traitements les plus sensibles, recommandations fixant une doctrine, cadres

juridiques simplifiant les formalités préalables, réponse à des demandes de conseils. Elle certifie la conformité des processus d'anonymisation des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation.

Contrôler et sanctionner : le contrôle sur place, sur pièces, sur audition ou en ligne permet à la CNIL de vérifier la mise en œuvre concrète de la loi. Un programme des contrôles est élaboré en fonction des thèmes d'actualité, des grandes problématiques identifiées et des plaintes dont la CNIL est saisie.

Anticiper : dans le cadre de son activité d'innovation et de prospective, la CNIL met en place une veille pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée. Elle a pour mission de conduire une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies numériques.

8 Annexe 2 Loi informatique et liberté

1- **Un droit de regard** sur les données possédées et leur finalité défini dans l'article 39

« Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

1° la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ;

4° la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci »

2- **Un droit d'opposition** présenté dans l'article 38

« Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement. »

3- **Un droit de correction et de suppression** détaillé dans ces deux alinéas de l'article 40

« I. — Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiés, complétés, mis à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. [..]

II. — Sur demande de la personne concernée, le responsable du traitement est tenu

d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci. »

9 Annexe 3 Le questionnaire de l'étude

Quelle est votre fonction dans la pharmacie ?

- ○ Pharmacien titulaire
- ○ Pharmacien adjoint
- ○ Préparateur
- ○ Etudiant en pharmacie
- ○ Apprenti préparateur
- ○ autre

autre :

Quelle est la situation géographique de la pharmacie ?

- ○ Pharmacie de centre-ville
- ○ Pharmacie de quartier
- ○ Pharmacie en zone rurale

Quel est votre âge ?

18

18 75

Quel est votre sexe ?

- ○ Masculin
- ○ Féminin

Quel système d'exploitation utilisez-vous ?

- ☐ Windows
- ☐ Linux
- ☐ Mac OS
- ☐ Autre

Autre :

Quelle version de Windows utilisez-vous parmi les suivantes ?

- Windows 10
- Windows 8.1
- Windows 8.0
- Windows XP ou Vista service pack 2
- Windows 7
- Windows Vista Service pack 1
- Windows XP Service pack 1
- Une version antérieure 95, 98 et 98 SE, Millenium , 2000
- Je ne sais pas
- Autre

Autre :

Vous pouvez connaitre votre version de Windows en appuyant sur la touche Windows + R et en entrant winver

Utilisez-vous une version antérieure à la version Apple OS X 10.10 (Yosemite)

- oui
- non
- Je ne sais pas

Quel navigateur internet utilisez-vous ?

- Chrome
- Firefox
- Safari
- Opera
- Internet Explorer
- Microsoft Edge
- autre

autre :

Quelle est votre version d'internet explorer ?

- ○ Internet Explorer 11
- ○ Internet Explorer 9
- ○ autre

Parmi ces logiciels, pour lesquels contrôlez-vous la mise à jour ?

- ☐ Antivirus
- ☐ Navigateur internet
- ☐ Système exploitation
- ☐ Tous les logiciels de la pharmacie
- ☐ Je ne sais pas

Parmi ces mesures lesquelles sont mises en place pour sécuriser les postes de travail de la pharmacie ?

- ☐ un pare-feu
- ☐ Un antivirus sur un ou plusieurs postes
- ☐ Un antivirus sur chaque poste de travail
- ☐ Les sessions de travail sont-elles en mode administrateur (configuration de base sur Windows)
- ☐ Je ne sais pas

Pour la navigation internet utilisez-vous une session utilisateur ?

- ○ Oui
- ○ Non
- ○ je ne sais pas

Ces différentes actions nécessitent-t-elles un mot de passe ?

- ☐ L'allumage d'un poste de travail
- ☐ la sortie de veille d'un poste de travail
- ☐ aucun des 2
- ☐ je ne sais pas

Quel est le mode de fonctionnement de votre pharmacie, pour l'accès au logiciel de gestion d'officine

- ☐ Chaque employé s'identifie avant chaque opération
- ☐ Chaque employé s'identifie lors de sa première connexion quotidienne
- ☐ Chaque employé utilise un mot de passe qui lui est propre avant chaque opération
- ☐ Chaque employé utilise un mot de passe qui lui est propre uniquemement lors de sa première connexion quotidienne
- ☐ autre

autre :

Quel est le mode de fonctionnement de votre pharmacie en matière de politique de mot de passe ?

