Ordre national des pharmaciens

RECOMMANDATIONS

Respect de la confidentialité des données de patients

dans l'usage de l'informatique

Sommaire

La sécurité du système d'information

ASPECTS THÉORIQUES — 1ÈRE PARTIE

La sécurité du système d'information

ASPECTS PRATIQUES — 2ÈME PARTIE

Lettre de mission 1/2

CONSEIL NATIONAL
DE L'ORDRE DES PHARMACIENS

La Présidente

Madame Catherine GONZALEZ

26 rue Bonfa
30 000 NIMES

Paris, le 25 octobre 2010

IA/ac

Chère collègue,

L'utilisation de l'informatique devient quotidienne dans le domaine de la santé.

Les pharmaciens ont été parmi les précurseurs en la matière. Au début, simple outil de facturation, l'informatique a ensuite pris une place prépondérante dans la gestion des commandes, entre métiers de la distribution et de la dispensation. Puis, les sociétés informatiques spécialisées dans les différents métiers ont développé des modules pour accompagner les professionnels dans leur exercice pharmaceutique ou médical (biologistes).

Des registres sont ainsi tenus par informatique, des dossiers patients sont archivés sur les disques durs etc. Au fil du temps, grâce au développement fulgurant des technologies de communication, les pharmaciens ont réalisé diverses « télétransmissions ».

Demain, « télémédecine » et coopération entre professionnels de santé, sujets largement abordés dans la loi « droits des malades » de 2004, puis à nouveau dans la loi de 2009, « Hôpital, Patients, Santé, Territoires », seront réalité. Le Dossier Pharmaceutique en est un des exemples et le Dossier Médical Personnel devrait être prochainement déployé. Les courriels devraient peu à peu remplacer pour partie les fax et les appels téléphoniques.

Pour autant, si l'on ne peut que se féliciter de l'utilisation de l'informatique et des technologies de communication qui favorisent la coopération entre professionnels, reste une question majeure qui me semble actuellement insuffisamment traitée : le respect de la confidentialité des données.

Pour exemple, l'usage interne de codes d'accès à l'informatique n'est pas utilisé dans toutes les entreprises ; les maintenances des logiciels font appel à des techniciens qui à distance ont une vue sur tout ou partie des données, y compris celles des patients ; des disques durs sont « remisés » sans destruction préalable des données patients ; des télétransmissions sont effectuées avec des sociétés non pharmaceutiques pour gérer la liquidation des dossiers de tiers payant etc.

Parmi ses missions, l'Ordre National des Pharmaciens, garant de l'éthique professionnelle, a pour objet de veiller à la compétence des pharmaciens et de contribuer à promouvoir la santé publique et la qualité des soins notamment la sécurité des actes professionnels. Aussi, il me semble pertinent qu'il contribue à la réalisation de recommandations sur le thème : « usage de l'informatique et respect de la confidentialité des données de patients ».

4, avenue Ruysdaël 75379 Paris Cedex 08
Téléphone : 01.56.21.34.04 - Fax : 01.56.21.34.79 – Email : iadenot@ordre.pharmacien.fr

Lettre de mission 2/2

J'ai souhaité vous confier la direction de ces travaux et vous remercie de l'avoir acceptée.

Vos travaux ne porteront ni sur les échanges de données de santé, sujets traités par la HAS (recommandations pour la permanence des soins), l'ASIP (référentiels portant sur l'authentification des PS par carte CPS et sur l'utilisation des messageries) ou l'Ordre (obligations mises en œuvre pour le DP), ni sur le respect de la confidentialité des données des patients de manière plus large (utilisation des fax, etc.). Vos travaux se centreront sur le respect de la confidentialité des données au regard de l'utilisation informatique au sein des structures pharmaceutiques et tiendront compte pour l'officine, de la charte écrite par l'ordre sur les logiciels de dispensation. Ils concerneront tous les métiers pharmaceutiques qui traitent des données de santé des patients. Ils pourront avantageusement proposer aux professionnels concernés des méthodes d'auto évaluation.

Pour établir ces recommandations, vous utiliserez la méthodologie, proche des pratiques de la HAS, et mises en oeuvre par Xavier DESMAS pour les « recommandations » dont il a la charge. Votre groupe de travail et votre groupe de relecture, devront comprendre des pharmaciens de toutes les sections ordinales concernées, des pharmaciens d'autres instances (syndicats, groupements, organismes de formation…), et toute personne dont vous jugeriez la compétence utile à vos travaux (sociétés informatiques, sociétés de gestion des tiers payants …). La Direction des Technologies en Santé, ainsi que la commission en regard de cette direction, présidée par Patrick FORTUIT, seront concernées par vos travaux.

S'agissant de recommandations portant sur l'exercice professionnel, la Direction de l'Exercice Professionnel sera votre soutien pour les questions logistiques.

Afin de limiter les coûts pour notre Ordre, seuls les membres ordinaux pourront bénéficier de la prise en charge de leurs frais de déplacement et d'indemnisation. Vous privilégierez autant que possible, les échanges par mail ou par réunions téléphoniques.

Je vous demanderai de bien vouloir me rendre compte régulièrement de la progression de vos travaux, pour une finalisation dans le courant du dernier trimestre 2011.

En vous remerciant de votre engagement pour la bonne fin de ces travaux essentiels pour l'avenir de la profession, je vous prie de croire, Chère collègue, à l'expression de mes salutations confraternelles.

Isabelle ADENOT

Copie : **Membres du Conseil national**
Présidents des Conseils centraux
Directions des Services communs

4, avenue Ruysdaël 75379 Paris Cedex 08
Téléphone : 01.56.21.34.84 - Fax : 01.56.21.34.79 – Email : iadenot@ordre.pharmacien.fr

Introduction

Règle d'éthique essentielle, le secret professionnel est au fondement même de la relation patient-professionnel de santé.
Le pharmacien est ainsi dans l'obligation de garantir la confidentialité des informations médicales qu'il détient et auxquelles il a accès. Illustrée par le serment d'Hippocrate dès le IVe siècle avant J.-C , *« Admis a l'intérieur des maisons, mes yeux ne verront pas ce qu'il s'y passe, ma langue taira les secrets qui me seront confiés »*, cette exigence est aujourd'hui formellement posée par le Code de déontologie des pharmaciens. La garantie de la confidentialité des données de santé doit se traduire par le respect de normes ou standards définis pour encadrer les actions portant sur la conservation et le traitement de ces données.
Le développement des systèmes d'information et l'essor de la technologie multiplient la complexité du respect de cette confidentialité, rendant nécessaire la reconnaissance des droits du malade et une prise de conscience collective.

Pris en application de l'article L.1110-4 du Code de la santé publique et de l'article L.161-36-1 du Code de la sécurité sociale, le décret n°2007-960 du 15 mai 2007 *« relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique »* en définit les modalités. Le *« respect de référentiels définis par arrêtés du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés »* s'impose ainsi à tout professionnel, tout établissement, tout réseau de santé ou tout autre organisme intervenant dans le système de santé.
Ces dispositions s'appliquent pour la conservation sur support informatique et la transmission par voie électronique des informations médicales.

Partie intégrante des systèmes d'information (SI) et des technologies de communication, l'informatique relève du quotidien de tous les pharmaciens, qu'ils exercent en officine, laboratoire de biologie médicale, établissement de santé ou encore en industrie des produits de santé. Au sein d'une organisation, le système d'information constitue un ensemble de ressources (matériels, logiciels, personnel, données et procédures) permettant de collecter, de stocker puis de traiter et communiquer les informations. Fortement impliqué dans l'utilisation des systèmes et technologies d'information, le pharmacien doit en

Introduction *(suite)*

- assurer la sécurité afin de protéger la confidentialité des données de patients.

En raison de la spécificité et de la complexité de cette démarche sécuritaire, il apparaît essentiel que les pharmaciens, tous profondément attachés au secret professionnel, soient soutenus dans sa mise en œuvre. Ainsi, ces recommandations sur le thème « Respect de la confidentialité des données de patients dans l'usage de l'informatique » proposent t'elles la synthèse des bases juridiques existantes. Elles ont pour vocation de permettre aux pharmaciens, tous secteurs d'activités confondus, d'aller à l'essentiel de la pratique. Pour autant, elles n'ont pas pour objectif de traiter des échanges de données de santé ou de l'utilisation des messageries et des télécopieurs.

Le respect de la confidentialité passant essentiellement par la sécurité du système informatique, les pharmaciens et les Sociétés de services en ingénierie informatique (SSII) doivent travailler de concert pour optimiser cette sécurité tout en la simplifiant au maximum sur le plan pratique..

L'essor des nouvelles technologies et l'évolution rapide des systèmes d'information qui en découle, soulèvent fréquemment des problématiques qui n'ont pas été anticipées par le législateur. Les situations exposées dans ce document et les recommandations qui en résultent ne peuvent dès lors être exhaustives. Elles sont ainsi susceptibles de paraître insuffisantes aux yeux des professionnels des systèmes d'information.

À l'inverse, les solutions apportées pourront sembler contraignantes pour les pharmaciens.

Pour cette raison, ces recommandations forment un support théorique et pratique élémentaire, pour chaque ressource et à chaque étape du traitement des données à caractère personnel. Apportant aux pharmaciens des conseils de base et des mises en garde essentielles, elles proposent une méthode simple de mise en œuvre et d'évaluation de la sécurité de leur système informatique.

1ÈRE PARTIE

La sécurité du système d'information

Aspects théoriques

Préambule

La France fût l'un des premiers pays européens à se doter d'une loi relative à la protection des données à caractère personnel[1], la Loi Informatique et Libertés (LIL) qui a pu servir de modèle en Europe[2].

Elle dispose de nombreuses institutions, organismes ou autorités administratives indépendantes qui sont en charge de la protection des données de santé, ou qui ont pour mission d'évaluer et d'expertiser les systèmes d'information, parmi lesquels : la Commission nationale de l'informatique et des libertés (CNIL), le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS), l'Agence des systèmes d'information partagés de santé (ASIP Santé), l'Institut des données de santé (IDS), les Comités de protection des personnes (CPP), le Conseil national de l'information statistique (CNIS), la Commission d'accès aux documents administratifs (CADA), l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP), etc.

Enfin, le conseil d'administration de l'ASIP Santé a créé un conseil d'éthique et de déontologie, qui a pour vocation d'émettre des avis et recommandations sur les projets mis en œuvre par l'ASIP Santé dans le respect de la protection des données de santé à caractère personnel.

