LES GUIDES DE LA CNIL

GUIDE
PROFESSIONNELS DE SANTÉ

Édition 2011

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr

Avant-propos

Vous êtes un professionnel de santé exerçant à titre libéral, un membre d'une équipe soignante au sein d'un établissement de santé ou bien encore un médecin effectuant des recherches dans le domaine de la santé…. Vous allez être amenés à mettre en place des fichiers informatisés qui concernent vos patients et/ou les personnes participant à des recherches médicales. Vous envisagez également de recourir à des réseaux pour recevoir et transmettre des informations à caractère médical (feuilles de soins, résultats d'analyses ou gestion partagée de dossiers médicaux).

Tous ces fichiers vont comporter de nombreuses informations, et en particulier des données de santé.

La loi Informatique et Libertés encadre la collecte et le traitement de toutes ces données. Elle a pour objet de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à l'intimité de leur vie privée. Elle assure une protection renforcée aux informations de santé considérées comme « sensibles ».

Le respect, par le responsable de fichiers que vous êtes, des règles de protection des informations est un facteur de transparence et de confiance à l'égard de vos patients. C'est aussi un gage de sécurité juridique. Vous pouvez en effet voir votre responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

C'est pourquoi notre Commission, qui veille au respect de ces principes, souhaite vous conseiller sur les mesures à adopter pour la gestion des fichiers mis en place et l'information des patients sur les droits qui leur sont reconnus par la loi Informatique et Libertés.

Alex TÜRK
Président de la CNIL

I – Les 5 principes clés à respecter

La loi Informatique et Libertés est applicable dès lors qu'il existe un traitement, automatisé ou manuel (c'est-à-dire un fichier informatique ou un fichier « papier ») contenant des informations relatives à des personnes physiques.

Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantit un certain nombre de droits pour les personnes.

1. Le principe de finalité

Les informations qui concernent les patients ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.

Par exemple : la mise en place d'un fichier de patients par un médecin exerçant à titre libéral doit lui permettre de gérer ses dossiers médicaux, d'éditer des feuilles de soins, de gérer les rendez-vous. Ce fichier ne peut pas être utilisé à des fins de prospection commerciale ou de communication politique.

Tout détournement de finalité est passible de sanctions pénales (article 226-21 du code pénal).

2. Le principe de pertinence des données

Seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis par le traitement.

Par exemple : l'enregistrement de la nationalité d'un patient dans le fichier du cabinet médical ou encore dans le fichier clients d'une pharmacie n'est pas pertinent. L'enregistrement des informations relatives aux habitudes de vie d'un patient peut en revanche être admis dans la mesure où ces informations sont nécessaires au diagnostic et aux soins.

3. Le principe d'une durée limitée de conservation des informations : le droit à l'oubli

Les informations ne peuvent être conservées pour une durée illimitée. Elles doivent être conservées pendant une durée précise et déterminée en fonction de l'objet de chaque fichier.

Par exemple : dans le cadre d'une recherche biomédicale, les informations seront conservées jusqu'à la première autorisation de mise sur le marché ou la publication des résultats de la recherche.

4. Le principe de sécurité et de confidentialité des données

Le professionnel de santé, comme tout responsable de fichier, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des informations et éviter leur divulgation à des tiers non autorisés.

Par exemple : chaque personne doit disposer d'un mot de passe individuel régulièrement renouvelé. Les droits d'accès aux données doivent être précisément définis en fonction des besoins réels de chaque personne (lecture, écriture, suppression). Il peut également être utile de prévoir un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte période de veille.

Ainsi, les informations ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Par exemple : Les informations peuvent néanmoins être communiquées à des tiers autorisés à en connaître en application de dispositions législatives particulières (les autorités judiciaires, les procureurs de la République, les juges d'instruction et officiers de gendarmerie agissant en flagrant délit ou sur commission rogatoire).

5. Le principe du respect des droits des personnes

> Information des personnes

Lors de la collecte des informations qui les concernent, les personnes doivent être clairement informées des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires et des modalités d'exercice de leurs droits au titre de la loi « Informatique et Libertés » (droit d'accès, de rectification et d'opposition).

Cette information peut être assurée de différentes manières : panneaux d'affichage, livret d'accueil de l'établissement de santé, page « protection des données » ou « informatique et libertés » sur le site internet de l'établissement de santé ou du cabinet médical.

Lorsque les informations sont recueillies par voie de questionnaires, papier ou informatisés, ceux-ci doivent comporter ces mentions légales.

> Droits d'accès et de rectification

Toute personne peut demander au détenteur d'un fichier de lui communiquer toutes les informations qui la concernent. Elle a également le droit de faire rectifier ou supprimer les informations erronées.

Par exemple : un patient peut accéder à son dossier médical (voir fiche le droit d'accès au dossier médical).

> Droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes à ce que des données qui la concernent, soient enregistrées dans un fichier informatique. Sauf si ce motif résulte d'une obligation légale ou réglementaire.

Par exemple : Un patient atteint d'une affection grave, souhaite que son dossier médical ne soit pas accessible dans le système d'information de l'hôpital. Le motif légitime invoqué à l'appui de cette demande est d'éviter qu'un membre de sa famille, appelé à travailler dans l'hôpital, accède à son dossier car le patient ne souhaite pas lui révéler sa pathologie.

II – Les missions de la CNIL

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante, est chargée d'assurer le respect des dispositions de la loi Informatique et Libertés.

1. Le rôle de conseil et d'information

La CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques par téléphone, par courrier ou par ses publications. Son service d'orientation et de renseignement apporte une réponse rapide aux questions les plus fréquemment posées par les particuliers ou les professionnels.

2. Le contrôle de la conformité des fichiers à la loi

La CNIL vérifie, lors de l'instruction des demandes d'autorisation de fichiers que les caractéristiques des traitements sont bien conformes à la loi. Les autorisations n'interviennent que pour la mise en œuvre des traitements qui nécessitent une attention particulière du fait de leur contenu ou de leur finalité. S'agissant des autres traitements, leur déclaration à la CNIL fait l'objet d'un simple récépissé qui n'exonère pas le déclarant de sa responsabilité. La Commission peut simplifier les formalités déclaratives, voire exonérer de déclaration certains fichiers.

La CNIL reçoit les plaintes concernant le non-respect de la loi.

La CNIL dispose d'un pouvoir de contrôle a priori qui permet à ses membres et ses agents d'accéder à tous les locaux professionnels. Ils peuvent demander communication de tout document nécessaire et en prendre copie, recueillir tout renseignement utile et accéder aux programmes informatiques.

3. Le pouvoir de sanction

La CNIL peut notamment :

- adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi ;
- prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et, en cas d'urgence, décider l'interruption du traitement ou le verrouillage des données ;
- prononcer des sanctions pécuniaires pouvant aller jusqu'à 300 000 € en cas de réitération ;
- dénoncer au parquet les infractions à la loi dont elle a connaissance.

III – Le correspondant informatique et libertés (CIL) : un vecteur de diffusion de la culture informatique et libertés

Institué en 2004 à l'occasion de la refonte de la loi Informatique et Libertés, le correspondant à la protection des données ou correspondant informatique et libertés (CIL) est un acteur et un relais incontournable de la culture informatique et libertés.