- ☐ Pour les mots de passe le nombre d'essai est limité
- ☐ Il existe des contraintes dans le choix du mot de passe (nombre de caractères, pas de mots courant ...)
- ☐ Un système de déconnexion automatique en cas d'inactivité est-il mis en place
- ☐ La date et l'heure de la dernière connexion au compte s'affiche lors de la connexion

Concernant le système de traçabilité

- ○ Il n'y a pas de journal des traces
- ○ Il existe un journal des traces
- ○ je ne sais pas

Un journal des traces conserve l'identifiant de celui qui intervient sur les données

A propos de votre journal des traces

- ☐ Le journal des traces conserve une trace des consultations
- ☐ Le journal des traces conserve une trace des modifications
- ☐ Le journal des traces conserve une trace des suppressions
- ☐ Le journal des traces conserve une trace des connections
- ☐ Le journal des traces conserve une trace des opérations de maintenance
- ☐ Le journal des traces contient les dates et heures des actions effectuées

Politique d'habilitation : dans votre logiciel de gestion d'officine certaines fonctionnalités (la caisse par exemple) ou données ne sont accessibles qu'avec un mot de passe ?

- ○ Oui
- ○ Non
- ○ Je ne sais pas

Pour lesquelles ?

- [ ] Les sauvegardes
- [ ] L'historique du patient
- [ ] La caisse
- [ ] Les transmissions avec les organismes de sécurité sociale
- [ ] Le journal des traces
- [ ] Autres

Autres :

Formation et contrat : parmi ces mesures lesquelles appliquez-vous ?

- [ ] Les employés non professionnels de santé signent une charte de confidentialité
- [ ] Vous avez une charte informatique
- [ ] Les employés de la pharmacie ont suivi une ou plusieurs formations informatiques ?
- [ ] Aucune de ces mesures

Quelles données sensibles sont chiffrées ?

- [ ] L'ensemble des données contenues dans le logiciel de gestion d'officine
- [ ] L'ensemble de vos sauvegardes et archives
- [ ] Je ne sais pas
- [ ] Autre

Autre :

Connaissez-vous le logiciel de cryptage et l'algorithme qui sont utilisés ?

- ( ) Non
- ( ) Oui, pouvez vous préciser

Oui, pouvez vous préciser :

Des sauvegardes sont-elles effectuées?

- ( ) Oui
- ( ) Non
- ( ) Je ne sais pas

Sauvegardes :
parmi ces mesures lesquelles appliquez-vous

- [ ] Vous utilisez plusieurs périphériques distincts pour les sauvegardes (par exemple une clef USB pour les jour pairs une pour les impairs)
- [ ] Les sauvegardes sont stockées dans un lieu physique distinct des postes de travail
- [ ] Vous avez une sauvegarde de votre logiciel de gestion d'officine et des logiciels indispensables au fonctionnement de l'officine
- [ ] Vous avez déjà effectué un test de vos sauvegardes
- [ ] Vous organisez des purges de vos données informatiques quand elles dépassent la durée limite d'archivage
- [ ] Aucune de ces mesures
- [ ] Je ne sais pas

Lors d'un changement de matériel informatique contenant des données sensibles (ordonnances, historiques de patient ...) une procédure particulière est-elle prévue pour sa destruction ?

