{ À L'ÈRE NUMÉRIQUE }

COMMENT GARANTIR LA SÉCURITÉ DES DONNÉES DE SANTÉ ?

Que deviennent les données de santé à l'heure où les technologies de l'information et de la communication (TIC) se développent dans la pratique professionnelle ? Si la profession sait qu'elle doit respecter le secret professionnel, est-elle assez sensibilisée aux questions de sécurité informatique des données de patients ? Or la dématérialisation n'en est qu'à ses débuts. Pour vous aider à mieux connaître les obligations propres à votre métier, l'Ordre a édité des recommandations pratiques.

Dossier

COMMENT GARANTIR LA SÉCURITÉ DES DONNÉES DE SANTÉ ?

JE N'HÉSITERAIS PAS À SAISIR LA CNIL

Isabelle Adenot, président du Conseil national de l'Ordre des pharmaciens

En tant que président du Conseil national de l'Ordre des pharmaciens, je suis particulièrement attachée à la sécurité de l'hébergement, des accès et des échanges de données de santé à caractère personnel. **Cette sécurisation est une de mes priorités.** Le secret professionnel qui s'impose à la profession est un élément fondamental de la relation de confiance établie entre le patient et le pharmacien.

Si mon attention était attirée sur des risques, par la mise à disposition auprès des pharmaciens de logiciels ou de dispositifs qui me sembleraient non conformes aux règles prescrites par la loi Informatique et libertés, je n'hésiterais pas à saisir la CNIL.

Des évolutions technologiques qui ont profondément bouleversé l'exercice pharmaceutique

Quelles précautions prendre pour que personne ne lise les données de santé stockées sur un disque dur remisé ? Comment vous assurer que l'accès aux données est protégé lorsque vous faites appel à une télémaintenance ? Nombreuses sont les questions soulevées par la protection de votre système d'information.
En une dizaine d'années, les technologies ont profondément modifié le quotidien des pharmaciens. Simple outil de facturation, l'informatique s'est progressivement imposée dans la gestion des stocks, l'aide à la dispensation aux patients ou les échanges entre professionnels de santé. **Officines, laboratoires de biologie médicale, établissements de santé sont aujourd'hui à la tête de systèmes d'information qui recèlent de précieuses données de patients.**

La protection des données : une obligation

« Les pharmaciens ont une obligation de protection des données de santé dans le cadre du secret professionnel imposé par le code de déontologie. Ils doivent également respecter la loi Informatique et libertés, qui s'applique dès lors que des données relatives à des personnes physiques sont stockées sur papier ou sur informatique », rappelle Catherine Gonzalez, membre du Conseil national de l'Ordre et missionnée sur ce sujet.

Qu'entend-on exactement par « données de santé » ?

Les données que traitent les pharmaciens sont des données à caractère personnel. Ce sont des informations sensibles comme d'autres, telles que les origines ethniques ou raciales, les opinions politiques, syndicales, religieuses…

Ce sont par exemple les données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins. La prescription de médicaments ou des résultats d'analyses médicales sont, par exemple, des données de santé, ou encore l'ensemble des informations dont a connaissance le professionnel de santé. *« Les données de santé appartiennent au patient et le pharmacien en est dépositaire,* explique Isabelle Adenot, président du Conseil national de l'Ordre des pharmaciens. *Les pharmaciens n'ont pas le droit de déroger au respect de la vie privée ou de trahir la confiance des patients. Ils doivent mettre en œuvre les mesures nécessaires pour respecter et faire respecter le secret professionnel. »*

Il existe un cadre légal strict pour la gestion et le traitement de ces données. La France est d'ailleurs pionnière en Europe : elle est la première à avoir encadré, dès 1978, la protection des données de santé avec la loi Informatique et libertés, qui décrit les droits d'accès, d'opposition, de modification, de suppression et d'information autour de ces questions. Cette protection juridique a été renforcée par la loi Kouchner du 4 mars 2002 sur le secret médical ainsi que par le décret sur la confidentialité*.

Que risque-t-on en cas d'exploitation frauduleuse de ces données ?

