



COMMISSION
NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

LES GUIDES DE LA CNIL

PROFESSIONS DE SANTÉ : Fiches thématiques



Vous avez décidé d'informatiser la gestion de votre cabinet. Pour cela, vous utilisez un ou plusieurs logiciels conçus pour gérer, sous forme de fichiers, les renseignements concernant vos clients et le cas échéant, votre personnel. Si ce n'est déjà fait, vous envisagez également de recourir à des réseaux pour recevoir et transmettre des informations à caractère médical, qu'il s'agisse des feuilles de soins, de messages entre confrères, de résultats d'analyse ou de gestion partagée de dossiers médicaux ...

Ces informations, parce qu'elles relèvent de l'intimité de la vie privée et que leur divulgation est susceptible de porter atteinte aux droits et libertés des personnes concernées, doivent être **particulièrement protégées**.

C'est l'objectif que le respect de la loi « informatique et libertés » vous permet d'atteindre.

Pour préserver toute atteinte aux libertés individuelles et à la vie privée de vos patients, **la loi « Informatique et Libertés » du 6 janvier 1978** définit des règles à respecter lors de la collecte, du traitement, de la conservation et de la transmission des informations nominatives.

Les informations nominatives ne peuvent être recueillies et traitées que pour une **finalité déterminée et légitime**. Ainsi les informations que vous recueillez sur vos patients ne peuvent être utilisées que pour faciliter leur suivi médical et dans les conditions déterminées par la loi, pour les besoins de la santé publique en particulier dans le domaine de la recherche médicale.

Elles ne peuvent en aucun cas faire l'objet d'une exploitation commerciale.

Ces informations, couvertes par le secret médical, ne peuvent être communiquées qu'à des destinataires habilités et des personnes autorisées en vertu de la loi.

En tant que responsable du fichier, vous êtes astreint à une **obligation de sécurité**. Ainsi vous devez prendre toutes précautions utiles pour garantir la confidentialité des données, éviter leur divulgation et empêcher leur altération.

Les personnes concernées doivent être **informées** de l'informatisation de leurs données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi « Informatique et Libertés » : droit d'accès direct aux informations qui les concernent, droit de rectification des informations incomplètes ou inexacts. ▶

La Commission Nationale de l'Informatique et des Libertés vous aide

La CNIL, autorité administrative indépendante, est chargée de veiller au respect des dispositions de la loi. A ce titre, elle a une triple mission d'information et de conseil dans l'exercice des droits, de conseil, d'expertise et de veille technologique.

La CNIL dispose de pouvoirs particuliers pour faire respecter la loi : elle contrôle la mise en œuvre des fichiers informatiques et peut également procéder à des vérifications sur place.

L'ensemble de ces informations est également disponible
sur le site Internet de la CNIL :

www.cnil.fr

FICHES THÉMATIQUES

SANTÉ

ÉDITION 02/2003



Sommaire

UN IMPÉRATIF : LA SÉCURITÉ	page 5
SÉCURITÉS POUR LES APPLICATIONS EN RÉSEAU	page 6
SOUS-TRAITANCE : CLAUSES DE CONFIDENTIALITÉ	page 7
DONNÉES DE SANTÉ, E-MAIL ET FAX	page 9
L'ACCÈS AU DOSSIER MÉDICAL	page 10
SESAM VITALE : LES CONTRAINTES DE CONFIDENTIALITÉ	page 12
LE NUMÉRO DE SÉCURITÉ SOCIALE	page 13
COMMUNICATION DES DONNÉES DE SANTÉ	page 14
COMMUNICATION A DES TIERS AUTORISÉS	page 16
DÉCLARATION OBLIGATOIRE DU VIH	page 17
LES SITES WEB DE SANTÉ	page 18
LE DOSSIER MÉDICAL SUR INTERNET	page 19



Assurer la sécurité de vos fichiers c'est pouvoir garantir, à vos patients la confidentialité des données qui y figurent et disposer, en permanence, d'un outil de travail fiable.