Le correspondant doit, si possible, être un employé du responsable de traitement (correspondant interne). Ainsi, il connaît mieux, a priori, l'activité et le fonctionnement interne de son organisme, il est à même de veiller en temps réel à la bonne application des règles et des conditions de mise en œuvre des traitements. Mais le correspondant peut également ne pas appartenir à l'organisme (correspondant externe).

Pour s'acquitter de sa tâche, le correspondant informatique et libertés doit disposer de la liberté d'action et des moyens qui lui permettront de recommander des solutions organisationnelles ou techniques adaptées. Il doit pouvoir exercer pleinement ses missions, en dehors de toute pression, et jouer son rôle auprès du responsable du fichier.

Le CIL – Quelques informations pratiques

Pourquoi désigner un CIL ?

Sa désignation, qui est facultative, exonère de déclaration la plupart des fichiers. Il contribue à une meilleure application de la loi.

Quels avantages pour l'organisme ?

Le CIL est un acteur de la sécurité juridique au sein de l'organisme. Son action peut prendre plusieurs formes : le conseil, la recommandation, la sensibilisation, la médiation et l'alerte en cas de dysfonctionnement.

Comment désigner un CIL ?

C'est simple, il suffit de compléter en ligne le formulaire de désignation sur le site internet de la CNIL.

Comment le CIL pourrait-il/elle être formé(e) ?

La CNIL propose des ateliers d'information gratuits, généralistes et thématiques, animés par ses propres experts.

Quelle relation avec la CNIL ?

La CNIL a mis en place un service spécifique pour garantir au CIL une réponse rapide et de qualité. Il s'agit d'un guichet unique pour toutes les questions juridiques ou les éclairages liés à l'exercice de la fonction.

D'autres avantages ?

Le CIL est un interlocuteur privilégié de la CNIL. Ses demandes sont donc traitées en priorité.

Il fait partie du réseau des CIL animés par la CNIL.

Il participe à la réflexion liée à l'évolution de la fonction, à la création d'outils de travail, des textes juridiques…

Fiche n°1 - La donnée de santé : une utilisation très encadrée

Les données relatives à la santé sont considérées par la loi Informatique et Libertés (article 8) comme des données sensibles dont le traitement et la collecte sont par principe interdits.

Des dérogations à ce principe existent.

Un usage encadré des données de santé

Les données de santé ne peuvent être utilisées et communiquées que dans des conditions déterminées par la loi et dans l'intérêt des patients (assurer le suivi médical, faciliter sa prise en charge par l'assurance maladie…) ou pour les besoins de la santé publique.

La loi Informatique et Libertés énumère les cas dans lesquels le traitement ou la collecte des données de santé est possible :

- les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf disposition contraire prévue par la loi ;
- les traitements nécessaires à la sauvegarde de la vie humaine ;
- les traitements nécessaires aux fins de suivi médical des personnes, de prévention, de diagnostic, d'administration de soins ou de traitements, ou de gestion de services de santé ;
- les traitements statistiques réalisés par un service statistique ministériel ;
- les traitements nécessaires à la recherche dans le domaine de la santé (chapitre IX de la loi Informatique et Libertés) ;
- les traitements de données de santé à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins de prévention (chapitre X de la loi Informatique et Libertés) ;
- si les données sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation ;
- les traitements justifiés par l'intérêt public et autorisés par la CNIL.

D'autres textes organisent l'accès aux données de santé :

- l'équipe de soins : les professionnels de santé peuvent 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. 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 (L. 1110-4 du code de la santé publique) ;
- la télémédecine : les professionnels participant à un acte de télémédecine peuvent, sauf opposition de la personne dûment informée, échanger des informations relatives à cette personne, notamment par le biais des technologies de l'information et de la communication ;

- la sécurité sociale : les professionnels de santé transmettent aux organismes d'assurance maladie obligatoire le code détaillé des actes, prestations et pathologies diagnostiqués chez leurs patients (L. 161-29 du code de la sécurité sociale) ;

- les déclarations obligatoires de certaines maladies : les professionnels de santé sont tenus de déclarer aux autorités sanitaires certaines maladies infectieuses qui nécessitent une intervention urgente (voir la fiche n°8 : les maladies à déclaration obligatoire).

Les utilisations interdites

Les données médicales concernant les patients ne peuvent pas faire l'objet de cession ou d'exploitation commerciale.

La constitution et l'utilisation à des fins de prospection ou de promotion commerciale 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 (article L. 4113-7 du code de la santé publique).

La communication à des tiers autorisés

Les tiers autorisés au sens de la loi sont les personnes habilitées par des textes législatifs ou réglementaires à obtenir un accès ponctuel et limité aux données.

Il s'agit :

- des autorités judiciaires

  Le procureur de la République, les juges, les officiers de police judiciaire de la police ou de la gendarmerie nationale doivent être considérés, lorsqu'ils agissent par réquisition judiciaire dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une instruction préparatoire éventuellement sur commission rogatoire, comme des tiers autorisés à obtenir communication des données contenues dans les dossiers ;

- des experts

  Les experts désignés par une juridiction administrative ou civile peuvent obtenir communication des données sous réserve du consentement du patient concerné ;

- des agents de l'administration fiscale

  Les professionnels de santé libéraux sont tenus de mentionner dans leur livre-journal (ou document détaillant leurs recettes professionnelles) accessible aux agents de l'administration des impôts : l'identité du client, le montant, la date et la forme du versement des honoraires.

Ces documents peuvent, toutefois, comporter à la place de l'identité du client : soit une référence à un document annexe permettant de retrouver l'identité du client (à la condition que l'administration ait accès à ce document) ; soit le nom du client, dans la mesure où son identité complète (nom, prénom et adresse) figure dans un fichier couvert par le secret professionnel (Article L. 86A du Livre des procédures fiscales).

Attention

Les médecins des compagnies d'assurance ou les employeurs ne peuvent être considérés comme des tiers autorisés à obtenir le dossier médical des patients.

En cas de doute, il convient de demander au tiers d'indiquer le fondement juridique de sa demande.

Attention

Le consentement du patient ne suffit pas à exonérer le professionnel de santé de son obligation de secret professionnel.

Fiche n°2 - Le droit d'accès au dossier médical : comment répondre aux demandes ?

Les patients ont un accès direct à l'ensemble des informations de santé les concernant[1]. Ils peuvent demander l'accès à leur dossier médical auprès de leur médecin ou de l'établissement de santé où ils ont été soignés. Ils peuvent, s'ils le souhaitent, accéder à ces données par l'intermédiaire d'un médecin de leur choix.

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

Dans quel delai répondre aux demandes de droit d'accès ?

La communication des informations 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, à partir de la date à laquelle l'information médicale a été constituée, le délai est porté à deux mois.

Quelles sont les modalités d'accès et de communication ?

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. Ils 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 pratique

Un modèle de courrier pour exercer le droit d'accès à son dossier médical est disponible dans la partie « les outils » de ce guide

En outre, si le patient a ouvert un dossier médical personnel, il a la possibilité d'accéder directement sur internet, depuis son ordinateur, au contenu de son DMP ainsi qu'au journal des opérations effectuées sur celui-ci.