NOTES

(1) LIL : loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004. (2) Convention européenne du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et Directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données personnelles.

1 Données à caractère personnel

Les données à caractère personnel, définies dans la LIL[3] se rapportent à une personne physique et permettent son identification directement ou indirectement.
On peut citer à titre d'exemple le nom, la date de naissance, l'adresse et le numéro de sécurité sociale. La définition couvre toutefois un champ plus vaste et englobe également, les adresses électroniques et le numéro de téléphone professionnel.

Données sensibles

Les opinions politiques, syndicales, religieuses, les origines ethniques ou raciales sont considérées comme des données sensibles[4].
Bien que leur traitement soit en principe interdit, la loi prévoit pour des raisons pratiques évidentes certaines dérogations limitativement énumérées[4] devant faire l'objet d'une protection renforcée.
Les données bancaires sont également des données sensibles.

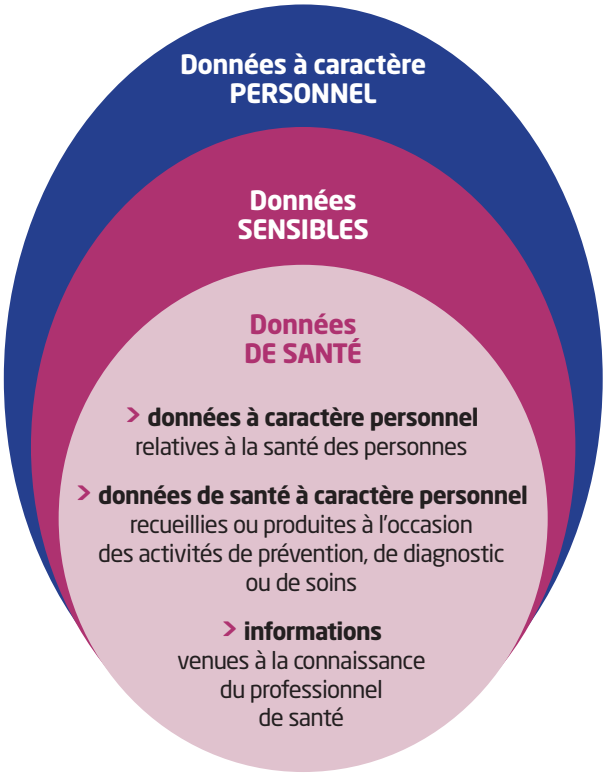
Données de santé

Les données de santé sont considérées comme des « données sensibles »[4][5].
Pour les données de santé, on peut citer :

- Les « données à caractère personnel (...) qui sont relatives à la santé des personnes »[4].
- Les « données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins »[6].
- « L'ensemble des informations concernant la personne, venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes »[7].

Une prescription de médicaments ou des résultats d'analyses médicales sont des exemples de données de santé.

Les données de santé : des données a caractère personnel



NOTES

(3) LIL - article 2 . (4) LIL - article 8. (5) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. (6) Code de la santé publique - article L.1111-8. (7) Code de la santé publique - article L.1110-4.

2 Traitement des données à caractère personnel

2.1 DÉFINITION

Le « traitement de données à caractère personnel » est défini comme « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé »[8].

Ces opérations concernent la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

2.2 CONDITIONS DE MISE EN ŒUVRE D'UN TRAITEMENT

Elles découlent des principes à respecter définis dans la LIL :

- Principe de finalité,
- Principe de pertinence,
- Principe d'une durée limitée de conservation,
- Principe de sécurité et de confidentialité,
- Principe du respect du droit des personnes (cf. chapitre 4 paragraphe 4.1).

2.2.1 Conditions liées à la collecte

- Les données « sont collectées et traitées de manière licite et loyale »[9],
- Les données « sont collectées pour des finalités déterminées, explicites et légitimes»[10].

2.2.2 Conditions relatives aux données

- Les données sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement »[11],
- Seules peuvent être collectées des « données exactes, complètes et, si nécessaire, mises à jour »[12],
- Les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »[13]. Cette durée sera précisée dans la demande d'autorisation ou dans la déclaration à la CNIL qui statuera sur ce point. Tout traitement de données personnelles doit donc prévoir, dès sa conception, les modalités de leur suppression: c'est le « droit à l'oubli ».

À RETENIR

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

- Respecter le principe de finalité et de proportionnalité en limitant le traitement à l'utilisation des données pour lesquelles il existe un rapport direct avec sa finalité
- Conserver les données pendant une durée dépendante de la finalité du traitement
- Collecter des données exactes et complètes

NOTES

(8) LIL - article 2, alinéa 3. (9) LIL - article 6, alinéa 1. (10) LIL - article 6, alinéa 2. (11) LIL - article 6, alinéa 3. (12) LIL - article 6, alinéa 4. (13) LIL - article 6, alinéa 5.

3 Responsabilité

Le responsable du traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens[14].
Il lui appartient de garantir le respect de la confidentialité et de la sécurité des données à caractère personnel.
Le responsable de la sécurité du système d'information gère les habilitations.

Cependant, au delà du responsable désigné de la sécurité du système d'information, les utilisateurs ont eux aussi leur part de responsabilité. Des recommandations dans le règlement intérieur et éventuellement la signature d'une charte précisant les droits et les devoirs de chacun semblent nécessaires.

Toute collecte ou traitement de données à caractère personnel nécessite une démarche auprès de la CNIL par le responsable des traitements des données.

Tableau simplifié des démarches à entreprendre auprès de la CNIL en fonction du secteur d'activité :

Pharmacie d'officine	> Norme simplifiée N°52
Laboratoire de biologie médicale	> Norme simplifiée N°53
Établissement de santé	> Déclaration normale
Entreprises ou exploitants de médicaments	> Autorisation unique N°13
Prestataire de services de santé à domicile et distributeur de matériels	> Déclaration normale

La déclaration initiale à la CNIL reste valable tant que le fichier n'a fait l'objet d'aucune modification substantielle portant notamment sur l'identité du responsable du traitement, la finalité, la catégorie de données enregistrées, les destinataires, etc.

3.1 PHARMACIE D'OFFICINE

Le pharmacien d'officine, qu'il soit gérant ou associé, est responsable des traitements des données à caractère personnel mis en œuvre au sein de son officine à des fins de gestion de la pharmacie et d'analyse statistique des ventes de médicaments, produits de santé et dispositifs médicaux. Ces données à caractère personnel ne doivent en aucun cas être exploitées à des fins commerciales[15].

Dans les officines, l'affichage du document de la CNIL intitulé « Traitement de fichiers informatiques » et disponible sur le site Internet de l'ordre, est obligatoire. ● ● ●

NOTES

(14) LIL - article 3-I. (15) CNIL - Délibération n°2006-161 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie.

3.2 LABORATOIRE DE BIOLOGIE MÉDICALE

Le biologiste médical est entièrement responsable du système d'information nécessaire à son exercice, et cela est précisé depuis fort longtemps, notamment dans le Guide de Bonne Exécution des Analyses de biologie médicale[16] :

- **Informatique :** obligation de déclaration à la CNIL, obligation de confidentialité, gestion des pannes informatiques, règles d'accès aux personnels autorisés, protection contre des accès non autorisés, traçabilité des modifications de programme informatique. Il est précisé également que « Le responsable du laboratoire ou l'établissement dont il dépend doit passer une convention avec l'organisme chargé de la maintenance du système informatique ».
- **Transmission des résultats :** notamment par voie électronique, « le biologiste doit utiliser un système de transmission fiable qui garantit la conformité des résultats transmis et le respect du secret professionnel ».
- **L'annexe D XI traite de la « sécurisation du transfert des données immuno-hématologiques vers le site de distribution » :** elle introduit notamment la nécessité de chiffrement des données « lorsque celles-ci doivent transiter sur un réseau ouvert » et « sur un réseau interne sur lequel peut se connecter du personnel non médical et non paramédical ».

Les démarches à entreprendre auprès de la CNIL pour les traitements informatisés de données à caractère personnel sont :

- Une déclaration simplifiée sous forme de « Norme Simplifiée » NS N° 53[17].
- Une demande d'autorisation dans le cadre d'un partage de données à caractère personnel ou de traitements ayant pour objet l'interconnexion de fichiers différents[18].

Dans le cas d'une externalisation des données, le recours à un hébergeur agréé est obligatoire.
Les laboratoires sont soumis à l'obligation prochaine d'accréditation, principalement selon la norme NF EN ISO 15189. Dans sa dernière version parue, les systèmes d'information font l'objet de mentions particulières. Cette norme précise bien l'implication obligatoire du biologiste dans la sécurité du fonctionnement général de son système d'information, dont les limites sont par ailleurs bien définies.
Un projet de décret va permettre aux laboratoires de biologie médicale d'adopter un même modèle de compte rendu structuré. Le Comité français d'accréditation (COFRAC) intègre déjà ces évolutions dans ses référentiels d'accréditation.

3.3 ÉTABLISSEMENT DE SANTÉ

Dans les établissements de santé, la direction est responsable de la sécurité de son système d'information[19]. Les établissements de santé doivent s'inscrire dans la démarche de certification pour la « sécurité du système d'information »[20]. Ils mettent en place un organe de management de la sécurité afin d'intégrer systématiquement dans toute démarche d'installation d'un système d'information, de mises à jour, d'intervention extérieure, d'interfaces, les moyens les plus efficaces ainsi que les clauses afférentes afin d'assurer la sécurité informatique dans toutes ses dimensions. Vis-à-vis d'un intervenant extérieur, il doit être signé un document d'engagement de confidentialité opposable juridiquement.

Des textes régissent les dispositifs de sécurité des systèmes d'information à mettre en place et leur gouvernance : la NORME ISO 27001 qui définit le système de gestion de la sécurité des systèmes d'information (SGSSI), les consignes du correspondant ministériel

NOTES

(16) Arrêté du 26 avril 2002 modifiant l'arrêté du 26 novembre 1999 relatif à la bonne exécution des analyses de biologie médicale. (17) CNIL - Délibération n° 2006-162 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les biologistes à des fins de gestion du laboratoire d'analyses de biologie médicale. (18) LIL - article 25. (19) Arrêté du 6 avril 2011 relatif au management de la qualité de la prise en charge médicamenteuse et aux médicaments dans les établissements de santé - article 7. (20) HAS, guide pratique « préparer et conduire votre démarche de certification » V2010, révisé 2012.

(haut fonctionnaire de défense et de sécurité), le référentiel de certification des établissements de santé, les recommandations de la CNIL[21][22].

