

actualités

▷ INFORMATIONS
▷ COMMUNIQUES
▷ RAPPORTS &
TRAVAUX

RELATIONS
▷ INTERNATIONALES
▷ LES JEUDIS
DE L'ORDRE

▷ VEILLE JURIDIQUE
exercice
professionnel
▷ GUIDES

▷ CONTRATS
▷ MÉDECINS -
INDUSTRIE

▷ DEMOGRAPHIE
▷ PROTECTION
SOCIALE
DU MÉDECIN

▷ ARCHIVES

code de
déontologie

▷ PAR ARTICLE
▷ RECHERCHE
▷ INTEGRALITE



Professeur Liliane DUSSERRE
septembre 1997

RECOMMANDATIONS DEONTOLOGIQUES POUR LE CHOIX DE LOGICIELS DESTINÉS AUX CABINETS MÉDICAUX

Résumé

Informatiser son cabinet est une décision qui conduit le médecin praticien à faire des choix auxquels il n'est pas habitué. En matière de logiciels il doit avant tout s'assurer que ses besoins ont été pris en compte d'une manière judicieuse et qu'il pourra recueillir et traiter les informations de ses patients dans le respect de la déontologie médicale. Il s'agit avant tout de protéger les droits des patients sur des informations qui leur sont personnelles et de ne pas aliéner son indépendance médicale par des contraintes commerciales. Les contrats suffisamment explicites et détaillés entre les médecins et leurs fournisseurs d'informatique doivent prévoir les garanties adaptées à chaque situation.

L'ordonnance N° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins prévoit que :

"Le 31 décembre 1998 au plus tard, les professionnels, organismes ou établissements dispensant des actes ou des prestations remboursables par l'assurance maladie et les organismes d'assurance maladie doivent être en mesure, chacun pour ce qui le concerne, d'émettre, de signer, de recevoir et de traiter des feuilles de soins électroniques ou documents assimilés conformes à la réglementation."

Cette injonction de la loi a ouvert le marché de l'informatisation des cabinets médicaux libéraux, marché qui jusqu'à présent restait limité. De nombreux éditeurs de logiciels proposent maintenant leurs produits aux médecins sans toujours bien maîtriser les spécificités de l'information médicale et leurs implications légales et déontologiques. Pour guider les praticiens dans leur choix nous examinerons les spécificités de l'information médicale et les principales garanties qu'ils doivent exiger des logiciels disponibles.

Spécificités de l'information en médecine

Les informations médicales relatives aux patients ont pour principale caractéristique d'être des informations personnelles (personal data des anglo-saxons). Elles sont protégées en France depuis 1978 par la loi dite "informatique et libertés" (1) et prochainement par la directive européenne "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" (2), qui sera transposée dans le droit français avant octobre 1998. Selon cette directive on entend par données à caractère personnel :

"Toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;... "

Les informations contenues dans un dossier médical répondent à cette définition. Des informations banales telles que l'âge, le sexe, la taille, le poids, le lieu d'habitation deviennent des informations "médicales" dans la mesure où elles ont été recueillies à l'occasion de la consultation médicale et qu'elles peuvent être utilisées dans la démarche diagnostique et thérapeutique du médecin. Leur spécificité médicale ne réside donc pas dans leurs caractéristiques intrinsèques mais dans leur utilisation et une même information personnelle peut être, selon le contexte, une donnée médicale ou une donnée administrative. Le Comité des ministres du Conseil de l'Europe dans l'annexe de la Recommandation N° R(97)5 considère que "l'expression "données médicales" se réfère à toutes les données à caractère personnel relative à la santé d'une personne. Elle se réfère également aux données ayant un lien manifeste et étroit avec la santé..." (3).

Si confidentielles que soient les informations médicales personnelles, elles sont paradoxalement destinées le plus souvent à être communiquées mais uniquement à des tiers autorisés et sous réserve de l'accord du patient. Ces tiers autorisés sont nombreux et divers. Les différents médecins et autres professionnels de santé qui interviennent dans les soins ainsi que les médecins qui ont la charge du contrôle des prestations de l'assurance maladie, sont les plus souvent concernés.

1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés complétée par la loi n° 94-548 du 1er juillet 1994

2) 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 (JOCE. 23/11/1995).

3) Recommandation n° R (97)5 du comité des ministres aux Etats membres relative à la protection des données médicales (adoptée par le Comité des ministres le 13 février 1997 lors de la 584^e réunion des délégués des ministres).

Dans l'intérêt de la recherche médicale et épidémiologique des dérogations légales peuvent être obtenues auprès de la CNIL pour la constitution des fichiers de données médicales personnelles (1).