Un mineur peut s'opposer à ce qu'un médecin communique au titulaire de l'autorité parentale des informations qui le concernent. En effet, un mineur qui souhaite garder le secret sur un traitement ou une intervention dont il fait l'objet, peut s'opposer à ce que le médecin communique au titulaire de l'autorité parentale les informations constituées à ce sujet (article 6 du décret n° 2002-637 du 29 avril 2002). Le médecin fait mention écrite de cette opposition. Tout médecin saisi d'une telle demande par le titulaire de l'autorité parentale doit s'efforcer d'obtenir le

(1) Article 43 de la loi du 6 janvier 1978 modifiée en août 2004 et articles L. 1111-7 et L. 1112-1 du code de la santé publique et le décret n° 2002-637 du 29/04/2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé.

consentement de la personne mineure. Si en dépit de ses efforts le mineur maintient son opposition, la demande du titulaire de l'autorité parentale ne peut être satisfaite.

Les ayants droits d'une personne décédée, sauf volonté contraire exprimée par l'intéressé de son vivant, peuvent accéder à certaines informations du dossier médical afin de :

- connaitre les causes de décès ;
- défendre la mémoire du défunt ;
- ou faire valoir leurs droits.

Ils doivent préciser le motif de la demande d'accès.

Les professionnels de santé doivent s'assurer avant toute communication :

- de l'identité du demandeur ;
- de sa qualité d'ayant droit ;
- du motif de la demande afin de s'assurer qu'elle correspond à un des cas prévus par la loi ;
- de l'absence d'opposition du défunt.

Les professionnels doivent ensuite veiller à ce que seules soient communiquées les informations nécessaires pour satisfaire la demande. Seules sont concernées les pièces du dossier répondant au motif de la requête.

Tout refus doit être motivé et peut être contesté dans un délai de deux mois auprès de la CADA.

Les Commissions régionales de conciliation et d'indemnisation (CRCI) peuvent également être saisies de tout litige entre usagers et professionnels de santé, dans le cadre de leur mission de conciliation.

Quelques précisions sur les documents pouvant être communiqués

- La patient a accès à l'ensemble des informations concernant sa santé, à savoir toutes celles qui sont formalisées et/ou ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention. Sont également concernés :
  - les échanges écrits entre professionnels de santé ;
  - les résultats d'examen ;
  - les comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation ;
  - les protocoles et prescriptions thérapeutiques mis en œuvre ;
  - 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 tiers.

- Ces informations sont communicables qu'elles soient sous forme papier ou sur support informatique. La communication doit être réalisée dans un langage clair (par exemple, par l'indication de la signification des codes utilisés).

- Les personnes peuvent demander à connaître les causes de la mort d'un proche pour défendre sa mémoire ou faire valoir des droits, sauf volonté contraire exprimée par le défunt.
- Les personnes peuvent également obtenir communication du résultat d'une expertise médicale demandée par une compagnie d'assurance.
- En cas d'hospitalisation d'office ou d'hospitalisation sur demande d'un tiers, le médecin peut estimer que la communication de son dossier au patient doit avoir lieu par l'intermédiaire d'un autre médecin. Dans ce cas, l'avis de la Commission départementale des hospitalisations psychiatriques doit être recueilli et s'impose.

Un médecin peut-il, sur demande de son patient, effacer du dossier médical des informations ?

Un patient a le droit de s'opposer, pour des motifs légitimes, à ce que des données personnelles fassent l'objet d'un traitement par un établissement (articles 38 et 40 de la loi du 6/01/1978 modifiée en 2004)

Par exemple, un patient désireux d'obtenir l'effacement des informations relatives à ses différentes hospitalisations au motif que, étant atteint d'une affection qu'il ne souhaitait pas révéler à sa famille, alors qu' un membre de sa famille, médecin dans l'hôpital concerné, pouvait consulter le système informatique et ainsi connaître la nature de sa pathologie. Sa demande a été considérée comme légitime et acceptée.

Afin d'apprécier les motifs légitimes invoqués par le patient, un échange avec le médecin qui le prend en charge apparaît important pour tenter de trouver des solutions alternatives (pseudonyme, accès restreint). Il convient également d'alerter le patient sur les conséquences de l'effacement de son dossier médical en cas de nouvelle hospitalisation (absence d'historique médical et risque d'une prise en charge moins rapide et moins efficace).

Si l'effacement des données sur support informatique est décidé, l'établissement doit conserver les données dans un fichier distinct, sur un support papier ou un support physique amovible de nature à assurer la pérennité de l'information. En effet, pour chaque patient hospitalisé dans un établissement de santé public ou privé, le code de la santé publique prescrit la constitution d'un dossier médical et sa conservation.

Quels sont les recours en cas de refus d'accès au dossier médical ?

- Si les données médicales sont détenues par un établissement public (hôpital) ou participant au service public hospitalier, c'est la Commission d'accès aux documents administratifs (CADA), 35 rue Saint Dominique, 75700 Paris 07 SP qui est compétente.
- Si les données médicales sont détenues par un établissement de santé privé (clinique) ou par un médecin, c'est la CNIL qui devra se prononcer.

Fiche n°3 - Le NIR : numéro de sécurité sociale

Le NIR, Numéro d'Inscription au Répertoire national d'identification des personnes physiques (RNIPP) est plus communément appelé numéro de sécurité sociale.

Le répertoire dont il est issu, le RNIPP, permet l'identification de toutes les personnes nées en France et de savoir si elles sont en vie ou décédées.

Les caractéristiques du NIR

Ce numéro composé de treize chiffres (plus une clé de contrôle de 2 chiffres) est attribué à chaque français dès sa naissance. Ces chiffres correspondent au sexe (1 chiffre), à l'année de naissance (2 chiffres), au mois de naissance (2 chiffres), et au lieu de naissance dont le département (5 chiffres ou caractères). Les trois chiffres suivants sont des numéros d'ordre non signifiants.

Sexe	Année naissance	Mois naissance	Département naissance	N° commune ou pays de naissance	N° d'ordre acte de naissance	Clé contrôle
1 : homme 2 : femme	00 à 99	01 à 12	- 01 à 95 : métropole - 970 à 989 : outre-mer - 99 : étranger	de 001 à 990	de 001 à 999	de 01 à 97

Le numéro de sécurité sociale (NIR) est donc un numéro particulier car :

- **signifiant :** il permet de connaître le sexe, le mois et l'année de naissance, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger ;
- **unique et pérenne :** un seul numéro est attribué à chaque individu ;
- **fiable :** certifié par l'INSEE à partir des données d'état civil transmises par les mairies.

La loi Informatique et Libertés soumet à autorisation l'utilisation de ce numéro.

Ce numéro, parce qu'il est plus facile à reconstituer à partir des éléments d'état civil, parce qu'il rend plus aisées les possibilités de rapprochements de fichiers et facilite la recherche et le tri des informations dans les fichiers, reste associé au risque d'une interconnexion généralisée ou d'une utilisation détournée des fichiers.

L'utilisation du NIR

Le NIR a été utilisé, dès l'origine, dans le secteur de la sécurité sociale. La CNIL a donc admis qu'il soit enregistré dans l'ensemble des fichiers des organismes en relation avec ce secteur.

Sont appelés à utiliser le NIR du fait de leurs relations avec la sécurité sociale :

- les acteurs du système de protection sociale ;
- les employeurs ;
- le pôle emploi pour le paiement des cotisations sociales des chômeurs et le maintien de leurs droits sociaux ;
- les organismes d'assurance maladie obligatoires et complémentaires ;
- les professionnels et les établissements de santé pour permettre la prise en charge totale ou partielle des frais de maladie...

Des décrets sont intervenus afin d'autoriser de telles utilisations. Ils ont veillé à ce que ce numéro demeure cantonné aux relations avec les organismes de sécurité sociale.