Il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées¹ et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées surtout s'il s'agit d'informations couvertes par le secret médical.²

La CNIL préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite de l'ordinateur, de sa configuration, de l'existence d'une connexion à Internet... (voir les recommandations de sécurité pour les applications fonctionnant en réseau) et recommande de chiffrer par cryptage les données figurant sur votre disque dur et sur vos supports de sauvegarde.

Les précautions élémentaires :

- **Protégez** l'accès à l'ordinateur, au système d'exploitation et aux applications par des mots de passe **individuels, propres à chaque utilisateur**. Le mot de passe choisi doit, si possible, être **alphanumérique**, d'une longueur de **6 caractères au moins**, pas trop courant (évités initiales, nom, prénom, etc.), changé périodiquement et conservé confidentiellement.
- Ne collez pas votre code personnel sur votre carte de professionnel de santé ni sur un autre support. Cette carte est strictement personnelle et votre responsabilité pourrait être engagée en cas d'utilisation frauduleuse de celle-ci (ex. envoi de feuilles de soins falsifiées).
- En cas d'absence, même temporaire, pensez à éteindre votre ordinateur, ou à mettre en place un écran de veille protégé par un mot de passe, et ne laissez pas votre carte de professionnel de santé dans le lecteur.
- Utilisez des antivirus régulièrement mis à jour et installez un « pare-feu » (firewall) logiciel si vous utilisez Internet. Les risques d'intrusion dans votre système informatique sont réels et peuvent conduire à l'implantation de virus ou de programmes « espions ».
- Effectuez régulièrement des sauvegardes sur des supports amovibles (CD-Rom, disquettes) et conservez-les dans un lieu différent de votre cabinet.
- Assurez-vous, lors de l'achat de votre équipement informatique, que celui-ci comporte les dispositifs répondant à l'obligation de sécurité qui vous incombe (ex : des disques durs amovibles se branchant sur le port USB).
- Vérifiez que le contrat d'assistance et de maintenance comporte une clause de confidentialité rappelant au fournisseur ses obligations (cf. proposition de clause type).
- Sensibilisez votre personnel à ces mesures de sécurité.

¹ Article 29 de la loi « informatique et libertés »

² Articles 226-13, 226-17 et suivants du Code pénal

La gestion des mots de passe

- Code utilisateur individuel distinct du nom de l'utilisateur.
- Interdiction de réutiliser les trois derniers mots de passe (blocage du système).

Modalités de connexion et de déconnexion

- Impossibilité pour les utilisateurs de se connecter à plusieurs sous le même code utilisateur et le même mot de passe.
- Indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage sur l'écran, des dates et heures de la dernière connexion sous les mêmes code utilisateur et mot de passe.
- Journalisation des connexions et exploitation de ces données.
- Après plusieurs frappes (ex. trois) incorrectes successives du mot de passe (associé à un code utilisateur correct), blocage de l'accès et message demandant à l'utilisateur d'appeler le responsable du système.
- Procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné (time out).
- Utilisation dans la mesure du possible de cartes à puce ou dispositifs analogues.

La confidentialité des données

- Utilisation dans la mesure du possible du codage des données nominatives.
- Cryptage de tout ou partie des données dans le cadre de la réglementation française et européenne en vigueur.

L'intégrité des données

- Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises.
- Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données.

En cas d'architecture client-serveur

- Prendre les dispositions nécessaires pour gérer le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun : limitation au minimum du transfert de fichiers complets, limitation du volume des informations rapatriées, journalisation des requêtes au niveau du serveur.
- Restriction d'accès aux données en fonction des habilitations.
- Séparation des réseaux de gestion administrative et de suivi médical.

Connexion à Internet

- En cas de connexion d'un des serveurs du réseau à Internet, prévoir des mesures de sécurités particulières comme la séparation physique des deux réseaux, la mise en place d'un firewall ou de barrières de protection logicielles.
- Lorsque des données de santé sont transférées via Internet, il convient de recourir au chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits).