Assurer la communication d'informations confidentielles à de nombreux intervenants tout en garantissant leur sécurité est une spécificité du traitement des informations médicales personnelles. Des protections parfois complexes doivent donc être mises en oeuvre pour concilier ces deux notions quelque peu antagonistes que sont sécurité et communication.

Protection des données médicales informatisées

Le médecin a l'obligation d'assurer la confidentialité des informations médicales qui lui sont confiées par ses patients. Cette obligation est définie par les articles 4 et 73 du code de déontologie médicale.

Art. 4

"Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi.

Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris."

Art. 73

"Le médecin doit protéger contre toute indiscretion les documents médicaux concernant les personnes qu'il a soignées ou examinées, quels que soient le contenu et le support de ces documents.

Il en va de même des informations médicales dont il peut être le détenteur.

Le médecin doit faire en sorte, lorsqu'il utilise son expérience ou ses documents à des fins de publications scientifiques ou d'enseignement, que l'identification des personnes ne soit pas possible.

A défaut, leur accord doit être obtenu."

et par l'article 226-13 du code pénal qui prévoit

"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 1 000 000 F d'amende. "

L'enregistrement et le traitement automatisé de ces informations aggravent les responsabilités des médecins à leur égard en ajoutant à la protection de leur confidentialité, l'obligation d'assurer la protection de leur intégrité et de leur disponibilité ainsi que le définit l'art. 226-17 du code pénal :

"Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende."

Les logiciels diffusés pour l'informatisation du cabinet médical doivent intégrer les protections

nécessaires pour assurer la sécurité des informations médicales et permettre ainsi au médecin de satisfaire ses obligations. D'ores et déjà ces logiciels devraient tous comporter une protection des accès par mot de passe d'au moins 8 caractères. Ce mot de passe, choisi par le médecin, est un code secret qui ne doit être connu que de lui seul, et si la secrétaire a la charge de saisir les informations médicales, elle doit disposer de son propre code d'accès. Le code doit être suffisamment complexe et formé d'une succession de lettres et de chiffres sans signification particulière notamment à des fins mnémotechniques trop faciles à découvrir.

Dans un très proche avenir tous les médecins seront équipés d'une carte de professionnel de santé (CPS) à même de les identifier, d'authentifier leur identité et de signer électroniquement en fournissant un code personnel selon un dispositif similaire à celui des cartes bancaires. Les logiciels du cabinet médical devront être capables d'intégrer d'emblée cette utilisation de la carte de professionnel comme clé d'accès obligatoire aux informations médicales.

De nombreux logiciels médicaux assurent la communication du médecin avec ses confrères sur des réseaux externes au cabinet. Les sécurités nécessaires à la protection des informations médicales personnelles qui circuleront à l'extérieur impliquent leur cryptage conformément aux recommandations de la CNIL (4). Par ailleurs toute connexion dans un réseau comporte un risque d'intrusion de la part d'un tiers extérieur relié au réseau et des barrières logicielles, dispositifs "coupe-feu" ou "fire wall", doivent être prévus pour interdire l'accès aux informations depuis l'extérieur. C'est ainsi que les liaisons Internet doivent être étroitement protégées.

Enfin les atteintes à l'intégrité et à la disponibilité des informations résultent non seulement de malveillances mais le plus souvent d'accidents techniques ou de maladroites et des sauvegardes doivent être assurées. Il est du devoir et de l'intérêt du médecin de les réaliser régulièrement avec l'aide éventuelle de logiciels appropriés. Ces logiciels archivent automatiquement les fichiers actifs d'une session de travail, ou de manière plus contraignante, prévoient de bloquer l'utilisation de l'ordinateur tant que l'utilisateur n'a pas satisfait à l'obligation de sauvegarde dont il a lui-même fixé la fréquence. Des logiciels anti-virus sont à utiliser pour prévenir la "contamination" ou "décontaminer" le système et assurer sa sécurité.

4) CNIL: 17e rapport d'activité pour 1996.

Respect de la finalité du recueil et des transmissions des données médicales personnelles

Bien des solutions informatiques proposées par les sociétés de service pour informatiser les cabinets médicaux comportent aujourd'hui une mise en réseau. Certaines d'entre elles ont même pour particularité d'imposer la société de service comme un intermédiaire obligé qui s'interpose entre les médecins du réseau.

C'est un choix d'organisation qui n'est pas toujours justifié et il est préférable d'aboutir à une communication libre de médecin à médecin grâce à un véritable "maillage" tel que le permettent les réseaux de type Intranet. Un réseau qui ne privilégie pas l'un des intervenants assure mieux leur indépendance et la sécurité des informations. Or dans certaines des organisations proposées, et c'est là un point sensible pour la sécurité, la structure du réseau est une configuration en étoile, centrée sur la société commerciale qui collecte des informations en échange d'un certain nombre de prestations. Ces prestations correspondent souvent à la fourniture du matériel informatique nécessaire à la gestion du cabinet médical en contrepartie du recueil d'informations sur l'activité et les prescriptions des médecins, ou de leur participation à des essais thérapeutiques et des enquêtes médico-économiques.