Des sanctions pénales sont prévues en cas de violation du droit des personnes et de la protection de leurs données. La révélation d'une information à caractère secret par une personne qui en est dépositaire est punie d'un an d'emprisonnement et 15 000 euros d'amende. La collecte de données non autorisée ou réalisée sans consentement, un hébergement de données réalisé par une structure non agréée sont également passibles de sanctions. L'exploitation de ces données dans un but commercial est condamnée par la loi, selon les modalités prévues par l'article L. 226-21 du code pénal. Et les peines encourues par le responsable du traitement des données, comme peut l'être le pharmacien, sont lourdes puisqu'elles peuvent aller jusqu'à 300 000 euros d'amende et cinq ans de prison en cas de négligence ou d'absence de mesures de sécurité.

Tous les métiers de la pharmacie sont-ils astreints aux mêmes obligations ?

Toutes les structures pharmaceutiques ont l'obligation de faire une déclaration auprès de la Commission nationale de l'informatique et des libertés (CNIL) dès lors qu'elles stockent des données à caractère personnel : elles doivent afficher le document CNIL « Traitement de fichiers informatiques » de façon accessible au grand public.
Si le principe est le même pour tous les métiers de la pharmacie, chacun répond à des spécificités propres à son environnement. Ainsi, les démarches à entreprendre auprès de la CNIL varient selon le secteur, et la notion de confidentialité et de sécurisation des données peut poser des questions différentes selon l'activité.
Garant de l'éthique professionnelle, l'Ordre a souhaité apporter son soutien à la profession pour l'aider à comprendre ces impératifs. Il vient d'éditer ses « Recommandations sur le respect de la confidentialité des données de patients dans l'usage de l'informatique » (voir aussi page 4, Actualités Ordre). Ce document regroupe des éléments très pratiques sur la façon de gérer son système d'information en dressant la liste des prérequis et les vigilances à avoir à tous les niveaux, depuis la gestion des locaux jusqu'à l'archivage des données, en passant par le stockage, la maintenance ou la sous-traitance des données.

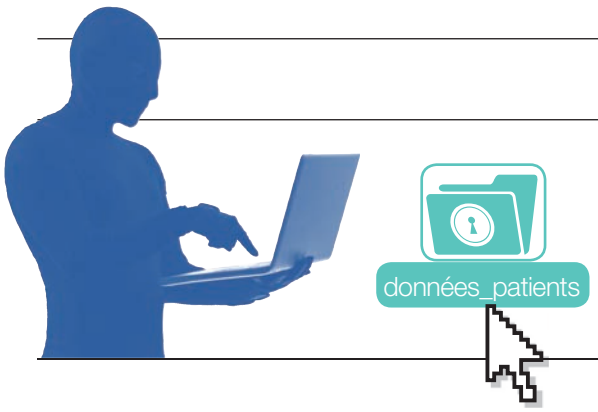
LES PRINCIPES CLÉS DE LA GESTION D'UN FICHIER DE DONNÉES À CARACTÈRE PERSONNEL

- ***La finalité :*** les informations relatives aux patients ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.
- ***La pertinence des données :*** seules les informations pertinentes et nécessaires à l'objectif poursuivi doivent être traitées.
- ***Le droit à l'oubli :*** la CNIL le rappelle sur son site web, les données personnelles ont une date de péremption. Il revient au responsable du fichier de fixer une durée de conservation raisonnable en fonction de l'objectif du fichier.
- ***La sécurité et la confidentialité :*** le professionnel de santé doit prendre toutes les mesures nécessaires pour garantir la confidentialité des informations et éviter leur divulgation à des tiers non autorisés.
- ***Le respect des droits des personnes :*** information, droit d'accès et de rectification, droit d'opposition.

Les droits des patients* envers ces données

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

* Ces droits sont définis dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.



Pour en savoir plus

www.ordre.pharmacien.fr > Communications > Rapports/ Publications ordinales > Respect de la confidentialité des données de patients

Quels sont les réflexes à adopter ?