Au sein de chaque établissement de santé, le comité de pilotage composé du Directeur de l'établissement, de la Commission médicale d'établissement (CME), du Directeur du système d'information, du responsable du Comité Opérationnel de la Sécurité du Système d'Information (COSSI), élabore la PMSSI (la politique de management de la sécurité du système d'information). Il existe au sein des établissements de santé, un organigramme des responsabilités en matière de traitements de données à caractère personnel.

Les traitements mis en place par le promoteur au cours d'études cliniques ne comportent pas l'identité complète du patient et ne constituent donc pas un traitement de données anonymisées au sens de la LIL. Les données ainsi codées sont considérées comme étant indirectement nominatives puisque l'investigateur est en mesure d'identifier les personnes concernées. Ainsi, les traitements de données sur des personnes, doivent faire l'objet d'un avis du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé et doivent être suivis d'une autorisation de la CNIL.

Au sein du Département d'information médicale (DIM), les données sont anonymisées; l'établissement de santé transmet des fichiers de données anonymisées à l'Agence Régionale de santé (ARS) et à la Caisse Régionale d'Assurance Maladie (CRAM) qui permet de mesurer l'activité médicale de l'établissement.

3.4 INDUSTRIE DES PRODUITS DE SANTÉ

3.4.1 Vigilances des produits de santé

Toute entreprise ou organisme exploitant un produit de santé doit mettre en œuvre un système de vigilances (pharmacovigilance, matériovigilance, etc....) dans le but d'assurer le recueil, l'enregistrement et l'évaluation des informations relatives aux effets indésirables susceptibles d'être dus à l'utilisation de ces produits de santé.
À titre d'exemple, le service de pharmacovigilance est placé sous la responsabilité d'un médecin ou d'un pharmacien justifiant d'une expérience dans ce domaine.
Le responsable de pharmacovigilance doit veiller au respect des obligations de déclaration de pharmacovigilance auprès de l'ANSM. En effet, « toute entreprise ou tout organisme exploitant un médicament ou produit mentionné à l'article R. 5121-150 est tenu de conserver des informations détaillées relatives à tous les effets indésirables survenus à l'intérieur ou à l'extérieur de la Communauté européenne, et susceptibles d'être dus à ce médicament ou produit »[23].
Ainsi, les traitements de pharmacovigilance mis en œuvre doivent faire l'objet d'une autorisation auprès de la CNIL : Autorisation Unique n°13.

3.4.2 Recherches biomédicales

En application des dispositions de la LIL, la CNIL a homologué par décision du 5 janvier 2006 une méthodologie de référence pour les traitements de données à caractère personnel contenues ou appelées à figurer dans des fichiers réalisés dans le cadre des recherches biomédicales (MR 001).
Cette méthodologie de référence a pour but de simplifier les modalités de déclaration à la CNIL des fichiers nécessaires à la conduite des recherches biomédicales.
Elle définit la nature des données collectées et les modalités de conduite et d'analyse de ces études.
Les traitements mis en œuvre dans le cadre des recherches biomédicales conformes aux dispositions de la méthodologie de référence MR 001, font uniquement l'objet d'un engagement de conformité adressé à la CNIL.

NOTES

(21) CNIL - Le guide de la sécurité des données personnelles, édition 2010 . (22) CNIL - Guide Professionnels de santé, édition 2011 (23) Code de la santé publique - article R.5121-172.

3.4.3 Fichiers commerciaux

Les données à caractère personnel et plus particulièrement les données de santé (même rendues anonymes à l'égard des patients) ne peuvent pas être constituées en fichiers qui seraient utilisés à des fins de prospection ou de promotion commerciale[24].

3.5 PRESTATAIRE DE SERVICES DE SANTÉ À DOMICILE ET DISTRIBUTEUR DE MATÉRIELS

Les prestataires de services de santé à domicile (PSAD) et les distributeurs de matériels sont tenus d'établir « des documents nécessaires à la personne et pour chaque personne prise en charge, un dossier contenant tous les éléments permettant le suivi de la personne, du matériel et service délivrés »[25].
Ce dossier contient donc des données de santé à caractère personnel. Le prestataire de services de santé à domicile ou le distributeur de matériels est alors le « responsable du traitement » de ces données de santé à caractère personnel[26].
Il est enfin tenu de « prendre toute précaution utile, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[27].

L'hébergement des données de santé à caractère personnel peut se faire :

- Soit sur des supports détenus par les PSAD ou les distributeurs de matériels avec une déclaration normale auprès de la CNIL,
- Soit par externalisation des données de santé sur des serveurs appartenant aux PSAD et aux distributeurs de matériels. Elle offre alors la possibilité de partager ces informations à des fins de prise en charge et de suivi des patients avec dans ce cas la nécessité de faire une demande d'autorisation auprès de la CNIL,
- Soit par externalisation des données de santé auprès d'un prestataire tiers. Dans ce cas, ce sous-traitant du PSAD ou du distributeur de matériels devra être agréé en tant qu'hébergeur. Le dossier d'agrément doit être déposé à l'ASIP Santé en s'appuyant sur leurs référentiels. La CNIL émet un avis sur la demande d'agrément qu'elle transmet alors au Comité d'agrément des hébergeurs (CAH). Le CAH se prononce sur la conformité du dossier puis le ministre en charge de la santé prend la décision d'attribution d'agrément.

À RETENIR

RESPONSABILITÉ

- Le responsable du traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
- Le responsable du traitement de données à caractère personnel doit faire une déclaration auprès de la CNIL.
- L'externalisation des données à caractère personnel nécessite une déclaration spécifique auprès de la CNIL ou doit se faire sur un hébergeur agréé.
- Le traitement des données à caractère personnel implique le respect de la confidentialité basé sur les droits des patients et les devoirs des professionnels de santé.
- Une nouvelle déclaration à la CNIL est nécessaire lorsque l'identité du responsable du traitement des données change.

NOTES

(24) Code de la santé publique - article L. 4113-7. (25) Arrêté du 19 décembre 2006 définissant les modalités de la délivrance mentionnées aux article D. 5232-10 et D.5232-12 et fixant la liste des matériels et services prévue à l'article L. 5223-2 du code de la santé publique - article 1er, 8. (26) LIL- article 3. (27) LIL - article 34.

Focus

CORRESPONDANT INFORMATIQUE ET LIBERTÉS (CIL)

Le CIL ou correspondant à la protection des données à caractère personnel a été créé lors de la refonte de la Loi Informatique et Libertés en 2004. Il est le garant des droits des usagers et des patients en matière informatique et de l'application des exigences juridiques pour les responsables de traitements de fichiers de données à caractère personnel.

> La désignation d'un CIL doit être notifiée à la CNIL. La liste de ses missions doit être accessible à toute personne qui en fait la demande. De nombreuses entreprises, administrations, collectivités ou organismes (parmi lesquels des établissements de santé) ont déjà désigné un CIL et leurs formalités déclaratives s'en trouvent largement allégées. Le CIL peut être une personne interne ou externe à la structure (selon le nombre de salariés) mais il est indispensable qu'elle soit formée à l'activité et aux besoins de la structure.

> Les missions du CIL ont pour but d'assurer le respect de la sécurité donc de la confidentialité des données à caractère personnel. Il est en charge de proposer des mesures d'application concrètes et pratiques adaptées à l'activité professionnelle, et est obligatoirement consulté préalablement à la mise en œuvre de traitements. Il est l'intermédiaire entre les usagers et les responsables des traitements. Il a un rôle d'information et de conseil.
Le CIL dispose d'une autonomie d'action et doit pouvoir exercer ses missions de façon indépendante. Son rôle est reconnu. De même, il ne peut être désigné qu'en l'absence de conflit d'intérêt avec d'autres fonctions qu'il serait amené à exercer.

> Face à une évolution constante et complexe du paysage juridique sur la protection des données à caractère personnel, l'Ordre national des pharmaciens (ONP) souhaite mutualiser et fédérer l'ensemble de la profession sur des enjeux aussi majeurs pour nos métiers que ceux constitués par le maintien de la confiance de nos patients. Le CIL sera un acteur incontournable du garant de la sécurité de nos systèmes d'information.

4 Protection de la vie privée des personnes face aux traitements automatisés de leurs données à caractère personnel – notion de confidentialité

L'article L. 1110-1 du code de la santé publique affirme en priorité le droit à la protection de la santé et prévoit que les acteurs de la santé doivent employer tous les moyens à disposition pour mettre en œuvre ce droit à la santé, et au bénéfice de toute personne. Ils se doivent de garantir l'accès de chaque personne aux soins nécessités par son état de santé et d'assurer le respect du droit des patients.

Afin de protéger la vie privée des personnes dont les données à caractère personnel font l'objet d'un traitement, il est nécessaire d'assurer la sécurité et la confidentialité de leurs données. La confidentialité est définie comme « la protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées »[28].
Le respect de la confidentialité constitue un principe fondamental des règles d'éthique et des codes de déontologie.

À RETENIR

CONFIDENTIALITÉ

- Le respect de la confidentialité des données de santé est fondé sur les droits reconnus aux patients, sur les devoirs incombant aux professionnels de santé et se traduit en particulier par la mise en œuvre de mesures de sécurité.
- Le droit au respect de la vie privée est un principe de valeur constitutionnelle consacré à plusieurs reprises par le conseil constitutionnel.

4.1 DROITS DES PATIENTS

Le Ministère chargé de la santé a fait de l'année 2011 « L'année des patients et de leurs droits » dans le but de renforcer la visibilité et l'effectivité des droits des patients, d'améliorer leur information et de promouvoir leur place dans le système de santé.

4.1.1 Droit au respect de la vie privée

La vie privée, et plus précisément « le droit à l'intimité de la vie privée » fait partie des droits civils[29].
Les composantes de la vie privée n'ont pas fait l'objet d'une définition ou d'une énumération limitative afin d'éviter de limiter la protection aux seules prescriptions légales. Les tribunaux ont appliqué le principe de cette protection au droit à la vie sentimentale et à la vie familiale, au secret relatif à la santé, au secret de la résidence et du domicile, et au droit à l'image.

Le droit au respect de la vie privée est garanti en Europe depuis l'adoption de la Convention Européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales (CEDH) en 1950[30].
En France, le droit au respect de la vie privée tend à renforcer la garantie des droits individuels des citoyens[31] « Chacun a droit au respect de sa vie privée »[29]. ● ● ●

NOTES

(28) Règlement (CE) N°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information - article 4. (29) Code civil - article 9. (30) Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) ,1950 - article 8. (31) Loi n°70-643 du 17 juillet 1970.