Les professionnels de santé et les établissements sont autorisés, depuis un décret du 12 septembre 1996, à utiliser le NIR dans le cadre de leurs relations avec la sécurité sociale à des fins de facturation. **Ils ne sont cependant pas autorisés à utiliser ce numéro comme identifiant du dossier médical du patient**. **En effet, la CNIL, dans une recommandation du 20 février 2007 prise à l'issue d'une série d'auditions, a exclu l'utilisation du NIR comme identifiant national de santé.**

L'utilisation du NIR par les organismes de recherche

En l'état actuel des textes, les organismes de recherche médicale et les autorités sanitaires ne sont pas autorisés à utiliser le NIR.

Ces acteurs ont alerté la CNIL sur les difficultés juridiques et techniques rencontrées pour obtenir des indicateurs fiables et pérennes, nécessaires à la définition et à l'évaluation des politiques de santé publique. Parmi ces indicateurs figurent les informations détenues par la sécurité sociale.

L'accès aux données issues de ces bases (assurance maladie, CAF, CNAV…) et leur recoupement est problématique dans la mesure où la clé d'accès à de nombreux fichiers et, notamment, aux fichiers de l'assurance maladie ou de l'assurance vieillesse, est le numéro de sécurité sociale.

Compte tenu des enjeux que soulève cette question et de la nécessité de maintenir le niveau de la recherche française sur le plan international, la CNIL a décidé d'œuvrer activement pour l'élaboration de solutions juridiques et techniques aptes à remédier à cette situation dans le respect de la protection des données personnelles et de la vie privée. Elle a demandé aux pouvoirs publics de prendre les dispositions réglementaires nécessaires pour permettre une utilisation encadrée du NIR à des fins de recherche médicale et d'études de santé publique et travaille à leur élaboration en concertation avec l'ensemble des acteurs concernés.

Fiche n°4 - La sécurité : un impératif

La loi Informatique et Libertés impose au responsable de fichiers de garantir la sécurité des informations. Les données de santé sont considérées par la loi comme des informations sensibles qui nécessitent donc un haut niveau de sécurité.

Vous êtes responsable

Le responsable du dispositif, par exemple le médecin exerçant à titre libéral ou le directeur de la clinique, doit assurer la sécurité des informations collectées. Il lui appartient de prendre les dispositions nécessaires pour garantir leur sécurité. Ainsi, les informations collectées ne doivent pas être déformées, endommagées ou accessibles à un tiers non autorisé, et les personnes concernées doivent pouvoir exercer leurs droits.

Pour aller plus loin : Que dit la loi ?

« 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. » **article 34 de la loi Informatique et Libertés.**

La négligence ou l'absence de mesures de sécurité peuvent être sanctionnées de 300 000 euros d'amende et de 5 ans d'emprisonnement (article 226-17 du Code Pénal).

La sécurité des postes de travail

• Le mot de passe

Le responsable du dispositif doit protéger l'accès aux informations par des mots de passe individuels et par l'utilisation de la carte de professionnel de santé (CPS). Le mot de passe choisi doit :

- être constitué de huit caractères au moins ;
- comprendre trois types de caractères parmi les quatre possibles (majuscules, minuscules, chiffres et caractères spéciaux) ;
- être renouvelé au moindre doute de compromission et si possible de manière périodique (tous les ans).

Il doit être conservé de manière à préserver sa confidentialité.

En pratique

Utiliser des moyens mnémotechniques pour créer votre mot de passe. Par exemple en utilisant les premières lettres de chaque mot d'une phrase. Ainsi, la phrase « J'habite au 8 rue Vivienne à Paris » deviendra « J'ha8rVaP ».

Les conseils de la CNIL :

- limiter le nombre de tentatives d'accès à un compte, par exemple à 3 tentatives infructueuses. Lorsque cette limite est atteinte, le compte doit être

bloqué temporairement ou jusqu'à l'intervention d'un administrateur système.

- protéger l'accès aux locaux et aux postes informatiques. En cas d'absence, penser à éteindre l'ordinateur, ou à mettre en place un écran de veille protégé par un mot de passe et ne pas laisser de CPS dans le lecteur.
- utiliser un logiciel antivirus mis à jour régulièrement, ainsi qu'une application contre les logiciels espions (*anti-spyware*) et un « pare-feu » (*firewall*) lors de l'utilisation d'Internet.
- tenir à jour tous les logiciels et le système d'exploitation.
- effectuer régulièrement des sauvegardes chiffrées sur supports amovibles (disque dur externe, clé USB…) et les conserver dans un lieu différent ou dans un coffre ignifugé.
- effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne, à sa mise au rebut ou pour les postes partagés.
- pour chiffrer les données, le logiciel *TrueCrypt* (www.truecrypt.org) est certifié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°4 – La sécurité des postes de travail.

La sécurité des applications réseau

- Prévoir une politique d'habilitation permettant de restreindre l'accès aux seules personnes habilitées. Cette politique doit notamment prévoir de supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder aux bâtiments ou applications, ainsi qu'à la fin de leur période d'emploi.

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°3 – La gestion des habilitations et la sensibilisation des utilisateurs.

- Rédiger une charte informatique et l'annexer au règlement intérieur de l'entreprise.
- Faire en sorte que la connexion à plusieurs postes sous le même identifiant avec le même mot de passe ne soit pas possible.
- Afficher systématiquement les dates et heures de la dernière connexion sous les mêmes identifiant et mot de passe.
- Journaliser les connexions et les actions effectuées sur les données.

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°8 – La traçabilité et la gestion des incidents.

- Chiffrer la communication par l'usage du protocole SSL avec une clé de 128 bits lors de la mise en œuvre de **services web.**
- Empêcher les accès illégitimes aux données de santé à caractère personnel dans les bases de données de l'application, par exemple en chiffrant les données.

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°10 – La sécurité du réseau informatique interne.

Sensibilisez votre personnel à ces mesures de sécurité

Ces bonnes pratiques sont destinées à pallier les risques que les traitements de données à caractère personnel peuvent engendrer pour les personnes concernées. Chaque traitement ayant un fonctionnement et un contexte particuliers, ces risques diffèrent d'un traitement à l'autre. Il est donc essentiel d'adapter les bonnes pratiques au contexte spécifique du traitement considéré. Il est également possible de traiter les risques à l'aide d'autres mesures que celles présentées.

Les bonnes pratiques de ce guide sont fondées sur des référentiels légaux, normatifs ou sectoriels qui peuvent évoluer.

Fiche n°5 - La messagerie électronique et la télécopie : quelles sécurités apporter ?

La messagerie électronique et la télécopie apportent un gain de temps considérable. Cependant un certain nombre de précautions s'imposent.

Une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des informations couvertes par le secret médical : adresse électronique erronée, erreur de numéro de télécopie… Les virus, les attaques contre les systèmes informatiques et l'absence générale de confidentialité du réseau Internet, font de la transmission d'informations de santé par courrier électronique un moyen risqué de communiquer.

Il est impératif de garantir la confidentialité lors de la transmission des informations de santé à des partenaires extérieurs.

Comment sécuriser les messages électroniques ?

La confidentialité et l'intégrité des informations envoyées par message électronique doivent être assurées. Ainsi, lors de l'utilisation d'une messagerie professionnelle interne, il faut s'assurer que celle-ci est sécurisée, notamment par le chiffrement des messages lors de leur transmission.