- [ ] Oui, une procédure à l'intérieur de la pharmacie est prévue
- [ ] Oui, la pharmacie fait appel à un sous-traitant
- [ ] Non
- [ ] Je ne sais pas

La destruction est effectuée par le pharmacien pour les supports suivant :

- [ ] Disque dur
- [ ] CD/DVD
- [ ] Clef USB
- [ ] je ne sais pas
- [ ] Autre

Autre :

Destruction de disque dur ou de clef USB

- ( ) Vous jetez le disque à la poubelle sans autre opération
- ( ) Vous effectuez un formatage avant de jeter le disque
- ( ) Vous utilisez un logiciel agréé pour l'effacement des données
- ( ) Je ne sais pas
- ( ) Autre

Autre :

Destruction de CD et / ou DVD

- ○ Vous les jetez simplement à la poubelle
- ○ Vous utilisez une broyeuse
- ○ Je ne sais pas
- ○ Autre

Autre :

Dans le cadre de votre exercice professionnel, utilisez-vous des périphériques mobiles autres que des CD, clefs USB ou disque dur pour les sauvegardes comme un ordinateur portable, un smartphone ou une tablette ?

- ○ Oui
- ○ Non
- ○ Je ne sais pas

Périphériques mobiles : quelles sont les propositions qui s'appliquent à votre officine ?

- ☐ Sont-ils verrouillés par un mot de passe ?
- ☐ Sont-ils verrouillés par une authentification forte* ?
- ☐ Sont-ils connectés à internet ou au réseau local ?
- ☐ Possèdent-ils des applications non indispensables à l'usage professionnel ?
- ☐ je ne sais pas

**authentification forte : un mot de passe couplé à un support physique : carte à puce, empreinte digitale...*

Quelles clauses prévoit votre contrat de maintenance ?

- ☐ Aucune intervention ne sera faite sans l'accord préalable du pharmacien
- ☐ Les employés chargés de la maintenance ont tous signé une clause de confidentialité
- ☐ Toutes les données transmises à l'organisme de maintenance sont chiffrées
- ☐ La société responsable de la maintenance vous communique un rapport après chaque opération
- ☐ Je ne sais pas

Lors d'une télé-maintenance

- [ ] Vous pouvez voir quand l'opération débute et finit
- [ ] Vous avez une action à effectuer avant que la maintenance puisse débuter (transmettre une séquence de chiffre ou de lettre ou cliquer sur une fenêtre)
- [ ] je ne sais pas
- [ ] Le logiciel de télémaintenance est contrôlé concernant l'existence de failles majeures (par exemple certification de premier niveau par ANSII)

Sur quel(s) périphérique(s) les identifiants par défaut (fournis par l'installateur lors de leur configuration) ont-ils été modifiés ?

- [ ] Routeur (box internet)
- [ ] Fax/Imprimante/Scanner
- [ ] Caméra
- [ ] je ne sais pas
- [ ] Aucun
- [ ] autre

autre :

Le wifi est-il activé sur la box de la pharmacie ?

- ○ Oui
- ○ Non
- ○ Je n'ai pas connaissance que la configuration initiale soit changée
- ○ Je ne sais pas

Le wifi est-il nécessaire au bon fonctionnement de la pharmacie ?

- ○ oui
- ○ non
- ○ je ne sais pas

Comment se connecte-t-on au wifi ?

- [ ] En entrant une clef de sécurité
- [ ] En appuyant sur un bouton présent sur le routeur (la box internet)
- [ ] Je ne sais pas

Type de clef Wifi

- ○ Clef WEP
- ○ Clef WPA
- ○ je ne sais pas
- ○ Autre

Autre :

Savez vous si le réseau de la pharmacie est segmenté en VLAN (virtual Local Area Network) ?

- ○ Oui
- ○ Non
- ○ Je ne sais pas

Pour vos communications interprofessionnelles, par quels canaux communiquez vous ?

- ☐ Mail
- ☐ Téléphone
- ☐ Fax
- ☐ Autres

Autres :

Mail, utilisez-vous

- ☐ Une boite mail conventionnelle (Gmail,orange,ou autre)
- ☐ Un système de messagerie sécurisé
- ☐ Un système de messagerie sécurisé pour professionnel de santé (ZEPRA , MSSanté ....)
- ☐ autres

autres :

Fax

- ☐ Tous les numéros utilisés pour les transmissions de données de santé sont-il pré-enregistrés
- ☐ Vous envoyez des copies papier en plus de l'envoi de fax
- ☐ Aucun
- ☐ Autre

Autre :

Utilisez vous une application mobile pour recevoir des ordonnances patients ou pour vos communications interprofessionnelles ? Si oui la(les)quelle(s)