Face à l'évolution des technologies de l'information, la législation a été remaniée et de nombreux textes européens visant à garantir le droit au respect de la vie privée ont vu le jour.

Ainsi, la réglementation de l'Union européenne et nationale en matière de traitements de données a pour objet de concilier droit au respect de la vie privée et liberté de circulation de ces données.

Il faut également prendre en considération la notion de vie personnelle instituée au fil des années par la jurisprudence de la Cour de cassation et qui va plus loin que la simple vie privée. Elle englobe non seulement cette dernière mais aussi toutes les activités publiques que l'intéressé peut entreprendre à titre personnel (mandats syndicaux, politiques, activités religieuses, responsabilités associatives, etc.).
Ces deux notions de vie privée et de vie personnelle font aujourd'hui l'objet de nombreuses décisions judiciaires.

4.1.2 Droit à l'information [32]

Toute personne doit être informée de la collecte et du traitement de ses données à caractère personnel.

Le responsable du fichier de données à caractère personnel doit informer les personnes concernées de :

- L'identité du responsable du traitement,
- L'objectif du traitement poursuivi,
- Le caractère obligatoire ou facultatif des réponses,
- Les conséquences à leur égard de l'absence de réponse,
- Les destinataires des informations,
- Les droits reconnus à la personne,
- Les éventuels transferts de données vers un pays hors de l'Union Européenne.

L'obligation d'information peut dans certains cas être allégée :

- Lorsque les données collectées sont anonymisées dans un bref délai,
- Lorsque les données ne sont pas recueillies directement auprès de la personne.

4.1.3 Droit d'opposition [33]

Toute personne peut s'opposer, pour des motifs légitimes, à la collecte et au traitement de ses données à caractère personnel.

Le droit d'opposition peut s'exprimer :

- Par un refus de répondre lors d'une collecte non obligatoire de données,
- Par le refus de donner l'accord écrit obligatoire pour le traitement de données sensibles telles que les opinions politiques ou les convictions religieuses,
- Par la faculté de demander la radiation des données contenues dans des fichiers commerciaux,
- Par la possibilité de s'opposer à la cession ou la commercialisation d'informations, notamment par le biais d'une case à cocher dans les formulaires de collecte.

Le droit d'opposition ne s'applique pas pour certains fichiers du secteur public qui sont des fichiers obligatoires, tels que ceux de la sécurité sociale, des services fiscaux, des services de police, des services de la justice. Cela n'est pas dû à leur nature mais à l'obligation pour le responsable du traitement de les gérer.

4.1.4 Droit d'accès [34]

Toute personne justifiant de son identité a le droit d'accéder et d'obtenir l'intégralité de ses données à caractère personnel auprès de la personne responsable du fichier.

La personne peut s'informer :

- Des finalités du traitement,
- Du type de données enregistrées,
- De l'origine et des destinataires des données,
- Des éventuels transferts de ces informations vers des pays n'appartenant pas à l'Union Européenne.

NOTES

(32) LIL - article 32. (33) LIL - article 38. (34) LIL - article 39.

4.1.5 Droit de rectification[35]

Toute donnée à caractère personnel peut être rectifiée, complétée, actualisée, verrouillée ou effacée à la demande de la personne concernée.
Le droit de rectification constitue un complément essentiel du droit d'accès. Le responsable du traitement doit alors justifier des opérations qu'il a effectuées.
Tout traitement de données personnelles doit prévoir dès sa conception, ses modalités de suppression.

À RETENIR

DROITS DES PATIENTS

Ceux-ci incluent :

- Le droit au respect de la vie privée,
- Le droit à l'information,
- Le droit d'opposition,
- Le droit d'accès,
- Le droit de rectification.

Ces droits sont une expression du droit constitutionnel au respect de la vie privée.

4.2 DEVOIRS DES PROFESSIONNELS DE SANTÉ

Des règles d'éthique et de déontologie strictes doivent êtres observées par les professionnels de santé, afin de préserver la dignité des patients.
Le respect des devoirs des professionnels de santé passe par une sensibilisation du personnel aux menaces et enjeux de la confidentialité des données de patients (cf. 2ème partie, chapitre 3).

4.2.1 Respect du secret professionnel

Le droit à la confidentialité a pour corollaire l'obligation du respect du secret professionnel qui s'impose à tout professionnel dans les conditions établies par la législation.

« La révélation d'une information à caractère secret par une personne qui en est dépositaire [...], est punie d'un an d'emprisonnement et de 15 000 euros d'amende »[36].

Cette protection juridique est renforcée dans la législation nationale par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (dite loi Kouchner) : « Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et au secret des informations la concernant »[37].

D'autre part, en ce qui concerne les pharmaciens, ces dispositions complètent le code de déontologie : « Le secret professionnel s'impose à tous les pharmaciens dans les conditions établies par la loi. Tout pharmacien doit en outre veiller à ce que ses collaborateurs soient informés de leurs obligations en matière de secret professionnel et à ce qu'ils s'y conforment »[38].
Ainsi, tous les professionnels de santé doivent s'assurer du respect du secret professionnel par leurs collaborateurs. A titre d'exemple, au sein d'une officine ou d'une Pharmacie à usage intérieur (PUI), tous les personnels détachés auprès du pharmacien titulaire ou gérant sont tenus au secret professionnel.

Le secret partagé précise que : « Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible [...] »[39].
Le secret partagé est fondé sur l'information préalable et le droit d'opposition permanent du patient.

NOTES

(35) LIL - article 40. (36) Code pénal - article 226-13. (37) Code de la santé publique - article L.1110-4. (38) Code de la santé publique - article R.4235-5. (39) Code de la santé publique - article L.1110-4.

4.2.2 Le recueil du consentement

Tout traitement de données à caractère personnel doit faire l'objet du recueil du consentement de la personne concernée[40] sauf dans certaines situations prévues par la loi telles que la sauvegarde de la vie de la personne concernée[41] ou l'exécution d'une mission de service public.

Le consentement de la personne concernée est défini comme « toute manifestation de volonté, libre, spécifique, et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »[42].

En pratique, on considère que le consentement du patient doit être libre et éclairé, c'est-à-dire, recueilli en l'absence de contraintes et précédé d'une information suffisante.

En 2011, le Parlement européen souligne l'importance de renforcer le droit des patients : « le consentement ne doit être jugé valable que lorsqu'il est clair, informé, donné de plein gré, spécifique et explicite et que des mécanismes appropriés doivent être mis en œuvre afin de consigner le consentement ou la révocation du consentement des utilisateurs »[43].

À titre d'exemple, l'hébergement des données de santé à caractère personnel nécessite le consentement exprès de la personne[44].
De même le consentement du patient[45] est requis lors de la création d'un dossier pharmaceutique.
Le guide des professionnels de santé élaboré par la CNIL en 2011 précise le caractère exprès du consentement dans le cas des traitements des données de santé.
Cependant la remise de la carte vitale par l'usager au pharmacien, qui permet l'accès à ses données de santé et pourrait être considérée comme un consentement, ne peut être envisagée comme tel selon la CNIL.

4.2.3 Respect des obligations techniques et organisationnelles : la sécurité du système d'information

Le Décret Confidentialité[46] introduit trois notions principales, ainsi que des obligations techniques visant à garantir la confidentialité des données médicales personnelles conservées sur support informatique ou échangées par voie électronique :

- Les professionnels de santé doivent se conformer à des référentiels qui décrivent les règles de sécurité et de confidentialité[47].
- Les professionnels de santé qui accèdent aux données de santé à caractère personnel doivent être obligatoirement identifiés par leur carte CPS[48].
- Le responsable de traitement est chargé de la gestion de la liste nominative des professionnels habilités à accéder aux informations médicales et de la mise en œuvre des procédés assurant l'identification et la vérification de la qualité des professionnels de santé[49].
- L'obligation de confidentialité implique de définir les obligations techniques à respecter pour garantir la sécurité du système informatique. Des référentiels d'interopérabilité et de sécurité définis par l'ASIP Santé sont imposés par la loi HPST[50].

À RETENIR

DEVOIRS DES PROFESSIONNELS DE SANTÉ

Les devoirs des professionnels de santé sont :

- Le respect du secret professionnel,
- Le recueil du consentement de la personne,
- Le respect des obligations techniques et organisationnelles, avec l'obligation pour les professionnels de santé de s'identifier grâce à leur carte CPS.

NOTES

(40) LIL - article 7. (41) LIL - article 8 II, 2°. (42) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - article 2. (43) Proposition de résolution du Parlement européen sur une approche globale de la protection des données à caractère personnel dans l'Union européenne 2011/2025(INI) - alinéa 12. (44) Code de la santé publique - article L.1111-8 alinéa 1. (45) Code de la santé publique - article L.1111-23. (46) Décret Confidentialité n°2007-960 du 15 mai 2007, pris en application de la loi du 4 mars 2002 (« Loi Kouchner ») relative aux droits des malades et à la qualité du système de santé. (47) Code de la santé publique article R. 1110-1. (48) Code de la santé publique - article R. 1110-3. (49) Code de la santé publique - article R. 1110-2. (50) Code de la santé publique - article L. 1111-8 alinéa 4.

Focus

SANCTIONS PÉNALES

Des sanctions pénales, complémentaires aux sanctions administratives, sont prévues en cas de violation du droit de la protection des données de santé à caractère personnel. Ainsi, la collecte des données sans en être autorisée ou sans le consentement du patient alors que ce dernier est requis, l'hébergement des données sans un agrément préalable, sont autant de violations passibles de sanctions pénales.
Nous pouvons citer, à titre d'exemple, les sanctions pénales encourues en cas de non respect du secret professionnel, du principe de finalité, ou des obligations incombant au responsable de traitement des données de santé à caractère personnel.

Secret professionnel

« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. » (art. 226-13 du code pénal).

Principe de finalité de traitement des données de santé

Les informations qui concernent les patients ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.Tout détournement de finalité est passible de sanctions pénales (art. 226-21 du code pénal).

Responsable du traitement

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (art. 34 de la LIL).
La négligence ou l'absence de mesures de sécurité peuvent être sanctionnées de 300 000 euros d'amende et de 5 ans d'emprisonnement (art. 226-17 du Code pénal).

2ÈME PARTIE

La sécurité du système d'information

Aspects pratiques

Préambule

La sécurité du système d'information passe par la sécurité du système informatique qui correspond à l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Ces moyens peuvent être d'ordre technique, organisationnel, juridique et humain.