En l'absence de messagerie interne sécurisée, les informations de santé doivent être placées dans des documents joints au message. Ces documents doivent être chiffrés avant la transmission (ex. : programme de chiffrement dénommé PGP(1)) et le secret nécessaire à la lecture du fichier (ex : mot de passe) doit être transmis par un canal de nature différente (ex. : téléphone, SMS…).

Attention

Les messageries sur internet (hotmail, yahoo, gmail, wanadoo,…) ne garantissent pas la confidentialité des messages, le chiffrement des pièces jointes s'impose alors.

Il est important de sensibiliser les utilisateurs au fait qu'ils doivent éviter d'ouvrir des courriers électroniques d'origine inconnue, et encore plus les pièces jointes à risque (extensions .pif, .com, .bat, .exe, .vbs, .lnk…).

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°14 – L'échange d'informations avec d'autres organismes.

(1) Pretty Good Privacy

Comment sécuriser la transmission par télécopie ?

- Le télécopieur doit être situé dans un local médical à l'accès physique contrôlé, uniquement accessible 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 de la télécopie, le télécopieur doit afficher l'identité du destinataire.
- Doubler l'envoi par télécopie d'un envoi postal des documents originaux au destinataire.
- Si possible, préenregistrer dans le carnet d'adresses les numéros des destinataires habituels.

Fiche n°6 - Le dossier médical personnel (DMP) : le dossier du patient

Le dossier médical personnel (DMP) est un dossier informatisé créé pour chaque bénéficiaire de l'assurance maladie qui le souhaite. Il permet le regroupement et le partage entre les professionnels et établissements de santé des informations utiles à la coordination et à la continuité des soins.

Le DMP : de quoi s'agit-il ?

C'est un dossier médical informatisé accessible depuis internet. Il est hébergé par le groupement d'entreprises solidaires ATOS-La Poste qui a été agréé par le ministre de la santé le 10 novembre 2010, après l'avis de la CNIL et du Comité d'agrément des hébergeurs.

Le DMP permet aux professionnels de santé (ex. : médecin traitant, cardiologue, rhumatologue…) choisis par le patient, de connaître les soins qui lui ont été dispensés pour assurer une meilleure prise en charge médicale et un meilleur suivi. Il doit être tenu dans le respect du secret médical.

Le partage d'informations entre professionnels de santé répond également à une volonté d'éviter les examens redondants et limiter les actes inutiles.

L'accès au DMP est interdit aux médecins du travail et aux médecins des compagnies d'assurance.

Quelles sont les spécificités du DMP ?

Le DMP présente un certain nombre de particularités qui le distinguent des autres dossiers médicaux partagés :

- il a vocation à suivre le patient durant toute sa vie et à le prendre en charge sur l'ensemble du territoire grâce à une centralisation des informations et un partage des données utiles à la coordination des soins entre les professionnels et les établissements ;

- il est conçu comme le « dossier du patient » qui en maîtrise le contenu et les accès. Le patient a la possibilité d'accéder directement, depuis son ordinateur, à son dossier médical. Il peut désigner chacun des professionnels de santé à qui il souhaite ouvrir des droits d'accès. Il a aussi la possibilité de masquer des données qui y figurent.

Comment le DMP va-t-il se généraliser ?

La première phase, qui devrait se dérouler sur trois ans, est consacrée à la mise en place progressive sur l'ensemble du territoire d'un dossier médical « socle », alimenté, notamment, par les comptes rendus d'hospitalisation et de consultation. Il s'agit de mettre l'ensemble des professionnels de santé en mesure de partager des documents, avec l'accord et sous le contrôle du patient.

Le DMP n'a pas vocation à se substituer au dossier papier ou informatisé établi dans les cabinets des médecins libéraux et dans les établissements de santé, mais à s'y ajouter.

Ce déploiement progressif s'appuie notamment sur la convergence de quatre régions pilotes déjà engagées dans des dispositifs d'échanges de données (Aquitaine, Picardie, Alsace, Franche-Comté).

La seconde phase de déploiement devra s'inscrire dans un cadre réglementaire qui fixera le contenu du DMP, les conditions pour y accéder, le recours à un identifiant national de santé (INS) et les modalités de son utilisation.

Comment fonctionne le DMP ?

Les professionnels de santé peuvent créer un DMP à partir de leur logiciel rendu préalablement DMP-compatible ou à partir du site www.dmp.gouv.fr.

Pour aller plus loin

Des informations sur la procédure d' « homologation » des logiciels de professionnels de santé sont disponibles sur le site de l'ASIP Santé, e-santé.gouv.fr

Tout bénéficiaire de l'assurance maladie doté d'une carte Vitale individuelle peut ouvrir un DMP auprès d'un professionnel de santé ou à l'accueil d'un établissement de soins et y accéder directement depuis son ordinateur personnel.

La création d'un DMP est volontaire et chaque patient donne son consentement à sa création. Il a la faculté de fermer son DMP à tout moment. Ce dernier est alors archivé pendant dix ans, puis supprimé. Pendant ces dix ans, il peut être réactivé à la demande du patient. Une suppression définitive est également possible sans délai, à la demande du patient.

Le patient peut avoir accès à son DMP et à l'historique des traces, ou obtenir une copie auprès de l'hébergeur. Il a également la possibilité de « masquer » certaines informations de son dossier ou de demander à un professionnel de santé de le faire.

Quels ont été les points sur lesquels la Commission a porté une particulière attention ?

- Le 2 décembre 2010, la CNIL a autorisé la première phase de généralisation du DMP sur l'ensemble du territoire, après s'être assurée du respect des droits des citoyens et du déploiement de conditions de sécurité effectives et de haut niveau

- **Le recueil du consentement du patient à la création du dossier médical personnel.** La CNIL a veillé à ce que le patient soit clairement informé des spécificités du DMP et mis en mesure d'apprécier les conséquences de l'accord qu'il donne. Une copie papier du document électronique par lequel le personnel habilité à ouvrir un DMP atteste avoir procédé à l'information du patient et recueilli son consentement exprès est systématiquement remise au patient.

- **L'information du patient** sur le fonctionnement du dispositif et sur les modalités d'exercice de ses droits. Le patient doit ainsi être informé de la possibilité d'accéder à son DMP depuis son ordinateur personnel, du rôle spécifique dévolu au médecin traitant dans la gestion de son DMP et de ses droits.

- **Les conditions de sécurité du DMP** tant chez les professionnels et établissements de santé que chez l'hébergeur. Les informations enregistrées dans le DMP sont couvertes par le secret professionnel. Elles ne sont consultables que moyennant l'utilisation d'une carte de professionnel de santé. Une trace de tous les accès et consultations du DMP est gardée. Un chiffrement des données de santé contenues dans le DMP et des communications est effectué.

Les formalités à accomplir

Les professionnels de santé libéraux ou les établissements qui souhaitent alimenter un DMP n'ont pas de formalités spécifiques à accomplir dans la mesure où ils ont déjà déclaré la gestion de leurs patients (norme simplifiée 50 pour les professionnels de santé agissant à titre libéral ou déclaration normale pour les établissements).

Fiche n°7 - Le dossier pharmaceutique (DP): un outil professionnel

Créé par la loi du 30 janvier 2007, le dossier pharmaceutique (DP) est un outil professionnel actuellement mis à la disposition des pharmaciens d'officine. Son principal objectif est de sécuriser la délivrance des médicaments.