CLAUSES DE CONFIDENTIALITÉ

Modèle de clauses de confidentialité pouvant être utilisées en cas de sous-traitance

Les supports informatiques et documents fournis par la société X à la société Y restent la propriété de la X.

Les données contenues dans ces supports et documents **sont strictement couvertes par le secret professionnel** (article 226-13 du code pénal), il en va de même pour toutes les données dont Y prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 29 de la loi du 6 janvier 1978 relative à l'Informatique, aux Fichiers et aux Libertés, Y s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Y s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel:

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

A ce titre, Y ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de X.

X se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par Y.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

X pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

En cas d'opération de maintenance ou de télémaintenance

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à X.

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y prendra toutes dispositions afin de permettre à X d'identifier la provenance de chaque intervention extérieure. A cette fin, Y s'engage à obtenir l'accord préalable de X avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de X et Y, mentionnant les date et nature détaillées des interventions de télémaintenance ainsi que les noms de leurs auteurs.

La messagerie électronique et le fax, même s'ils apportent un gain de temps, ne constituent pas a priori un moyen de communication sûr pour transmettre des données médicales nominatives.

Une simple erreur de manipulation (e-mail erroné, erreur de numérotation du fax destinataire...) peut conduire à divulguer à des destinataires non habilités des informations couvertes par le secret médical et à porter ainsi gravement atteinte à l'intimité de la vie privée des personnes.

En outre la transmission par e-mail de données nominatives sur l'état de santé d'une personne comporte, compte tenu de l'absence générale de confidentialité du réseau Internet, **des risques importants de divulgation de ces données et d'intrusion** dans les systèmes informatiques internes.

Dès lors, des précautions particulières s'imposent.

Si vous êtes amené à utiliser une messagerie électronique, vous devez impérativement recourir à une **messagerie sécurisée** intégrant un module de chiffrement (cryptage) des données (les messages transitent sur des serveurs intermédiaires et restent stockés sur votre serveur de messagerie tant que vous ne les avez pas téléchargés sur votre micro-ordinateur). Ces produits sont aujourd'hui disponibles sur le marché. Renseignez-vous auprès de votre fournisseur d'accès.

Si vous êtes amené à utiliser **le fax**, il est recommandé de mettre en place les mesures suivantes :

- le fax doit être situé dans un local médical, physiquement contrôlé et accessible uniquement au personnel médical et paramédical ;
- l'impression des messages doit être subordonnée à l'introduction d'un code d'accès personnel ;
- lors de l'émission des messages, le fax doit afficher l'identité du fax destinataire afin d'être assuré de l'identité du destinataire ;
- doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
- pré enregistrer dans le carnet d'adresses des fax (si cette fonctionnalité existe) les destinataires potentiels.

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a posé le principe de l'accès direct du patient à l'ensemble des informations de santé le concernant et le décret du 29 avril 2002³ a organisé cet accès.

Néanmoins le patient peut toujours, s'il le souhaite, accéder à ces données par l'intermédiaire d'un médecin de son choix.

La communication doit être faite au plus tard dans les huit jours suivant la demande et au plus tôt dans les 48 heures. Si les informations remontent à plus de cinq ans, le délai est porté à deux mois. Cette période de cinq ans court à compter de la date à laquelle l'information médicale a été constituée.

La présence d'une tierce personne peut être recommandée par le médecin mais ne peut empêcher un accès direct au dossier en cas de refus du patient de suivre cette recommandation.

Qui peut demander l'accès au dossier médical ?

L'accès au dossier médical peut être demandé auprès du professionnel de santé ou de l'établissement de santé, par la personne concernée, son ayant droit en cas de décès de cette personne, le titulaire de l'autorité parentale, le tuteur ou le médecin désigné comme intermédiaire.

Quelles sont les informations communicables ?

Toute personne a accès à l'ensemble des informations concernant sa santé, c'est à dire à toutes les données qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment les résultats d'examen, les comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, les protocoles et prescriptions thérapeutiques mis en oeuvre, les feuilles de surveillance, les correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers⁴.