La gestion de la sécurité des données se base sur des exigences fondamentales, notamment :

- **Disponibilité :** les données sont accessibles et utilisables au moment voulu par les personnes autorisées.
- **Intégrité :** les données ne doivent subir aucune autres modifications que celles prévues et planifiées par le système informatique.
- **Confidentialité :** les données ne sont accessibles ou ne peuvent être diffusées qu'à des personnes autorisées. La confidentialité consiste également à rendre l'information inintelligible à d'autres personnes que les seuls auteurs de la transaction.
- **Traçabilité ou preuve :** les accès et les tentatives d'accès aux données sont tracés et les traces sont conservées et exploitables.
- **Non-répudiation de l'information :** elle est la garantie qu'aucun des correspondants (émetteur et destinataire) ne pourra nier une transaction.

Ces notions détermineront les critères d'évaluation de la sécurité informatique.
Dans ce chapitre, sont cités les risques identifiés ainsi que les mesures proposées pour les réduire. Ces risques et mesures ne sont pas exhaustifs.

Principes

DE LA DÉMARCHE DE SÉCURISATION DU SYSTÈME INFORMATIQUE

1 ANALYSE DES RISQUES

Identifier et quantifier les risques informatiques (cause, potentialité, impacts, effets, conséquences, gravité) et les coûts associés :

- **Recenser les fichiers de données** à caractère personnel et les traitements associés,
- **Identifier les supports** tels que matériels, logiciels et canaux de communication,
- **Déterminer les atteintes possibles** et les classer selon leur gravité et leur mode de traitement :
  - Confidentialité = usurpation d'identité
  - Disponibilité = non détection d'une contre-indication
  - Intégrité = modification d'un fichier dans un but d'accusation à tort,
- **Étudier les risques** en fonction des menaces (vol matériel, contagion, saturation des canaux de communication) et les hiérarchiser (impacts et probabilité d'occurrence),
- **Déterminer les mesures de sécurité** pour réduire, détourner ou éviter les risques.

2 POLITIQUE DE SÉCURITÉ

- **Élaborer des règles** et des procédures pour pallier aux risques identifiés,
- **Définir les actions** à entreprendre et les personnes à contacter en cas de détection d'un risque,
- **Sensibiliser les utilisateurs** aux problèmes liés à la sécurité du système informatique,
- **Préciser les rôles** et responsabilités de chacun.

3 TECHNIQUES DE SÉCURISATION

- **La sécurité des données :** chiffrement, authentification, contrôle d'accès,
- **La sécurité du réseau :** pare-feu, système de détection d'intrusion,
- **La surveillance** des informations de sécurité,
- **La formation des utilisateurs,**
- **Le plan de reprise** des activités et le plan de continuité des activités,
- **L'audit de vulnérabilités,** tests de pénétration ou d'intrusion.

1 Locaux et matériels

La sécurisation des systèmes d'information informatiques commence par la sécurisation des locaux et du matériel.

1.1 SÉCURITÉ PHYSIQUE DES LOCAUX CONTENANT DES INFORMATIONS SENSIBLES ET LES MOYENS DE TRAITEMENT DE L'INFORMATION

RISQUES

- Intrusion,
- Accès par un personnel non autorisé,
- Incendie,
- Inondation,
- Augmentation de température (panne de climatisation).

MESURES

- Alarmes,
- Interdiction de tout accès non autorisé,
- Dispositifs anti-incendie,
- Panneaux anti-inondation, surélévation du matériel,
- Détecteurs de température.

1.2 SÉCURITÉ DU MATÉRIEL ET DU CÂBLAGE

RISQUES

- Pertes d'alimentation,
- Surchauffes,
- Pannes.

MESURES

- Système de secours électrique (onduleur),
- Climatisation,
- Contrat de maintenance.

1.3 MISE AU REBUT OU RECYCLAGE

(cf. chapitre destruction).

2 Postes de travail - Systèmes d'exploitation - Logiciels

RISQUES

- Tentative d'accès frauduleux,
- Exécution d'un virus,
- Prise de contrôle à distance, notamment via Internet,
- Existence supplémentaire de failles dans la sécurité du SI dues à l'interfaçage entre les différents logiciels métier,
- Logiciels supportés par des serveurs nécessitant l'utilisation de navigateurs et d'hébergeurs,
- Pannes matérielles.

MESURES

- Harmoniser les logiciels pour faciliter les interfaces,
- Créer des référentiels normatifs reconnus et agréés,
- Établir des niveaux d'accès selon les métiers et les fonctions et rétablir la notion d'administrateur,
- Renforcer les mesures de sécurité dans le cas des serveurs et faire appel à des outils de détection des vulnérabilités pour détecter les failles de sécurité,
- Limiter les actions sur chaque poste de travail uniquement à celles strictement nécessaires à l'activité à partir de ce poste,
- Exiger la possibilité de visualiser les modifications effectuées sur les données sensibles (couleur différente ou date de dernière modification par exemple),
- Effectuer régulièrement les mises à jour des logiciels et des systèmes d'exploitation pour éviter les failles non corrigées,
- Installer un « pare-feu »,
- Utiliser un anti-virus et prévoir sa mise à jour régulière (base de signatures),
- Établir et respecter les règles de connexions et déconnexions des postes de travail (voir chapitre « accès aux données »).

Notion d'administrateur

Le responsable du traitement des données à caractère personnel doit posséder les droits d'administrateur lui permettant de modifier des paramètres de sécurité, installer des logiciels et des matériels et accéder à tous les fichiers de l'ordinateur. Il sera ainsi également habilité à modifier d'autres comptes d'utilisateurs. Le compte administrateur permettra d'accéder à l'ensemble des informations relatives aux utilisateurs y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978.

Notion de pare-feu

Un firewall, pare-feu ou garde-barrière, est un système permettant de protéger un ordinateur connecté à un réseau ou à Internet, de messages provenant de domaines interdits (sites de commerce) ou d'attaques externes (filtrage entrant) et de connexions illégitimes à destination de l'extérieur (filtrage sortant), initialisées par des programmes ou des personnes.

Le pare-feu a pour but de protéger contre plusieurs types de menaces :

- Les intrusions sur l'ordinateur, depuis l'Internet ;
- Certains virus et certains vers (infection et propagation) ;
- 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.

3 Accès aux données sensibles

Le suivi du patient impliquant le traitement de ses données à caractère personnel, nécessite un accès à la totalité de ses données qui n'est possible que si deux critères de sécurité informatique sont respectés : **la disponibilité et l'intégrité des données.**

Juridiquement, en dehors du professionnel de santé responsable de ces données, **l'accès aux données du patient est limité :**

- Au patient,
- À ses ayants-droits en cas de décès[51],
- À l'autorité parentale,
- Au tuteur,
- Dans certaines conditions, à la personne de confiance désignée par le patient[52],
- À un autre professionnel de santé désigné par le patient lui-même.

RISQUES

- Accès aux données de santé par une personne non autorisée (y compris au sein des structures extérieures en cas d'externalisation d'activités),
- Accès à des données sensibles sans rapport avec l'activité de l'utilisateur,
- Connexions avec le code d'un autre utilisateur.

MESURES

1- SÉCURISER L'ACCÈS AUX DONNÉES SENSIBLES

A - IDENTIFICATION : l'identification permet de s'identifier par un moyen fourni qui est l'identifiant ou login. Les éditeurs de logiciels fournissent souvent des comptes par défaut avec des identifiants déjà définis. Dans ce cas, les comptes par défaut doivent être désactivés et les identifiants redéfinis.

B - AUTHENTIFICATION : l'authentification est toujours précédée par l'identification. L'authentification apporte la preuve de son identité. À titre d'exemple, la carte de professionnel de santé (CPS) constitue un moyen d'authentification. L'authentification peut également se faire par une politique de mots de passe sécurisés, uniques et non utilisables simultanément.

Concernant le mot de passe, on peut retenir les instructions suivantes :

- Ne pas conserver le mot de passe fourni,
- Ne pas communiquer son mot de passe,
- Créer un mot de passe contenant si possible au minimum 8 caractères,
- Utiliser des caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux),
- Ne pas utiliser des suites logiques de chiffres ou de lettres (1234 …, defgh …, azerty …),
- Ne pas utiliser des mots de passe ayant des liens avec soi (date de naissance etc.),
- Ne pas utiliser le même mot de passe pour des accès différents (réseau, Internet etc.),
- Ne pas utiliser les exemples donnés,
- Renouveler régulièrement le mot de passe (en général tous les 3 mois),
- Bloquer l'accès au mot de passe après trois tentatives infructueuses.

NOTES

(51) Code de la santé publique - article L. 1111-4 dernier alinéa. (52) Code de la santé publique - article L. 1111-6.

- **Le mot de passe peut être créé par des moyens simples et faciles à retenir :**
  - Choisir une phrase et ne retenir que les 1ères lettres (Ex : Blanche Neige et les sept nains de Walt Disney, le mot de passe sera : BNel7n2WD),
  - Utiliser la méthode phonétique (Ex : j'ai acheté cinq CD pour 100 euros cet après-midi : gHt5cD%e7Am).

C - HABILITATION : les habilitations définissent des niveaux d'accès aux données par les utilisateurs, 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. Il s'agit de mettre en œuvre une politique de contrôle d'accès en fonction de la finalité du traitement. Les habilitations sont justifiées par le métier ou par une mission. Elles doivent garantir la continuité des soins.

2 - DÉTERMINER LES RÈGLES DE CONNEXIONS ET DE DÉCONNEXIONS DES UTILISATEURS

- **L'horodatage :** un procédé d'horodatage est utilisé pour attester de l'existence d'une donnée à un instant, ou de la date d'un acte réalisé par voie électronique (Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, JORF n°0094 du 21 avril 2011).
- **L'impossibilité de se connecter** avec le même code utilisateur (ou identifiant) et mot de passe sur plusieurs postes en même temps.
- **La limitation du nombre de tentatives d'accès :** en général, trois frappes incorrectes 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.

3 - FORMALISER PAR UNE PROCÉDURE LA CRÉATION ET LE BLOCAGE D'ACCÈS DES COMPTES INFORMATIQUES

- Création des comptes informatiques pour tout nouvel utilisateur dans les plus brefs délais.
- Désactivation immédiate de l'accès dès qu'un utilisateur n'est plus habilité (changement d'activité, de mission ou départ).