Le DP : de quoi s'agit-il ?

Le dossier pharmaceutique est un dossier professionnel hébergé sur internet qui permet au pharmacien d'avoir accès à l'historique des médicaments prescrits ou délivrés à une personne, au cours des quatre derniers mois, quelle que soit l'officine de délivrance. Cet outil permet de sécuriser la délivrance des médicaments en calculant le risque d'interactions médicamenteuses à partir de la liste de l'ensemble des médicaments dispensés.

Les informations accessibles au pharmacien concernent la dénomination des médicaments délivrés (avec ou sans prescription), leur quantité et leur date de délivrance. Aucune indication n'est donnée sur le prescripteur, le prix et le lieu de délivrance des médicaments.

Le DP permettra, accessoirement, d'assurer une meilleure traçabilité des médicaments et de diffuser des alertes sanitaires à la demande des pouvoirs publics auprès des pharmaciens d'officine. Il a vocation, à terme, à alimenter le volet « médicament » du dossier médical personnel (DMP).

Le 2 décembre 2008, la CNIL a autorisé la généralisation du dossier pharmaceutique dans l'ensemble des officines françaises après avoir validé les déploiements successifs du dispositif.

Par une délibération en date du 6 mai 2010, la CNIL a autorisé l'expérimentation pendant 9 mois de l'utilisation du DP dans un nombre limité de pharmacies dites « à usage intérieur » des établissements de santé volontaires afin d'étudier la faisabilité du projet.

Les modalités d'accès : le nécessaire consentement du patient

L'ouverture d'un DP est facultative et subordonnée à l'accord exprès du patient. Ce dernier a la faculté de fermer son DP à tout moment dans l'officine de son choix.

Le patient qui a ouvert un DP peut s'opposer à sa consultation par le pharmacien. Cette consultation ne peut être effectuée qu'en sa présence puisqu'elle nécessite la présentation de sa carte Vitale. Le patient a également la possibilité de refuser l'inscription de tel ou tel médicament dans son DP s'il ne souhaite pas qu'il y figure ; il est alors fait mention du caractère incomplet du DP.

Le patient a accès à son DP par l'intermédiaire du pharmacien de son choix. Une copie peut lui être remise à sa demande.

Les pharmaciens d'officine se connectent à la plate forme de l'hébergeur en utilisant leur carte CPS et la carte Vitale du patient. Seuls les pharmaciens peuvent consulter et alimenter l'historique des médicaments délivrés.

Les pharmaciens désireux d'utiliser le DP n'ont pas de formalités spécifiques à accomplir s'ils ont réalisé un engagement de conformité à la norme simplifiée 52.

Fiche n°8 - L'historique des remboursements (HR) ou le Web médecin

Les médecins peuvent, à l'occasion des soins qu'ils délivrent, consulter l'historique des actes et des prestations remboursés par l'assurance maladie obligatoire.

L'historique des remboursements : de quoi s'agit-il ?

L'historique des remboursements (HR) est un service proposé par l'Assurance Maladie. Il permet aux médecins d'accéder à l'ensemble des soins, médicaments et examens qui ont été remboursés à ses patients au cours des 12 derniers mois.

Les données accessibles sont outre les données d'identité : le code des actes (consultations chez un médecin, un kinésithérapeute, examen de biologie, de radiologie…), produits (fauteuil roulant, prothèse auditive…), et médicaments (nom et posologie), des informations relatives aux affections de longue durée, les frais de transport, les indemnités et allocations journalières versées.

Le dispositif a pour objet de limiter les risques d'effets indésirables des médicaments, les examens redondants et le nomadisme des patients.

L'accès ne peut avoir lieu qu'à l'occasion de la délivrance de soins. Dès lors, les médecins du travail, les médecins experts et les médecins des compagnies d'assurance ne sont pas fondés à accéder à ces données.

Les modalités d'accès : le nécessaire consentement du patient

La Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés (CNAMTS) a mis en place un portail sécurisé donnant l'accès aux serveurs des organismes des différents régimes d'assurance maladie obligatoire. Chaque régime d'assurance maladie assure une liaison sécurisée entre le portail géré par la CNAMTS et ses systèmes d'information.

Pour consulter les données, le médecin s'authentifie au moyen de sa carte de professionnel de santé.

Il doit également présenter de manière simultanée la carte d'assurance maladie du patient.

Le médecin recueille l'accord du patient préalablement à la consultation des données. Cet accord se matérialise par la remise au praticien de sa carte d'assurance maladie. Le refus du patient de donner au médecin l'accès à son relevé d'informations n'entraîne aucune conséquence en matière de remboursement.

Le médecin qui souhaite utiliser ce service n'a pas de formalités spécifiques à accomplir auprès de la CNIL.

Les points appelant une vigilance particulière

La CNIL a attiré l'attention du ministère et de la CNAMTS sur :

Le rôle ambigu de la carte Vitale qui permet à la fois de transmettre à l'assurance maladie la demande de remboursement de la consultation et d'accéder à l'historique des remboursements. Préalablement à l'utilisation du service, une information claire sur l'accès et sa signification doit donc être délivrée au patient.

L'articulation entre le web médecin et le dossier médical personnel (DMP), sur la matérialisation du consentement différent pour l'accès au DMP et au web médecin et sur le droit de masquage qui n'existe pas pour le web médecin.

Fiche n°9 - Les réseaux de santé : un partage des données de santé

Outre le dossier médical personnel d'envergure nationale et le dossier pharmaceutique, sectoriel, les réseaux de santé, généralement centrés sur une pathologie ou une zone géographique déterminée permettent d'assurer une meilleure coordination des différents acteurs du système de santé et une meilleure prise en charge des patients qui y consentent.

Les réseaux de santé : de quoi s'agit-il ?

Les réseaux de santé (de lutte contre le diabète, de soins en cancérologie…) ont pour objet de faciliter l'intervention des différents acteurs du système de santé (établissements de santé, professions de santé, travailleurs sociaux, groupes de patients), la transmission des informations entre ces acteurs et d'assurer une meilleure prise en charge des patients qui y consentent. Les réseaux sont organisés autour de problématiques de santé (cancers, diabète…) ou d'une population spécifique (personnes âgées, femmes enceintes…).

La mise en place de ces réseaux de santé s'accompagne souvent d'un dossier médical partagé entre les acteurs. S'il est fait appel à un hébergeur de données de santé dans le cadre du réseau, l'hébergeur doit être agréé (cf. fiche hébergement de données de santé).

Les droits des patients : un nécessaire consentement éclairé

Le patient doit être clairement informé par une note d'information ou par une charte de fonctionnement du réseau :

- de l'identité du responsable du traitement ;
- le cas échéant de l'identité de la société appelée à héberger les dossiers et les engagements de confidentialité pris par cette dernière (cf. fiche hébergement de données de santé) ;
- de la finalité poursuivie par le réseau ;
- du caractère obligatoire ou facultatif des réponses, en distinguant les informations indispensables à la création d'un dossier et celles qui sont facultatives ;
- des destinataires des données et en particulier des modalités de désignation de ces destinataires par le patient ainsi que les personnes habilitées à collecter les données, à compléter le dossier, à lire le dossier (...) ;
- des modalités d'exercice de ses droits d'accès, de rectification, d'opposition et de retrait ;
- le cas échéant, des transferts d'informations envisagés à destination d'un État non membre de l'Union européenne.