Ces informations sont communicables qu'elles soient sous forme papier ou sur support informatique. La communication, en langage clair (par exemple, par l'indication de la signification des codes utilisés) doit être conforme au contenu des enregistrements.

³ Décret n°2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique

⁴ Article L. 1111-7 alinéa du CSP ; voir également l'article R. 710-2-2 du CPS relatif au contenu du dossier médical

Quelles sont les modalités d'accès et de communication ?

La demande est adressée au professionnel de santé ou au responsable de l'établissement ou à la personne désignée à cet effet par ce dernier.

L'accès aux données se fait, au choix du demandeur, soit par consultation sur place avec éventuellement remise de copies, soit par l'envoi des documents (si possible en recommandé avec accusé de réception). Les frais de délivrance de ces copies sont à la charge du demandeur et ne sauraient excéder le coût de la reproduction et, le cas échéant, de l'envoi des documents.

Préalablement à toute communication, le destinataire de la demande doit vérifier l'identité du demandeur (ou la qualité de médecin de la personne désignée comme intermédiaire).

En cas de refus ou d'absence de réponse du professionnel ou de l'établissement de santé, le demandeur peut saisir la CNIL.

Cas particuliers

- Une **personne mineure** peut s'opposer à ce qu'un médecin communique au titulaire de l'autorité parentale des informations qui la concernant. Le médecin fait mention écrite de cette opposition.

Si le titulaire de l'autorité parentale saisit le médecin d'une demande d'accès, le praticien doit s'efforcer d'obtenir le consentement du mineur. Si ce dernier maintient son opposition, la demande du titulaire de l'autorité parentale ne peut être satisfaite.

- **L'ayant droit d'une personne décédée** peut accéder aux informations concernant le défunt dans la mesure où ces données sont nécessaires pour connaître les causes de la mort, défendre la mémoire du défunt ou faire valoir des droits, sauf volonté contraire exprimée par la personne décédée.

L'ayant droit doit indiquer le motif de sa demande d'accès. Tout refus doit être motivé. La délivrance d'un certificat médical ne comportant pas d'information couverte par le secret professionnel ne peut être refusée.

- En cas **d'hospitalisation d'office ou sur demande d'un tiers**, le détenteur des informations peut estimer que la communication doit avoir lieu par l'intermédiaire d'un médecin. Dans ce cas il en informe l'intéressé. Si le demandeur refuse de désigner un médecin, le détenteur des informations saisit la Commission départementale des Hospitalisations psychiatriques. Le demandeur peut également saisir cette Commission. L'avis de la Commission est notifié au demandeur et au détenteur des données et s'impose à eux.

LES CONTRAINTES DE CONFIDENTIALITÉ

La mise en œuvre du dispositif SESAM Vitale résulte de la loi : plusieurs dispositions du code de la sécurité sociale (article L 161-29, L161-31 et suivants, R 161-34 et suivants) ont défini les conditions dans lesquelles en particulier la télétransmission des feuilles de soins devait s'opérer.

Le déploiement de ce dispositif s'est donc traduit par une multiplication des fichiers informatiques et par un développement considérable des échanges d'informations. La CNIL suit bien entendu avec une particulière attention sa mise en œuvre et est très attentive aux mesures prises pour assurer la confidentialité tant des télétransmissions que des fichiers constitués par les professionnels de santé et les caisses de sécurité sociale, comme en témoignent les nombreux avis rendus sur le sujet depuis 1998.

Ainsi, la Commission préconise tout particulièrement le cryptage des informations lors de leur transmission pour éviter leur divulgation et leur utilisation à d'autres fins, dès lors qu'en particulier il est fait appel à des prestataires intermédiaires.

La transmission des feuilles de soins électroniques entre le professionnel de santé et les organismes d'assurance maladie peut être effectuée soit directement, soit par l'intermédiaire d'organismes concentrateurs techniques qui reçoivent alors les feuilles de soins et effectuent, éventuellement après traitement des informations, le routage de celles-ci vers les organismes d'assurance maladie obligatoires et/ou complémentaires concernés.