Afin de garantir la confidentialité de ces données en toutes circonstances, les pharmaciens doivent donc s'assurer de la sécurité de leur stockage, de l'accès aux postes informatiques et de la consultation des informations, mais aussi de la façon dont ils protègent les données lors d'échanges ou d'externalisations. Pour Catherine Gonzalez, *« les pharmaciens n'ont pas tous ces enjeux à l'esprit, il était important de les leur rappeler. Ainsi, des choses très simples, comme des codes d'accès pour utiliser les postes informatiques, devraient être mises en place systématiquement. Lorsque du matériel informatique est remisé, il faut aussi penser à se poser la question du devenir des données stockées dans les disques durs. De même pour les données archivées, dont il faut s'assurer qu'elles restent accessibles lorsque le système informatique de la structure est renouvelé ».* **Les recommandations de l'Ordre permettent de conduire une analyse des risques informatiques dans sa structure grâce à la fiche d'auto-évaluation.** Dès lors, vous pourrez établir une feuille de route dans laquelle vous vous fixerez vos priorités en matière d'amélioration de l'existant.

Qui entreprend cette démarche de sécurisation des données ?

Selon ses compétences, le pharmacien pourra gérer ces évolutions seul ou avec l'aide d'une société de services en ingénierie informatique. Dans les entreprises de taille conséquente, ou dans les établissements de santé, un correspondant Informatique et libertés (CIL) est souvent nommé à cet effet : il gère tous les aspects liés au traitement des données à caractère personnel. Si sa nomination ne revêt pas de caractère obligatoire, ce correspondant facilite les démarches auprès de la CNIL et permet au pharmacien responsable de se dégager de ce problème. Le CIL peut être une personne interne à la structure. *« Les officines ou les laboratoires de biologie médicale ont tout intérêt à adopter eux aussi cette démarche »,* reconnaît C. Gonzalez.

Si de nombreux référentiels sont disponibles sur la gestion des données personnelles informatisées, aucun n'était spécifique à la profession pharmaceutique. Le manque est maintenant comblé. **Ces recommandations apportent un éclairage sur la sécurité des données appliquée à la pratique des pharmaciens, devenu essentiel dans le contexte actuel de l'e-santé.** Une fois acquis, ces fondements prépareront aussi le terrain pour les années à venir : avec l'émergence du partage des données de santé, de nouvelles recommandations et exigences viendront les compléter pour sécuriser ces nouveaux vecteurs d'information.

* Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique.

DP ET SÉCURITÉ

C'est l'Ordre et non le pharmacien qui est responsable du traitement des informations stockées dans le Dossier Pharmaceutique (DP) : la CNIL, le 2 décembre 2008 (délibération CNIL n° 2008-487), a autorisé l'Ordre à ce traitement. Le DP dispose d'un haut niveau de sécurisation, l'Ordre n'ayant souhaité faire aucun compromis sur cette question. Les données relatives à l'identification du patient et à la dispensation sont ainsi dissociées et hébergées séparément sur deux bases cryptées d'un hébergeur agréé par le ministre de la Santé. Ces deux niveaux de données ne sont rapprochés que lors d'une consultation par un pharmacien. Les échanges entre l'officine et l'hébergeur se font alors via des données cryptées circulant par réseau Internet sécurisé.

En savoir plus sur www.ordre.pharmacien.fr

INTERVIEW

Tous les métiers de la pharmacie sont concernés

Isabelle Adenot, président du Conseil national de l'Ordre des pharmaciens

La profession est-elle aujourd'hui suffisamment sensibilisée aux questions de sécurité des données issues des systèmes d'information pharmaceutique ?

I. A. : Les pharmaciens savent qu'ils doivent respecter scrupuleusement le principe déontologique du secret professionnel et que le droit au respect de la vie privée est un principe de valeur constitutionnelle. Mais aujourd'hui, alors que la profession est passée du crayon à la « souris », le respect de cette obligation est plus complexe. L'essor et l'évolution des usages des systèmes d'information nécessitent une nouvelle prise de conscience.

Les pharmaciens doivent aussi être lucides : les données dont ils disposent sont des « trésors » qui peuvent être convoités pour de multiples raisons. Comme ils sont responsables du traitement de ces données (celles des patients comme celles des prescripteurs), il m'a paru absolument essentiel de les sensibiliser à nouveau, tant sur leurs devoirs que sur leurs droits.