Le consentement exprès (écrit) du patient à la constitution d'un dossier médical partagé au sein du réseau doit être recueilli préalablement à sa mise en œuvre. Ce consentement doit pouvoir être modifié et/ou retiré à tout moment.

Les droits des professionnels de santé : consentement

La CNIL recommande qu'un document contractuel soit remis aux professionnels de santé qui désirent participer au réseau dans lequel figurent les conditions de leur adhésion et la nature de leur responsabilité dans la gestion du dossier de santé dans le réseau.

Un haut niveau de securité pour les données échangées

La mise en place d'un dossier médical partagé dans le cadre d'un réseau impose un haut niveau de sécurité :

- identification et authentification du professionnel de santé par sa carte professionnelle (CPS) ;
- chiffrement des données transmises ;
- traçabilité : la Commission recommande que les mises à jour du dossier soient signées électroniquement par leurs auteurs et que les consultations du dossier soient tracées.

Pour aller plus loin se reporter à la fiche n°4 : « *La sécurité : un impératif* »

Les formalités à accomplir : une demande d'autorisation

Les réseaux de santé qui souhaitent mettre en œuvre un dossier médical partagé accessible via internet par les professionnels de santé doivent effectuer une demande d'autorisation préalable auprès de la CNIL. Un formulaire de demande d'autorisation en ligne est disponible sur le site de la CNIL : www.cnil.fr

Fiche n°10 - La télémédecine : médecine à distance

La télémédecine permet de pratiquer la médecine à distance au moyen des technologies de l'information et de la communication. Elle a pour objet de répondre à la désertification médicale de certaines zones géographiques, à la spécialisation de la médecine, à l'augmentation du nombre de personnes atteintes de maladies chroniques et à la volonté de réduire les coûts de transport et d'hospitalisation. Le décret n°2010-1229 du 19 octobre 2010 organise cette activité.

La télémedecine : de quoi s'agit-il ?

Constituent des actes de télémédecine :

- une **téléconsultation** qui permet à un patient de requérir à distance l'avis d'un médecin ;
- une **téléexpertise** qui permet à un professionnel médical de solliciter l'avis d'un ou de plusieurs professionnels médicaux (échanges entre médecins pour arrêter une thérapie) ;
- une **télésurveillance** médicale, c'est-à-dire, un acte de surveillance ou de suivi par un professionnel de santé qui interprète les données de suivi (dialyse à domicile) ;
- une **téléassistance** médicale qui permet à un médecin d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte de soins (ex. télé chirurgie) ;
- ou, la réponse médicale donnée dans le cadre de la **régulation médicale** (permanence des soins et urgences) Ex. : appel au SAMU.

Quelques exemples :

- un médecin de garde qui prend en charge, en urgence, un accident vasculaire cérébral demande l'avis d'un spécialiste sur une radio, pour déterminer la meilleure prise en charge (téléconsultation neurologique et la télé-radiologie au sein du réseau de spécialiste) ;
- des patients diabétiques, après une formation, vérifient leur glycémie à domicile et transmettent les résultats de manière sécurisée à leur médecin pour qu'il les interprète (transmission des données à un serveur central qui envoie l'information au médecin) ;
- des résidents d'une maison de retraite, accompagnés de leur gérontologue consultent un spécialiste à l'hôpital (cardiologue, dermatologue…), sans avoir à se déplacer (visioconférence).

Le fonctionnement

Les organismes et les professionnels de santé qui organisent entre eux une activité de télémédecine (excepté pour la permanence des soins et urgences) doivent :

- *soit* entrer dans le cadre d'un programme national de télémédecine ;
- *soit* faire l'objet d'un contrat signé avec **l'agence régionale de santé** (ARS) qui **autorise les projets** en tenant compte des besoins de la population et des spécificités de l'offre de soins dans le territoire considéré.

Chaque projet de télémédecine doit ensuite faire l'objet d'une convention entre les différents acteurs.

Les professionnels de santé qui interviennent doivent être diplômés (respect des conditions d'exercice).

Les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne concernée, sauf cas particuliers (impossibilité de donner son consentement, coma…). La personne doit notamment être informée de son état de santé, des traitements et actions envisagés ainsi que des risques. Les mineurs doivent recevoir une information adaptée à leur âge. Les professionnels participant à un acte de télémédecine peuvent, sauf opposition du patient dûment informé, échanger des informations le concernant.

Les professionnels de santé doivent pouvoir accéder aux données médicales du patient nécessaires à la réalisation de l'acte de télémédecine.

Le dossier du patient, détenu par chaque professionnel de santé intervenant et la fiche d'observation[2], doivent mentionner : le compte-rendu de l'acte, les actes et prescriptions réalisés, l'identité des professionnels participant, la date et l'heure de l'acte et les éventuels incidents techniques.

Un haut niveau de sécurité des échanges doit être assuré compte tenu des risques que comporterait la transmission d'informations dégradées ou la divulgation de celles-ci à des tiers. La CNIL considère que les dispositifs de télémédecine doivent garantir, outre l'authentification des professionnels de santé, la confidentialité des données, le chiffrement des données transmises, la traçabilité des connexions, l'intégrité des données et la mise en place d'un archivage sécurisé des données. Les technologies utilisées dans le cadre de la télémédecine (ex. logiciel) doivent être conformes aux référentiels d'interopérabilité et de sécurité élaborés par l'ASIP-Santé. Lorsque le traitement fait appel à un hébergeur de données de santé agréé, le consentement exprès du patient à cet hébergement est requis. Il peut être exprimé par voie électronique.

Les organismes et professionnels qui exercent une activité de télémédecine ont jusqu'au 20 avril 2012 pour se mettre en conformité avec le décret.

(2) Article R. 4127-45 du code de la santé publique : Indépendamment du dossier de suivi médical prévu par la loi, le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques.

Un cadre inachevé

Aujourd'hui les actes de télémédecine ne sont inscrits ni dans la classification commune des actes médicaux (CCAM), ni dans la nomenclature générale des actes et prestations (NGAP). Ils ne peuvent donc pas être facturés ni pris en charge par l'assurance maladie.

Des financements sont en revanche possibles dans le cadre :

- des Fonds d'Intervention pour la Qualité et la Coordination des Soins (FIQCS) ;
- des dotations « MIGAC » (missions d'intérêt général et aide à la contractualisation) ;
- des nouveaux modes de rémunérations ;
- des appels à projets, etc…

Le recours à des ordonnances électroniques serait, pour certains projets, utile mais les textes ne sont pas encore parus.

La responsabilité professionnelle des différents acteurs reste à définir plus précisément (établissements, professionnels de santé intervenant, prestataires de service, fournisseurs de matériel…).

Comment déclarer ?

La mise en place d'un traitement de télémédecine, parce qu'il implique un partage de données de santé, doit faire l'objet d'une autorisation préalable de la CNIL (art. 25-I-1 de la loi Informatique et Libertés). Un formulaire de demande d'autorisation en ligne est disponible sur le site de la CNIL (www.cnil.fr).

Dans l'hypothèse d'un recours à un hébergeur de données de santé, ce dernier doit être agréé (voir fiche sur Les hébergeurs de données de santé).

Fiche n°11 - Les hébergeurs de données de santé : un agrément nécessaire

L'externalisation des données de santé auprès d'un organisme spécialisé, distinct du professionnel ou de l'établissement de santé qui soigne le malade a été placée sous contrôle. Le but recherché est d'amener les acteurs de l'hébergement au plus haut niveau de sécurité afin d'offrir un espace de confiance aux patients et aux professionnels.