La CNIL a, dès 1993, souligné que ces intermédiaires ne devaient, assurer aucun traitement particulier des données pour leur propre compte, effectuer ni enrichissement ni consultation hormis celles rendues nécessaires pour la maintenance des matériels utilisés, ni cession des informations.

A cet égard, un encadrement juridique de l'activité de ces organismes apparaît aujourd'hui indispensable.

Mais les fichiers des professionnels de santé et des caisses de sécurité sociale doivent aussi être sécurisés. La CNIL diffuse à cet effet des recommandations de sécurité (cf. fiche recommandations de sécurité).

Aux termes des **articles R115-1 et R115-2 du Code de la sécurité sociale**, les professionnels de santé qui dispensent des actes ou prestations pris totalement ou partiellement en charge par l'assurance maladie sont autorisés à utiliser les numéros de sécurité sociale de leurs patients dans le cadre des échanges avec les organismes d'assurance maladie obligatoire ou complémentaire.

Les professionnels de santé peuvent donc enregistrer dans leurs applications informatiques le numéro de sécurité sociale de leurs patients tel qu'il figure sur la carte vitale pour correspondre avec les organismes de sécurité sociale mais ne peuvent pas l'utiliser comme identifiant du dossier médical. La CNIL n'a été saisie d'aucun projet national en ce sens.

A cet égard, la CNIL suit avec attention les études menées par le ministère chargé de la santé et le groupement de modernisation du système d'information hospitalier (GMSIH) sur l'identifiant unique permanent du patient.

Les données de santé peuvent être communiquées et utilisées dans les conditions déterminées par la loi, que dans l'intérêt direct du patient (assurer son suivi médical, faciliter sa prise en charge par l'assurance maladie obligatoire...) ou pour les besoins de la santé publique.

Hypothèses dans lesquelles vous êtes autorisé à communiquer des données personnelles de santé

L'équipe soignante

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé autorise expressément les professionnels de santé à échanger des informations relatives à un même patient, sauf opposition de sa part, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge possible. Lorsque le malade est pris en charge par une équipe de soins dans un établissement de santé, les informations sont réputées confiées à l'ensemble de l'équipe.

La sécurité sociale

L'article L. 161-29 du code de la sécurité sociale prévoit que les professionnels de santé communiquent, sous forme nominative, aux organismes d'assurance maladie obligatoire, le code détaillé des actes, prestations et pathologies diagnostiquées.

Les déclarations obligatoires de certaines maladies

En application de l'article L 3113-1 du code de la santé publique, les professionnels de santé sont tenus de déclarer aux autorités sanitaires certaines maladies infectieuses qui nécessitent une intervention urgente (ex. : légionellose) ou dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique (cf. fiche la déclaration obligatoire du VIH/Sida).

La recherche médicale

La loi du 1^{er} juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé permet aux professionnels de santé de transmettre les données personnelles de santé qu'ils détiennent dans le cadre de recherches dans le domaine de la santé (études épidémiologiques, observationnelles, essais cliniques, pharmacovigilance). La mise en œuvre de ces traitements doit répondre à des règles spécifiques. A ce titre, les patients inclus dans l'étude doivent être informés au préalable, individuellement, de leurs droits pour être en mesure de s'opposer, s'ils le souhaitent, à la transmission de données les concernant (pour plus d'informations se reporter au site de la CNIL : <http://www.cnil.fr/declarer/index.htm>).

L'évaluation des pratiques de soins

L'article 41 de la loi du 27 juillet 1999 précise les conditions dans lesquelles peuvent être transmises et exploitées à des fins d'évaluation des pratiques de soins et de prévention les données de santé indirectement nominatives (à l'exclusion de celles comportant le nom, le prénom du patient ou son numéro de sécurité sociale), qu'elles soient issues des fichiers des professionnels de santé, des systèmes d'information hospitaliers, ou des fichiers des caisses de sécurité sociale, (pour plus d'informations <http://www.cnil.fr/declarer/index.htm>).