4 - FAIRE SIGNER UN ENGAGEMENT DE CONFIDENTIALITÉ POUR LES NON-PROFESSIONNELS DE SANTÉ

- Ou prévoir une clause de confidentialité dans le contrat de travail plus spécifiquement pour les données à caractère personnel.

5 - FAIRE ADHÉRER LES UTILISATEURS À CES MESURES DE BASE

- La formation des utilisateurs est la meilleure méthode de sensibilisation à la sécurité du système d'information.
- 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 l'entreprise.

6 - TENIR À LA DISPOSITION DES PATIENTS LA LISTE DES PERSONNES HABILITÉES À SAISIR, CONSERVER, ARCHIVER ET TRANSMETTRE PAR VOIE ÉLECTRONIQUE

- Tout établissement pharmaceutique doit tenir à la disposition des patients la liste des personnes habilitées à saisir, conserver, archiver et transmettre par voie électronique. Les personnes concernées par le traitement des fichiers de données à caractère personnel doivent connaître, entre autre, la finalité de ce traitement, les destinataires et les transmissions envisagées[53].

NOTES

(53) Code de la santé publique - article R.1110-2.

4 Stockage - Sauvegarde Archivage

RISQUES

- Non disponibilité des données,
- Perte d'une partie ou de la totalité des informations,
- Perte de la continuité de l'activité,
- Non restitution des données sauvegardées,
- Accès non autorisé à des données à caractère personnel.

MESURES

- Déterminer les dossiers actifs,
- Sélectionner les supports,
- Faire des sauvegardes régulières,
- S'assurer de la lisibilité des données archivées ou sauvegardées,
- Différencier les types d'archivages selon les types de données,
- Crypter ou sécuriser les archivages,
- Limiter l'accès aux sauvegardes et archivages,
- Respecter les durées de stockage et d'archivage prévues par la réglementation pour les données de santé à caractère personnel, selon la durée de vie des supports de stockage.

4.1 STOCKAGE

Le stockage informatique a pour but la conservation des informations sur supports magnétiques (disques durs), optiques (CD, DVD), clés USB ou cartes SD, etc.
Il permet d'envisager le traitement des informations stockées, leur archivage, leur sauvegarde, leur transfert, etc. Les supports sont nombreux et leur durée de vie est variable (4 ou 5 ans pour un DVD, par exemple).

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, déterminées par le concept de dossiers actifs ou non. **Un dossier actif est constitué par l'ensemble des éléments de ce dossier accessibles aux traitements automatisés. Il a des chemins d'accès valides.** Le plus important dans le stockage est de réunir les conditions de restitution des données. Par exemple, l'archivage ou la sauvegarde doit permettre la lecture des données. Pour cela, il est indispensable de stocker sur un support externe les données ou 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.

Le stockage est également possible chez un hébergeur. La procédure d'agrément des hébergeurs de données de santé à caractère personnel[54], a pour but de garantir la sécurité des données de santé personnelles hébergées par un organisme distinct du professionnel ou de l'établissement de santé qui soigne le malade.
Les conditions d'octroi de l'agrément ont été fixées par le décret du 4 janvier 2006 qui détermine la procédure d'agrément et le contenu du dossier qui doit être fourni à l'appui de la demande. Cet agrément est octroyé pour une durée de trois ans par le ministre chargé de la Santé, qui se prononce après avis de la CNIL et du Comité d'agrément créé auprès de lui. ● ● ●

4.2 SAUVEGARDE

Les sauvegardes dupliquent les données du système informatique à un moment donné afin de les mettre en sécurité. C'est une copie de sureté qui assure une reproduction exacte des données informatiques à un instant précis.
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.

ON DISTINGUE

- Des sauvegardes incrémentales journalières (ne concernent que les données ajoutées depuis la dernière sauvegarde),
- Des sauvegardes complètes hebdomadaires ou bimensuelles.

Il est nécessaire de sécuriser les sauvegardes, soit par une méthode de chiffrement (chiffrer les sauvegardes ou chiffrer les données à la source), soit en les stockant dans un lieu sécurisé, distant du lieu d'exercice.
Les mesures cryptographiques permettent de protéger la confidentialité, l'authentification et l'intégrité de l'information, par des algorithmes utilisant des clés de chiffrement. Ces mesures sont recommandées pour les données classifiées sensibles.
De même, l'accès aux sauvegardes répondra aux mêmes règles que l'accès aux données à caractère personnel, par le biais des habilitations.

4.3 ARCHIVAGE

Tout comme la sauvegarde, l'archivage est une copie des données à un moment déterminé. Mais ce recueil d'informations doit garantir la conformité des données sur le long terme.

Comme pour les sauvegardes, il est recommandé de sécuriser les archivages, par chiffrement ou stockage dans un lieu sécurisé.
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 SSII 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).

ON DISTINGUE

- Les archives courantes qui concernent des données d'utilisation courante,
- Les archives intermédiaires qui sont constituées par des données qui ne sont plus utiles mais qui gardent un intérêt ; elles sont conservées sur des supports distincts,
- Les archives définitives qui sont constituées par des données dont l'intérêt justifie leur conservation (scientifique par exemple).

NOTES

(54) LOI n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

La politique d'archivage doit intégrer la notion de cycle de vie des données.
La durée de stockage ou d'archivage est déterminée par les durées de conservation imposées par la CNIL[55] pour l'officine ou par le Code de la santé publique pour les établissements de santé[56] et pour les laboratoires de biologie médicale[57].

POUR LES OFFICINES[55] :
- 3 ans en accès direct,
- 15 ans sur support papier,
- 10 ans pour le registre des stupéfiants et les ordonnanciers, après la dernière inscription,
- 40 ans pour le registre des médicaments dérivés du sang après la dernière inscription.

POUR LES ÉTABLISSEMENTS DE SANTÉ :
- 20 ans à compter de la date du dernier séjour[56] pour les majeurs,
- 20 ans après leur majorité pour les mineurs,

En cas de décès, la durée est inférieure.

POUR LES LABORATOIRES DE BIOLOGIE MÉDICALE[57] [58] :
- 5 ans pour les résultats nominatifs pour les analyses effectuées par le laboratoire,
- 10 ans pour les résultats nominatifs des analyses d'anatomie et de cytologie pathologiques,
- 10 ans pour le relevé chronologique des analyses comportant l'origine des prélèvements.

Les « purges » seront définies par les durées de conservation légales pour « les traitements automatisés des données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de l'officine »[55].

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, dissocié de l'éditeur.

NOTES

(55) Délibération CNIL n°2006-161 du 8 juin 2006. (56) Code de la santé publique - article R 1112-7. 57) Code de la santé publique - article R 6211-23. (58) Code de la santé publique - article R 6211-24.

5 Destruction

RISQUES

- Persistance de données à caractère personnel sur les supports de stockage mis au rebut ou remplacés,
- Utilisation abusive de ces données par des tiers,
- Destruction ou élimination de données devant être conservées.

MESURES

- Élimination totale des données à caractère personnel stockées sur les supports mis au rebut ou remplacés, par destruction physique des supports de stockage ou effacement par réécriture avec un logiciel dédié,
- Document remis au pharmacien par les SSII attestant de la méthode de destruction des supports ou de l'effacement total des données stockées sur ces supports,
- Vérification avant destruction de la récupération des données,
- Information et autorisation du pharmacien selon une procédure formelle.

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. 80% des disques durs achetés sur des sites Internet réputés contiennent des informations privées ou confidentielles. Le formatage est insuffisant pour les effacer.

Dans le cas de prêt de matériel dans des situations de panne, la problématique de la destruction des données ayant transité sur les supports de stockage est encore plus importante. Il en est de même pour les matériels en fin de contrat de location.

Pour s'assurer de la destruction des données stockées, il faut procéder à :

- Une destruction mécanique des supports par écrasement, incinération ou torsion des disques durs, broyage des CD ou DVD,
- Ou une démagnétisation pour certaines unités de stockage,
- Ou la mise en œuvre d'une méthode d'effacement par réécriture (c'est à dire trois passages au minimum) proposée par certains logiciels.

Cas particulier de la fermeture d'une officine de pharmacie, d'un établissement de santé ou d'un laboratoire de biologie médicale :

L'article R.5125-30 du Code de la santé publique prévoit, lors d'une fermeture temporaire ou définitive d'une officine de pharmacie, que l'ordonnancier soit transmis par le titulaire à un pharmacien qu'il désigne au Conseil Régional de l'Ordre des Pharmaciens dont il dépend, ou, à défaut, au pharmacien le plus proche proposé par ledit conseil.

En pratique, en ce qui concerne les établissements de santé et les laboratoires de biologie médicale, l'ARS est décisionnaire.

On peut supposer pouvoir appliquer cette démarche aux données de santé stockées et archivées y compris les historiques.

6 Maintenance

RISQUES

- Interventions sur le système informatique sans que le pharmacien soit informé (au préalable ou à posteriori),
- Recueil de données sans l'accord du pharmacien et transmission à des tiers,
- Accès aux données à caractère personnel.

MESURES

- Clause dans le contrat de maintenance prévoyant qu'aucune intervention ne sera faite sans l'accord préalable du pharmacien,
- Clause de confidentialité,
- Demande d'un rapport détaillé disponible pour chaque intervention,
- Possibilité de tracer les interventions avec le système de journalisation (voir traçabilité),
- Cryptage des données à caractère personnel.

Toutes les SSII font de la maintenance et de la hotline. Beaucoup utilisent la télémaintenance.
Il s'est avéré que certaines transmissions d'informations étaient faites aux sociétés éditrices de logiciels sans l'accord du pharmacien, et sans même qu'il en soit informé.

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

Dans ces contrats, le pharmacien (ou le responsable de la sécurité informatique) doit s'assurer :

- De normes de sécurité garantissant l'authentification, l'intégrité et la disponibilité des données,
- D'une clause de confidentialité sur les données à caractère personnel des patients,
- De la traçabilité des interventions des SSII sur le système,
- D'une garantie qu'aucune intervention en télémaintenance ne s'effectuera sans son accord (par ouverture de la ligne de connexion),
- De la visualisation à l'écran du début et de la fin de la prise en main à distance,
- De la destruction des données sur les supports restitués ou échangés,
- Du chiffrement des données transmises.

7 Transmission Sous-traitance

7.1 TRANSMISSION

Dans les transmissions, il faut différencier celles 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 (TP) ou la transmission des rapports d'observance par les prestataires de services de santé à domicile aux prescripteurs. Mais ce recueil d'informations doit garantir la conformité des données sur le long terme.