Dans son organisation commerciale, la société éditrice des logiciels se réserve habituellement la possibilité de recevoir, ou même d'extraire directement à partir des fichiers des médecins, un certain nombre d'informations pour lesquelles elle affirme garantir l'anonymat des patients. La CNIL exige que le médecin soit en mesure de vérifier la réalité de cet anonymat. Les informations collectées auprès des cabinets médicaux sont rassemblées et traitées sur le système informatique de la société puis rétrocédées à d'éventuels clients, après anonymat des médecins en conformité avec l'article L.365-2 du code de la santé publique (5).

Malgré cet aspect rassurant, une telle organisation risque de mettre en danger le respect du secret médical et l'indépendance des médecins comme on le verra plus loin.

Dans un certain nombre de cas une association de médecins type loi 1901 prend la place de la société commerciale ou travaille étroitement avec elle. Ceci ne modifie en rien les contraintes déontologiques à respecter. Si l'association peut apporter aux médecins l'avantage d'une concertation sur les conditions de bon fonctionnement du système informatique, elle n'est pas une garantie du respect de la sécurité des informations et de l'indépendance des médecins.

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

Lorsque le médecin adhère à une organisation informatique centralisée il doit s'assurer qu'aucune information et aucun traitement des informations transmises à la société commerciale ne permettent l'identification des personnes concernées. La simple élimination du nom du malade ne suffit pas à garantir l'anonymat. Il faut tenir compte des prescriptions beaucoup plus exigeantes de l'article 4 de la loi du 6 janvier 1978 qui permet de considérer comme indirectement nominatif tout faisceau d'informations tel que par exemple l'association du sexe, de l'âge, du code postal et de la date de consultation. La directive européenne déjà citée va elle-même dans ce sens. Par ailleurs, le médecin doit garder la maîtrise de la transmission des informations à partir de son système informatique. La transmission d'informations doit être un acte volontaire, résultat d'une démarche active sur la base d'un engagement contractuel qui aura clairement défini les objectifs du recueil et du transfert d'informations.

Indépendance des médecins du réseau

La participation des médecins des réseaux informatiques mis en place par une société commerciale ne doit pas mettre en cause le principe déontologique de l'indépendance médicale. Tout comme la rémunération autorisée par l'article L.365-1 doit correspondre à une juste rétribution du travail fourni, et non pas à des incitations directes ou indirectes à la prescription, le fichier médical du médecin ne doit pas devenir le gage d'une transaction commerciale.

La mise à disposition des médecins d'un système informatique pour gérer les dossiers médicaux de leurs patients, et même l'ensemble des activités de leur cabinet, oblige à prévoir les conditions dans lesquelles leur système informatique restera fonctionnel en cas de rupture du contrat. Le médecin est-il véritablement libre de rompre son contrat ? Il conviendrait de prévoir des clauses de rachat acceptables qui préservent son indépendance.

Une rupture de contrat avec une société commerciale qui aboutirait au retrait du système informatique par cette dernière pourrait être considérée comme un manquement à l'un des trois piliers de la sécurité, c'est-à-dire la disponibilité des informations des patients. De plus elle serait à l'origine d'un préjudice potentiel pour ces patients.

Les conditions de la sécurité des informations, tant au niveau du fichier du médecin que des fichiers de la société commerciale, de même que les garanties d'indépendance du médecin vis-à-vis de cette société doivent donc être définies par voie contractuelle de manière explicite et détaillée.

CONCLUSION

Face aux conséquences déontologiques et légales dont ils assument la responsabilité, les médecins qui informatisent leur cabinet doivent exiger de leur fournisseur les garanties appropriées pour que les droits de leurs patients ne soient pas enfreints à leur insu.

En cas de malversation à l'encontre des données personnelles de leurs patients, même si elle n'est pas de leur fait, les médecins pourront se voir reprocher de s'être montré négligents dans le choix de leur équipement si celui-ci ne comporte pas les sécurités requises par l'exercice médical.

Les médecins doivent donc exiger de leur fournisseur informatique que soient assurées la confidentialité, la disponibilité et l'intégrité des informations qui leur sont confiées, que le contrat qui les lie avec lui ne porte pas atteinte à la déontologie médicale en particulier à leur indépendance, et qu'ils disposent des moyens de vérifier que les garanties proposées soient efficaces et pérennes.