Si vous êtes sollicité par un laboratoire, une société de service ou encore par un organisme pour participer à une recherche médicale ou une étude relative à l'évaluation des pratiques de soins, **une autorisation spécifique doit être demandée par cette structure et obtenue auprès de la CNIL.**

Les utilisations interdites

Les informations médicales concernant vos patients ne peuvent en aucun cas faire l'objet d'une cession ou d'une exploitation commerciale.

En outre, en application de l'article L. 4113-7 du code de la santé publique, la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des données personnelles de santé, sont interdites (même rendues anonymes à l'égard des patients) dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur.

Soyez vigilant

S'il vous est proposé de fournir des informations sur vos prescriptions médicales ou vos pratiques médicales en contrepartie de l'informatisation de votre cabinet ou d'équipement informatique permettant notamment de gérer les dossiers médicaux ou de télétransmettre les données, soyez vigilant. Vous devez, au préalable, être clairement informé en obtenant des réponses précises aux questions suivantes :

- Identité du ou des organismes responsables de ce dispositif de recueil ?
- Finalité et conditions d'utilisation des données par l'organisme qui les réceptionnera ?
- Nature exacte des informations susceptibles d'être communiquées et des modalités techniques selon lesquelles elles sont susceptibles d'être transmises ?
- Organismes susceptibles d'être destinataires des informations transmises ?
- Modalités selon lesquelles vous pourrez exercer votre droit d'accès, de rectification et de suppression pour les données vous concernant auprès du responsable du dispositif ?
- Modalités exactes de mise à disposition de moyens informatiques ?
- Conséquences à votre égard de la participation à un dispositif de télétransmission (ex.: obligation de transmettre à périodicité régulière, de participer à des études...) et dispositions prévues en cas d'abandon de collaboration ? En effet, l'organisme doit s'engager à fournir les moyens nécessaires pour vous permettre de continuer à gérer votre fichier ou d'effacer, avant restitution du matériel informatique, les informations nominatives enregistrées.

De façon générale, les demandes de renseignements sur vos patients ne peuvent être satisfaites que pour des autorités publiques qui disposent, dans le cadre de l'exercice de leur mission, de prérogatives particulières pour se voir communiquer des informations : ces autorités sont alors appelées Tiers Autorisés.

Ces demandes de communication doivent être ponctuelles et viser des personnes identifiées directement ou indirectement ; le fondement juridique ainsi que les catégories d'informations sollicitées doivent être précisés. En cas de doute sur les textes juridiques invoqués vous pouvez interroger la CNIL.

AUTORISES. Les autorités judiciaires, procureurs de la République, juges d'instruction, officiers de police nationale et de gendarmerie, doivent être considérées, lorsqu'elles agissent en flagrant délit ou sur commission rogatoire, comme tiers autorisés à obtenir communication d'informations issues de votre fichier sans que vous puissiez vous y opposer.

Toutefois, conformément à l'article 56-1 du Code de procédure pénale, la communication des informations doit s'opérer en présence conjointe du professionnel de santé et d'un membre du Conseil de l'Ordre et ne porter que sur les documents strictement indispensables à l'enquête.

AUTORISES. Les experts désignés par une juridiction administrative ou civile, ne peuvent obtenir communication des informations que sous réserve du consentement de votre patient.

AUTORISES. Les agents de l'administration fiscale ont, en application de l'article L.86 du Livre des Procédures Fiscales, un droit de communication à l'égard des membres des professions de santé et peuvent donc obtenir dans le cadre de leur mission un certain nombre de documents y compris extraits de fichiers informatiques. Toutefois, selon une jurisprudence constante du Conseil d'État, les dispositions de l'article 226-13 du Code pénal relatif au secret professionnel s'opposent à ce que les membres des professions auxquelles elles s'appliquent, fassent connaître à des tiers et donc à l'administration fiscale le nom des personnes qui ont eu recours à leurs soins.