Par exemple, les données, même rendues anonymes à l'égard des patients, ne peuvent pas être constituées en fichiers utilisés à des fins de prospection ou de promotion commerciale. Si le pharmacien accepte de permettre à autrui d'accéder aux données de son système d'information, il doit, en toutes circonstances, s'assurer qu'il dispose d'une information claire et complète sur la nature, les conditions de mise en œuvre et les finalités des traitements opérés, ainsi que sur les destinataires de l'information. Et ensuite, avant de s'engager, il doit se poser et poser la question de savoir si cet accès correspond à la déclaration relative aux traitements automatisés de données à caractère personnel qu'il a adressée à la CNIL.

Quels sont les risques pour les pharmaciens et les patients, face au détournement des données de santé ? Certains métiers de la pharmacie sont-ils davantage concernés ?

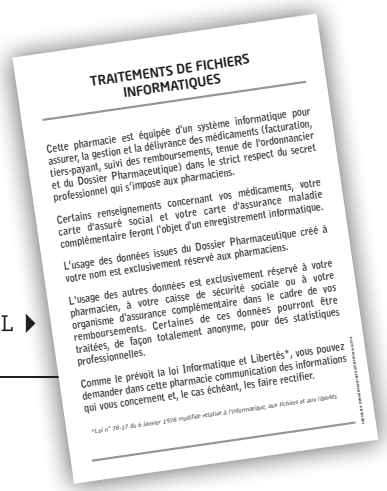
I. A. : Tous les métiers de la pharmacie sont concernés. Tous traitent des données à caractère personnel (les données des pharmaciens en font partie) et ceux en contact avec les patients, des données de santé.

S'ils ne garantissent pas la confidentialité et la sécurité des données qu'ils recueillent, par interception ou lecture de personnes non autorisées, s'ils en détournent la finalité, alors ils s'exposent à un risque de sanctions disciplinaires et pénales lourdes.

S'ils ne prennent pas toutes les précautions utiles, la sanction, au-delà de lourdes amendes, peut aller jusqu'à cinq ans d'emprisonnement ! Les pharmaciens doivent donc prendre toutes les précautions utiles. Sans compter l'autre sanction à laquelle s'exposent les professionnels, celle de perdre la confiance des patients !

Quelles sont les actions mises en œuvre par l'Ordre pour accompagner les pharmaciens sur ce sujet ?

I. A. : Lors du déploiement du DP, nous avons rappelé aux pharmaciens leur obligation de déclaration à la CNIL. Nous mettons également à leur disposition sur le site de l'Ordre l'affichette légale. De manière plus générale, pour soutenir les pharmaciens dans leurs démarches, nous venons d'éditer des recommandations. Elles reprennent les bases juridiques et permettent d'aller à l'essentiel en proposant une méthode simple de mise en œuvre d'auto-évaluation. Elles proposent également des actions concrètes.


TRAITEMENTS DE FICHIERS INFORMATIQUES

Cette pharmacie est équipée d'un système informatique pour assurer, la gestion et la délivrance des médicaments (facturation, tiers-payant, suivi des remboursements, tenue de l'ordonnancier et du Dossier Pharmaceutique) dans le strict respect du secret professionnel qui s'impose aux pharmaciens.

Certains renseignements concernant vos médicaments, votre carte d'assuré social et votre carte d'assurance maladie complémentaire feront l'objet d'un enregistrement informatique.

L'usage des données issues du Dossier Pharmaceutique créé à votre nom est exclusivement réservé aux pharmaciens.

L'usage des autres données est exclusivement réservé à votre pharmacien, à votre caisse de sécurité sociale ou à votre organisme d'assurance complémentaire dans le cadre de vos remboursements. Certaines de ces données pourront être traitées, de façon totalement anonyme, pour des statistiques professionnelles.

Comme le prévoit la loi Informatique et Libertés*, vous pouvez demander dans cette pharmacie communication des informations qui vous concernent et, le cas échéant, les faire rectifier.

*Loi n° 78-17 du 6 Janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

DP - affichette de la CNIL