Dans le 1er cas, la sécurisation, donc la confidentialité des données à caractère personnel est garantie car très encadrée par la législation. Dans le 2ème cas, le « transmetteur » (pharmacien ou prestataire) se doit de respecter la réglementation en vigueur et de s'assurer de la sécurisation et du bon destinataire de la transmission.

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.

7.2 SOUS-TRAITANCE

L'externalisation du TP par un Organisme Gestionnaire (OG) est une sous-traitance. Il convient de différencier le sous-traitant (l'exécutant) et le responsable du traitement. Bien que le réseau soit sécurisé et l'accès par l'OG assujetti à un identifiant et un mot de passe, l'OG a accès au logiciel du pharmacien et au fichier archivage contenant les documents patients scannés à toutes les heures ouvrées de l'OG, donc à toutes les informations confidentielles contenues dans le système d'information du pharmacien.

Dans l'externalisation du TP, du poste de travail jusqu'à l'organisme destinataire, le circuit emprunté par les flux est un VPN (Virtual Protocol Network). Les données sont transmises de façon chiffrée. C'est un 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.

Ainsi, le VPN vise à apporter certains éléments essentiels dans la transmission des données : l'authentification des interlocuteurs et la confidentialité des données (par le chiffrement).

Ceci garantit au professionnel de santé la sécurisation et la traçabilité des feuilles de soin électroniques.

Toutes ces garanties doivent être fournies au pharmacien et/ou vérifiées par celui-ci avant tout engagement de sous-traitance.

7.3 TRANSMISSION ET SOUS-TRAITANCE

Certains organismes sont habilités en sous-traitance et en transmission.

Le pharmacien peut, s'il le souhaite, faire appel à deux types d'organismes extérieurs pour l'aider dans les transmissions aux caisses d'assurance maladie et le recouvrement des prestations effectuées :

- Un organisme concentrateur technique (OCT)
- Un organisme gestionnaire (OG).

Les OCT et les OG peuvent être gérés par des groupements de pharmaciens, des syndicats, des SSII, des banques, des prestataires etc. Les transmissions à l'OCT nécessitent la carte de professionnel de santé (CPS) du pharmacien. Les données transmises à l'OCT sont cryptées. Mais elles sont décryptées au niveau de l'OCT avant fractionnement et transmission aux caisses. ● ● ●

7.4 TRANSMISSION DANS UN CADRE JURIDIQUE

Dans le cas d'une procédure pénale (enquête de flagrance, enquête préliminaire), des documents pouvant contenir des données à caractère personnel, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, peuvent être obtenus directement par le juge d'instruction ou par un officier de police judiciaire intervenant sur réquisition du juge d'instruction ou autorisation du procureur de la République. Il peut s'agir d'un officier de police judiciaire de l'Office central de lutte contre les atteintes à l'environnement et à la santé (OCLAEPS), de la Gendarmerie nationale, ou bien encore d'un contrôleur des douanes habilité à exercer les missions de police judiciaire.

Le secret professionnel ne peut être opposé, sauf motif légitime, pour refuser de répondre à une réquisition. Le fait de s'abstenir de répondre dans les meilleurs délais à une réquisition est puni d'une amende.

Cependant, le juge ou l'officier de police « a l'obligation de provoquer immédiatement toutes les mesures utiles pour que soit assuré le respect du secret professionnel » (Art. 96 et 97 du code de procédure pénale).

Par ailleurs, le code de la santé publique prévoit la consultation par des « autorités compétentes » de divers documents, notamment les ordonnanciers et autres registres dont la tenue est obligatoire, les prescriptions se rapportant aux stupéfiants, etc. Ceci relève des missions des pharmaciens inspecteurs de santé publique qui contrôlent le respect de la réglementation des substances vénéneuses. Ils peuvent donc accéder à tous les documents en rapport et sont tenus au secret professionnel.

En dehors de ces deux situations, qui sont la réquisition et l'inspection de santé publique, le pharmacien et ses collaborateurs doivent scrupuleusement respecter le secret professionnel.

8 Traçabilité

RISQUES

- Accès non autorisé à des données à caractère personnel,
- Utilisation abusive de données à caractère personnel,
- Détournement d'information,
- Altération des données (changées ou détruites),
- Défaut de sécurité.

MESURES

- Traçabilité,
- Non-répudiation,
- Journalisation,
- Gestion des incidents liés à la sécurité.

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. On parle de « journal des traces », qui doit être consulté régulièrement.
On peut y associer **la non-répudiation** qui est le fait que l'émetteur ou le destinataire de l'information ne peut ni nier l'avoir émise ou reçue, ni contester son contenu. La traçabilité et la non-répudiation participent au respect de la confidentialité des données à caractère personnel.

La traçabilité peut permettre d'identifier un accès frauduleux à des données personnelles ou une utilisation abusive de ces données.
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.

La traçabilité est souvent associée une gestion des incidents. On enregistre ainsi les activités des utilisateurs, poste par poste, et les évènements liés à la sécurité. On identifie et on enregistre les connexions ou tentatives de connexions, les accès aux données, les actions réalisées (ajout, modification, suppression). On effectue ce que l'on appelle **une journalisation** des accès avec identifiant, date et heure de connexion et de déconnexion, détail des actions effectuées par l'utilisateur et des données consultées. Il est donc important que l'horloge des différents systèmes de traitement de l'information soit synchronisée (routeurs, PC, serveurs, etc.).

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.

9 Réseau Internet

RISQUES

- Réseau non sécurisé,
- Réseau non fiable (coupures),
- Exécution d'un virus,
- Spams, malwares, chevaux de Troie,
- Accès illicite aux données à caractère personnel,
- Vol ou détournement de données,
- Usurpation d'identité.

MESURES pour le réseau

- Faire un cloisonnement réseau.

Un système d'information en réseau est un système de partage. Ce partage concerne les dossiers mais aussi le matériel 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.
A noter : le secret partagé n'exonère pas chacun de sa responsabilité en matière de secret professionnel.

MESURES pour Internet

- Sécuriser l'accès Internet,
- Utiliser un pare-feu,
- Installer un anti-virus,
- Restreindre la connexion à Internet (ou prévoir la séparation physique des deux réseaux),
- Limiter les flux réseau au strict minimum,
- Effectuer une mise à jour régulière des logiciels pour éviter les attaques au niveau des failles du système,
- Ne jamais utiliser un compte administrateur pour naviguer,
- Installer un système de détection d'intrusion,
- Utiliser le protocole WPA pour les connexions Wi-Fi,
- Rendre illisibles les informations qui transitent par des moyens de chiffrement de protocole.

Les cyber-menaces sont nombreuses et les solutions à apporter quelquefois complexes. Les fournisseurs d'accès à Internet doivent s'impliquer et s'engager dans la sécurité des réseaux.

10 Tableau de synthèse et d'auto-évaluation

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	☐

La sécurité du système d'information

Annexes

> MÉTHODE DE TRAVAIL

Le groupe de pilotage, constitué en octobre 2010, s'est attaché à collecter le plus large consensus possible. S'en est suivi la constitution d'un groupe de travail constitué de membres des conseils centraux concernés par le sujet. Après élaboration de la note de cadrage et sa validation en avril 2011, les réunions du groupe de travail ont permis la réalisation d'un livrable en version 0 en août 2011. La dernière version RECOS_CG_2012_05_16 a été soumise à un groupe de lecture sollicité pour évaluer le contenu du travail et apporter son expertise sous forme de remarques ou de commentaires qui ont été intégrés dans la version définitive.

> GROUPE DE PILOTAGE

Il est constitué par des membres du Conseil national de l'Ordre des pharmaciens :

- Xavier DESMAS, pharmacien titulaire d'officine, Président de la Commission Exercice Professionnelle.
- Patrick FORTUIT, Vice-Président du Conseil national de l'Ordre des pharmaciens.
- Catherine GONZALEZ, pharmacien d'officine intérimaire.
- Anna SARFATI, pharmacien gérant - praticien hospitalier, membre du bureau du Conseil national de l'Ordre des pharmaciens.
- François VIGOT, pharmacien titulaire d'officine.

Et par Sylvain IEMFRE, Directeur de la Direction des technologies en santé, Ordre national des pharmaciens.

Le groupe de pilotage est chargé, notamment :

- d'effectuer une étude préparatoire ciblant les thématiques et collectant les données bibliographiques disponibles,
- d'effectuer et d'analyser la bibliographie,
- d'assurer la coordination du projet,
- d'élaborer les versions successives des travaux,
- d'organiser les modalités de validation du document lors des différentes étapes (modalités d'obtention d'un consensus, etc.),
- d'organiser la validation de la version finale du document.

GROUPE DE TRAVAIL

Il est constitué par des membres de l'Ordre national des pharmaciens :

- Serge CAILLIER, *Vice-président d'EPhEU, membre du bureau du Conseil Central D*
- Pascal DONNY, *pharmacien-conseil chef de service, membre du Conseil Central D*
- Philippe FLOQUET, *pharmacien d'officine, membre du Conseil Central D*
- Jean-Charles TELLIER, *pharmacien titulaire d'officine, Président du Conseil Régional de l'Ordre des pharmaciens de Picardie*
- Pierre GAVID, *pharmacien titulaire d'officine, membre du Conseil national de l'Ordre des pharmaciens, Président de la Commission des systèmes d'information.*
- Christian HERVE, *pharmacien biologiste, membre du Conseil Central G*
- Serge TAKENNE-MEKEM, *pharmacien titulaire d'officine, représentant auprès du Conseil Central E des pharmaciens de Wallis et Futuna*
- Badr Eddine TEHHANI, *pharmacien praticien hospitalier, Président du Conseil Central H*
- Alain VANNEAU, *pharmacien praticien hospitalier, membre du bureau du Conseil Central H, représentant auprès du Conseil Central E des pharmaciens de Saint-Pierre et Miquelon*

La Direction de l'Exercice Professionnelle, représentée par Suzanne HAMDAN, a participé à la réalisation des travaux.