NON AUTORISES Les médecins des compagnies d'assurance, en revanche, ne peuvent être considérés comme tiers autorisés à obtenir le dossier médical du patient. Dans ces conditions, et dans l'attente d'un dispositif juridique spécifique au secteur des assurances, la Commission suggère que le patient communique à son médecin traitant les indications figurant dans sa police d'assurance et notamment les clauses d'exclusion, ainsi que les critères d'appréciation médicale définis par la compagnie de façon à ce que ce médecin ne communique au médecin conseil de l'assurance qu'un certificat médical adapté, indiquant si le cas du patient relève ou non des clauses d'exclusion du contrat.

NON AUTORISES Les employeurs ne peuvent en aucun cas obtenir communication d'informations nominatives à caractère médical.

Dans tous les cas de demande de communication d'informations issues de votre fichier, **sachez que le recueil du consentement de votre patient ne suffit pas à vous exonérer de votre obligation de secret professionnel telle que définie par le code pénal.**

DU VIH

Certaines maladies infectieuses qui nécessitent une intervention urgente locale, nationale ou internationale ou dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique doivent faire l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire (article L 3113-1 du code de la santé publique).

La CNIL a autorisé la mise en place par l'Institut national de veille sanitaire (InVS) du système de surveillance épidémiologique des maladies infectieuses à déclaration obligatoire dont le VIH/SIDA. Vingt-cinq maladies sont ainsi concernées par cette surveillance (délibération du 19 novembre 2002 accessible sur le site www.cnil.fr).

La Commission a considéré que l'anonymat des personnes, tel qu'il est imposé par la loi, était garanti par la technique d'anonymisation - double et irréversible - retenue par l'InVS et répondait à ses recommandations.

Cette technique permet, à partir de l'initiale du nom, du prénom, du sexe et de la date de naissance de la personne, de générer un code de 16 caractères qui doit, à l'exclusion de toute donnée nominative, figurer sur la déclaration transmise à la DDASS, à charge pour elle de la transmettre à l'InVS qui procédera à une seconde anonymisation.

La liste de correspondance entre l'identité de la personne et le code d'anonymat doit être conservée de façon confidentielle pendant six mois afin de permettre les contrôles de validité nécessaires. A l'issue de ce délai, cette liste doit être détruite.

Il vous appartient en tant que professionnel de santé susceptible de diagnostiquer une séropositivité au VIH (médecin et biologiste) de demander à l'InVS le logiciel d'anonymisation, disponible gratuitement, et l'ensemble des documents explicatifs accessibles sur le site de l'InVS (www.invs.fr).

L'InVS met également à votre disposition des dépliants d'information qui doivent être remis aux personnes concernées.

Restent exclus du dispositif les centres de dépistage anonymes et gratuits (CDAG).

La consultation des sites web consacrés à la santé répond à un besoin légitime d'information mais appelle des précautions particulières compte tenu des possibilités d'exploitation, notamment commerciale, des informations laissées sur le site (qu'il s'agisse d'informations communiquées par l'internaute ou des données de navigation).

Afin que les internautes appelés à consulter ces sites soient clairement informés de l'usage fait de leurs données, des destinataires de celles-ci et de leurs droits et des mesures de sécurité prises pour garantir la confidentialité de leurs données, la CNIL a été amenée, à la suite d'un audit effectué sur 60 sites de santé, à émettre un certain nombre de recommandations à l'attention des responsables de sites dont les principales sont énumérées ci-après (la liste complète de ces recommandations figure dans la **délibération du 8 mars 2001 accessible sur www.cnil.fr**).