A propos de sécurité informatique :

- [ ] Vous considérez que la sécurité informatique des données-patient soit de la responsabilité des pharmaciens
- [ ] Vous avez lu les recommandation d'organismes gouvernementaux ou de l'ordre des pharmaciens à ce sujet
- [ ] Vous pensez être suffisamment formé en matière de sécurité informatique
- [ ] Vous pensez que la sécurité informatique des données de santé devrait être assurée par les fournisseurs de logiciels à destination des officines
- [ ] Un correspondant informatique et liberté a été nommé au sein de votre équipe

10 Annexe 4 Auto questionnaire de l'ordre des pharmaciens

Mise en œuvre d'une politique de protection de l'information	> Mettre en œuvre une politique de sécurité informatique	☐
	> Informer les patients sur le recueil et le traitement de leurs données à caractère personnel	☐
	> Respecter le secret professionnel	☐
	> Former et informer les utilisateurs	☐
Évaluation des risques spécifiques aux données de santé	> Identifier les fichiers de données à caractère personnel	☐
	> Identifier les types de traitements de ces fichiers et y associer les risques pouvant impacter la vie privée	☐
	> Mettre en œuvre les mesures de sécurité adaptées aux risques	☐
Protection des locaux	> Limiter les accès	☐
	> Mettre en place un système anti-intrusion	☐
Sécurisation des postes de travail	> Mettre en place un système de verrouillage automatique des sessions ouvertes	☐
	> Bloquer l'accès après un nombre défini de tentatives infructueuses	☐
	> Utiliser un pare-feu	☐
	> Utiliser un anti-virus	☐
Sécurisation du réseau interne	> Limiter les flux réseau	☐
	> Cloisonner le réseau, segmenter en réseaux virtuels	☐
Sécurisation des serveurs	> Instaurer impérativement une politique de mots de passe	☐
	> Faire les mises à jour critiques sans délai	☐
	> S'assurer de la disponibilité des données	☐
Sécurisation de l'informatique mobile	> Prévoir le chiffrement ou le cryptage des données pour les ordinateurs portables et les unités de stockage amovibles	☐
	> Utiliser le protocole WPA pour les réseaux Wi-Fi	☐
Authentification des utilisateurs	> Attribuer un identifiant ou un login à chaque utilisateur	☐
	> Utiliser des mots de passe avec rigueur	☐
	> Changer le mot de passe après réinitialisation	☐
Gestion des habilitations	> Établir des profils d'habilitation en fonction des missions des utilisateurs	☐
	> Supprimer les accès des utilisateurs partis ou absents	☐
Encadrement de la maintenance	> Tracer les interventions	☐
	> Autoriser les interventions	☐
	> Prévoir une clause de confidentialité	☐
Encadrement de la sous-traitance	> Prévoir une clause de confidentialité	☐
	> Prévoir les conditions de restitution et de destruction des données en fin de contrat	☐
Sécurisation des transmissions	> Utiliser des méthodes de chiffrement ou de cryptage des données	☐
	> S'assurer de la transmission au bon destinataire	☐
Sauvegarde	> Faire des sauvegardes régulières	☐
	> Utiliser des supports préservant l'intégrité des données	☐
	> Tester régulièrement la restitution des données à partir des sauvegardes pour préserver la continuité d'activité	☐
	> Sécuriser les lieux de conservation des sauvegardes	☐
Archivage	> Sécuriser les archivages	☐
	> Définir les accès autorisés par la politique d'habilitation	☐
	> Détruire les archives après la période obligatoire de conservation	☐
Destruction	> Respecter les durées de conservation légales	☐
	> Utiliser des méthodes d'effacement efficaces ou des méthodes de destruction physique des supports	☐
	> Prévoir une clause avec les sous-traitants ou les SSII garantissant l'absence totale de données à caractère personnel sur les supports restitués ou détruits	☐
Traçabilité	> Mettre en œuvre un système de journalisation	☐
	> Informer les utilisateurs de la mise en œuvre d'un système de journalisation	☐
	> Informer les personnes concernées des accès frauduleux à leurs données	☐