Par ailleurs, certaines directions de l'Ordre ont également été sollicitées :

- La Direction des Technologies de Santé (DTS)
- La Direction de l'Organisation et des Systèmes d'Information (DOSI)
- La Direction des Affaires Juridiques (DAJ)
- La Direction de la Communication (DirCOM)

GROUPE DE LECTURE

Institutions et organismes sollicités :

- Académie Nationale de Pharmacie
- Agfa Healthcare
- Alliance Healthcare France
- Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP)
- Association Nationale des Etudiants en Pharmacie de France (ANEPF)
- Agence des Systèmes d'Information Partagés de santé (ASIP Santé)
- Asp Line Groupe Euralliance Acecom
- Cabinet Conseil En Informatique Falgon (CCIF)
- Caduciel Informatique
- Centre hospitalier Le Mas Careiron à Uzès
- Centre hospitalier universitaire de Clermont Ferrand : Commission des systèmes d'information constitutive de la conférence des DG de CHU
- Collectif Inter Associatif sur la Santé (CISS)
- Caisse Nationale d'Assurance Maladie des Travailleurs Salariés (CNAMTS)
- Collège des maîtres de stages
- Commission Nationale de l'Informatique et des Libertés (CNIL)
- Commission des systèmes d'information : DSI des Hôpitaux Universitaires de Strasbourg
- Computer Engineering
- Conférence des doyens
- Direction Générale de l'Offre de Soins (DGOS)
- Direction Générale de la Santé(DGS)
- DL Santé
- Délégation à la Stratégie des Systèmes d'Information de santé (DSSIS)
- Fédération de l'Hospitalisation Privée (FHP)
- Fédération Nationale des Syndicats d'internes en Pharmacie (FNSIP)
- Fédération des Syndicats Pharmaceutiques de France (FSPF)
- Haute Autorité de Santé (HAS)
- Institut des Données de Santé (IDS)
- Isipharm
- La source informatique
- Pharmagest Interactive
- Syndicat des Biologistes (SDB)
- Société Française de Pharmacie Clinique (SFPC)
- Syndicat Interhospitalier de Bretagne (SIB)
- Syndicat National des Biologistes des Hôpitaux (SNBH)
- Syndicat National des Pharmaciens Gérants Hospitaliers (SNPGH)
- Syndicat National des Pharmaciens Praticiens Hospitaliers et des Praticiens Hospitaliers Universitaires (SNPHPU)
- Syndicat National des Pharmaciens des Établissements Publics de Santé (SYNPREFH)
- Union Nationale des Pharmacies de France (UNPF)
- Union Syndicale des Pharmaciens d'Officine (USPO)

Relecteurs :

- Gilles BENAD, *Directeur de la sécurité des systèmes d'Information, CNAMTS*
- Marie-Noëlle BILLEBOT, *Manager, ANAP*
- Bernard BOCQUILLON, *Directeur adjoint du système d'information du CHU de Tours*
- Jeanne BOSSI, *Secrétaire générale, ASIP Santé*
- Philippe BURNEL, *Délégué, DSSIS*
- Gilles CEBE, *Médecin responsable du Département d'information médicale, Centre hospitalier Le Mas Careiron* à Uzès
- Pierre CHUZEL, *membre du bureau, SDB*
- Professeur Jean-Pierre FOUCHER, *Secrétaire général adjoint de l'Académie nationale de Pharmacie ; Vice Président de l'UFR Pharmacie Paris Sud XI ; membre honoraire du Conseil national de l'Ordre des pharmaciens*
- Emmanuel FRETTI, *Directeur général, Isipharm*
- Paule KUJAS, *Adjointe au chef du bureau qualité et sécurité des soins, DGOS*
- Pierre LIOT, *Chef de projet, Service Qualité de l'information médicale, HAS*
- Vincent MARY, *SIB*
- Francine PAULUS, *Doyen de la faculté de Pharmacie, Université de Lorraine*
- Grégory ROUSSEAU, *Directeur Technique, Pharmagest*
- Didier SICARD, *Président du Comité d'experts, IDS*
- Majid TALLA, *Pharmacien hospitalier, Manager, ANAP*
- Paul TSAMO, *Chef de projet, ANAP*

> BIBLIOGRAPHIE

Articles :

- BALLET Philippe, BENEAT Anne-Lise. *Dématérialisation des données de santé : quels référentiels ?* Gazette du Palais, 22 janvier 2011, n°21-22, p.22
- BERNARD Jean-Paul. *Dossier hospitalier et recherche : Actes du colloque : Le dossier médical: questions éthiques et juridiques - Accès au dossier médical par les tiers et liens avec d'autres dossiers.* Revue générale de droit médical, décembre 2010, n°37, p. 255-259.
- BICLET Philippe. *Hébergement et échange des données de santé.* Médecine & Droit, novembre 2010, vol. 2010, n°105, p. 159-160.
- Commission Nationale de l'Informatique et des Libertés (CNIL). Fiche pratique, *La santé numérique à l'heure des choix*. www.cnil.fr
- Commission Nationale de l'Informatique et des Libertés (CNIL). Article, *La télémédecine mieux encadrée*, 27 octobre 2010
- LE COZ Pierre, *Avis du CCNE à propos des questions soulevées par l'informatisation des données de santé.* Revue générale de droit médical, décembre 2010, n°37.

Ouvrages et rapports :

- Agence nationale de la sécurité des systèmes d'information (ANSSI). *Référentiel général de Sécurité.* Version 1.0 du 13 janvier 2010. 29 p.
- Commission Nationale de l'Informatique et des Libertés (CNIL). Guide. *La sécurité des données personnelles.* Édition 2010. 48 p.
- Commission Nationale de l'Informatique et des Libertés (CNIL). *Guide des professionnels de santé.* Édition 2011. 76 p.
- Conférence Nationale de Santé (CNS). *Comment utiliser les données de santé.* Compte-rendu de la 1ère réunion du débat publique, Paris. mercredi 3 février 2010. 52 p.
- Conférence Nationale de Santé (CNS). *Comment utiliser les données de santé.* Compte-rendu de la 2ème réunion du débat publique. Clermont Ferrand, mercredi 10 février 2010. 57 p.
- Conférence Nationale de Santé (CNS). *Avis sur les données de santé informatisées.* Adopté par l'Assemblée plénière le 19 octobre 2010. 11 p.
- DAHAN Muriel & SAURET Jacques, *Sécurisation du circuit du médicament à l'Assistance Publique - Hôpitaux de Paris (AP-HP).* Paris, Inspection générale des affaires sociales, 2010. 115 p.

- DUFOUR Jean-Charles. *Aspects juridiques et Traitement de l'Information en santé.* LERTIM, Faculté de médecine Timone. Université de la Méditerranée. Marseille. mars 2009.
- Groupement d'Intérêt Économique SESAM-VITALE (GIE SESAM-VITALE). *Rapport annuel d'activités.* 2009. 36 p.
- Haute Autorité de Santé (HAS). Service des recommandations professionnelles. *Recommandations pour la pratique clinique. Accès aux informations concernant la santé d'une personne. Modalités pratiques et accompagnement.* Décembre 2005.
- Institut des Données de Santé (IDS). *Données de santé : en France, qui peut en faire quoi ?* 2009.
- LAFFAIRE Marie-Laure, *Protection des données à caractère personnel.* Paris, Éditions d'Organisation, 2005. 542 p. (Collection Guides pratiques).
- LESAULNIER Frédérique. *L'informatisation des données de santé et la législation Informatique et Libertés.* CNIL. Colloque Gouvernance et sécurité des systèmes d'information de santé Marseille. 7 juin 2011. 32 p.
- LUCAS Jacques, *Dématérialisation des documents médicaux.* Rapport adopté par le Conseil national de l'Ordre des médecins le 18 juin 2010. 39 p.
- Ordre national des pharmaciens, FSPF, UNPF et USPO. *Charte qualité pour les logiciels à l'usage de l'exercice officinal.* Version 1.3. 2 avril 2008. 62 p.
- VOSS Axel. *Proposition de résolution du Parlement européen sur une approche globale de la protection des données à caractère personnel dans l'Union européenne.* 2011/2025(INI). Commission des libertés civiles, de la justice et des affaires intérieures. 22 juin 2011.

Documents juridiques :

- Agence des Systèmes d'information partagés de Santé (ASIP Santé). *L'agrément des hébergeurs de données de santé à caractère personnel.* Repères Juridiques. 7 février 2010.
- Agence des Systèmes d'information partagés de Santé (ASIP Santé). *Confidentialité des données de santé. Repères Juridiques.* 17 juin 2010.
- Agence des Systèmes d'information partagés de Santé (ASIP Santé). *Note d'information des usagers relative au consentement à l'hébergement de données de santé à caractère personnel et au DMP.* Repères Juridiques. 29 juillet 2011.

- Agence des Systèmes d'information partagés de Santé (ASIP Santé). *Note juridique relative à l'hébergement de données de santé à caractère personnel aux dossiers détenus par les PSAD et les distributeurs de Matériels*. Repères juridiques. 21 mars 2012.

- Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès. JORF n°65 du 17 mars 2004, texte n°16. page 5206.

- Charte des droits fondamentaux de l'Union Européenne. JO des Communautés européennes N° C364/01 du 18 décembre 2000.

- Commission Nationale de l'Informatique et des Libertés (CNIL). *Norme simplifiée n°52 : Délibération n°2006-161 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie*. Journal officiel n°154, texte n° 92. Paris. 5 juillet 2006.

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions (COM (2010) 609 final). *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*. Bruxelles. 4 novembre 2010.

- Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique. JORF n°4 du 5 janvier 2006. page 174.

- Décret n°2010-1229 du 19 octobre 2010 relatif à la télémédecine. JORF n°0245 du 21 octobre 2010, texte n° 13.

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. JO des communautés européennes N° L 281/31 du 23 novembre 1995.

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004. JORF du 7 janvier 1978. page 227.

- Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Version consolidée au 19 mai 2011. www.legifrance.gouv.fr

- Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Version consolidée au 07 août 2004. www.legifrance.gouv.fr

Sites web :

- ANAP: http://www.anap.fr/
- ANSSI : http://www.ssi.gouv.fr/
- ASIP Santé : http://esante.gouv.fr/
- CADA : http://www.cada.fr/
- CNIL: http://www.cnil.fr/
- CNS: http://www.sante.gouv.fr/conference-nationale-de-sante-c-n-s.html
- GIE SESAM-VITALE : http://www.sesam-vitale.fr/index.asp
- HAS: http://www.has-sante.fr/
- IDS: http://www.institut-des-donnees-de-sante.fr/
- LEGIFRANCE : http://www.legifrance.gouv.fr/

Ordre national des pharmaciens
4, avenue Ruysdaël - 75379 Paris cedex 08
Tél. : 01 56 21 34 34 - Fax : 01 56 21 34 99
www.ordre.pharmacien.fr

Ordre national des pharmaciens

CNOP - Février 2013 - tand'M www.tand-m.com