- L'indication de la raison sociale et du siège social du site doit apparaître clairement dès la page d'accueil (par exemple sous le titre : « qui sommes-nous ? »).
- Le site doit comporter une rubrique « Informatique et Libertés/Protection des données personnelles », accessible depuis la page d'accueil ; cette rubrique doit notamment spécifier l'usage qui sera fait des données de santé communiquées par l'internaute et/ou par le professionnel de santé, et préciser en particulier qu'elles ne feront l'objet d'aucune exploitation commerciale et ne seront transmises à quiconque à des fins commerciales ou de prospection commerciale.
- En cas de cession ou de mise à disposition de tiers, à des fins commerciales, de l'adresse e-mail ou des coordonnées de l'internaute, (à l'exclusion donc de toute donnée de santé), l'internaute doit en être informé et mis en mesure de s'y opposer, par le biais d'une case à cocher.
- En cas d'exploitation, à des fins commerciales, des données de connexion sous une forme nominative, l'accord des personnes doit être recueilli par le biais d'une case à cocher.
- Il doit être fait mention des coordonnées ou de l'adresse e-mail du service ou du correspondant chargé de répondre aux demandes de droit d'accès présentées par les internautes. Ce droit doit pouvoir s'exercer à tout moment en ligne.
- Toute collecte directe de données auprès de l'internaute (sous forme ou non de questionnaire) doit être accompagnée d'une information précisant, sur le support de collecte, le caractère obligatoire ou facultatif du recueil de chaque information demandée (par exemple par le biais d'un astérisque).
- Des mesures de sécurité reposant notamment sur le recours à des moyens de chiffrement ainsi que sur des dispositifs de journalisation des connexions doivent être mises en place pour assurer la confidentialité des données.

NB : cf. également la fiche « le dossier médical sur Internet ».

Pour assurer la coordination et la continuité des soins entre la ville et l'hôpital, pour améliorer la prise en charge de telle ou telle maladie chronique, pour assurer une surveillance épidémiologique ou pour participer à la conduite d'essais cliniques, le partage de l'information médicale devient aujourd'hui une nécessité pour l'ensemble des professionnels de santé et correspond à une demande accrue des patients.

L'utilisation d'Internet comme support de communication de l'information médicale appelle cependant une vigilance particulière compte tenu de l'absence de confidentialité propre au réseau et des possibilités d'utilisation détournée des données.

La gestion sur Internet du dossier médical ne peut être envisagée que dans le respect des conditions suivantes.

- Le patient doit être clairement informé des modalités de constitution, de mise à jour et d'utilisation et de conservation de ses données médicales ainsi que des conditions dans lesquelles il pourra lui-même accéder à ses données (le recours éventuel à un prestataire extérieur « hébergeur des données » doit être précisé). A cet effet, un document explicatif complet doit lui être remis. **Son consentement exprès doit être recueilli**. Ce consentement peut être retiré à tout moment.
- Tout professionnel de santé appelé à gérer des dossiers médicaux sur Internet doit être préalablement informé des conditions d'utilisation de ces dossiers, et des modalités de sa participation. Il doit être clairement informé de ses responsabilités dans la gestion des dossiers médicaux. Ces précisions doivent être apportées dans le cadre d'un document de nature contractuel. Les modalités retenues pour l'identification et l'authentification, en particulier le recours à la carte de professionnel de santé ainsi que les mesures de sécurité particulières doivent être décrites dans ce document.
- Les données appelées à circuler sur Internet doivent faire l'objet d'une procédure de chiffrement renforcée, le déchiffrement de ces données ne pouvant être effectué que par les professionnels de santé disposant de droits d'accès aux données. A cet effet, une politique d'accès aux données doit être prévue.

En cas de recours à un prestataire extérieur pour héberger les dossiers médicaux, les conditions de sécurité mises en place par la société hébergeur doivent être clairement définies (cf. recommandations de sécurité pour les applications en réseau).

Sachez qu'en application de la loi du 4 mars 2002 sur les droits des malades, il a été prévu que les sociétés qui hébergent des données médicales devraient faire l'objet **d'une procédure d'agrément** dans des conditions qui seront prochainement définies par décret (article L1111-8 du code de la santé publique).

Pour les réseaux de soins, sachez également que le code de la santé publique impose désormais que les critères de qualité des réseaux et leurs conditions de fonctionnement soient définies dans une convention constitutive et une charte du réseau.