Les hébergeurs de données de santé : de quoi s'agit-il ?

Les professionnels de santé, les établissements de santé et la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet : les hébergeurs de données de santé (article L.1111-8 du code de la santé publique).

L'activité d'hébergement consiste dans l'organisation du dépôt et de la conservation des données personnelles de santé, afin d'assurer leur pérennité et leur confidentialité. Un contrat est passé entre l'hébergeur et la personne ou l'organisme à l'initiative du dépôt de ces données (R. 1111-13 du code de la santé publique).

L'activité d'hébergement des données de santé peut être définie comme toute activité d'externalisation, de détention et de conservation des données personnelles de santé recueillies ou produites à l'occasion d'un acte de prévention, de diagnostic ou de soins et confiées à un tiers qui n'a pas eu mission de les collecter.

Ce dispositif d'encadrement est donc susceptible de concerner un grand nombre d'applications comme le dossier médical personnel (DMP), le dossier pharmaceutique (DP), les réseaux de soins dès lors qu'ils font héberger leurs données de santé, les sites ouverts au public qui hébergent les données de santé des patients qui s'y connectent….

Hébergement et Consentement

L'hébergement de données ne peut avoir lieu qu'avec l'accord de la personne concernée lorsqu'il existe un partage des données à des fins de coordination des soins.

Toutefois, par dérogation aux dispositions précédentes, les professionnels et établissements de santé peuvent utiliser leurs propres systèmes ou des systèmes appartenant à des hébergeurs agréés, sans le consentement exprès de la personne concernée. Cela est possible dès lors que l'accès aux données détenues est limité au professionnel de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée. Cependant, une information sur l'externalisation des données est préconisée.

La procédure d'agrément

Le décret du 4 janvier 2006 définit les conditions de l'agrément, organise la procédure et fixe le contenu du dossier qui doit être fourni à l'appui de la demande.

- **1ère étape : le contenu de la demande d'agrément**

Le candidat à l'agrément doit compléter un dossier en s'appuyant sur un référentiel élaboré par l'ASIP Santé en concertation avec les industriels du secteur et la CNIL, composé de 8 formulaires. Ce référentiel est disponible sur le site de l'ASIP Santé (http://esante.gouv.fr).

- **2ème étape : le dépôt du dossier**
  Le candidat doit adresser, en recommandé avec accusé de réception, son dossier de demande d'agrément au format électronique sur CD-ROM ou DVD-ROM, accompagné de deux exemplaires papiers complets, à l'adresse suivante :

  ASIP Santé
  Secrétariat du comité d'agrément des hébergeurs
  9, rue Georges Pitard - 75015 PARIS

  L'Agence qui assure le secrétariat de la procédure en adresse une copie à la CNIL.

- **3ème étape : l'avis de la CNIL**
  La CNIL dispose d'un délai de 2 mois, renouvelable une fois, pour donner son avis sur la demande d'agrément. En pratique, l'avis de la CNIL interviendra donc dans un délai maximum de 4 mois. Une fois adopté, la CNIL transmet son avis au comité des hébergeurs.

  Cet agrément est délivré pour une durée de trois ans par le ministre en charge de la Santé. L'agrément porte sur une prestation particulière : aucun organisme n'est agréé en général.

- **4ème étape : l'avis du CAH**
  Le comité d'agrément des hébergeurs placé auprès du ministre en charge de la Santé se prononce sur la conformité du dossier au regard des dispositions du décret du 4 janvier 2006 dont les exigences sont traduites dans le référentiel précité. Il émet son avis dans le mois qui suit la réception du dossier transmis par la CNIL (deux mois maximum).

- **5ème étape : la décision du ministre**
  Le ministre en charge de la Santé prend sa décision dans un délai de deux mois suivant l'avis du comité d'agrément.

Les mesures de sécurité

- **L'authentification :**

L'hébergeur doit mettre en place des moyens de vérification des habilitations des professionnels de santé.

Il veille à ce que seuls les personnels intervenant dans la prise en charge du patient (l'équipe de soins), aient accès aux données de nature médicale ou médico-sociale, couvertes par le secret professionnel.

Pour assurer la confidentialité des informations médicales, la loi prévoit une authentification forte des professionnels de santé par l'utilisation d'une carte de professionnel de santé (CPS) ou un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS, pour toute transmission ou tout accès aux données de santé. Ces dispositions doivent désormais être interprétées à l'aune des dispositions de la loi

« Hôpital Patient Santé Territoires » et des référentiels de sécurité définis par l'ASIP Santé qui a fixé un cadre national d'interopérabilité et de sécurité qui spécifie les standards à utiliser dans le contexte des échanges de données de santé applicable à la télémédecine et au DMP.

• La traçabilité :

Les hébergeurs doivent journaliser les accès, réussis ou en échec, et les actions effectuées par tous les intervenants sur les systèmes et les données de santé (article R.1111-14 du code de la santé publique).

Les habilitations nécessaires pour accéder à ces traces doivent être clairement établies. L'accès ne doit être possible qu'en lecture seule, c'est-à-dire sans possibilité de modification ou de suppression.

La traçabilité n'est dissuasive que si elle est connue et contrôlée. C'est pourquoi la Commission estime qu'elle doit s'accompagner d'une sensibilisation préalable du personnel (par exemple, par la rédaction et la diffusion d'une charte informatique), ainsi que d'un contrôle organisé et effectif de ces traces.

Pour aller plus loin

Se référer au guide relatif à *« la sécurité des données personnelles »*, fiche n°8 – La traçabilité et la gestion des incidents.

• Le chiffrement :

Pour garantir la confidentialité des données, le chiffrement des données doit intervenir non seulement sur les canaux assurant les échanges, mais aussi sur les données elles-mêmes.

Pour cela, les données doivent être chiffrées au moyen d'un algorithme réputé fort. À cet effet, il est indispensable d'utiliser un mécanisme cryptographique robuste, susceptible de résister à un attaquant ayant d'importantes ressources (niveau de compétence, capacité de calcul, temps, argent…). Il est possible de se référer sur ce point aux « règles de bonnes pratiques » édictées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ainsi que dans les référentiels de sécurité définis par l'ASIP santé.

Pour aller plus loin

Se référer au guide relatif à *« la sécurité des données personnelles »*, fiche n°17 – Le chiffrement.

• Les télécommunications :

Afin d'assurer la confidentialité et l'intégrité des données de santé, l'hébergeur doit mettre en place, entre les établissements de santé et le site, des liaisons fiables en utilisant des protocoles réseau sécurisés ainsi que des liens sécurisés entre le site principal et le site secondaire de l'hébergeur.

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiches n°10 – La sécurité du réseau informatique interne et 11 – La sécurité des serveurs et des applications.

• Les contrôles de la CNIL :

Avec la multiplication des transmissions de données médicales et l'accroissement du nombre de personnes susceptibles d'accéder aux réseaux informatiques, le déploiement de solutions de sécurité effectives et de haut niveau est aujourd'hui une priorité renforcée. La CNIL, particulièrement vigilante sur ce point, a inscrit les hébergeurs de données de santé à caractère personnel à l'ordre du jour de son programme annuel des contrôles. Un ordre public propre à garantir la sécurité des données de santé est ainsi en cours de construction auquel elle entend participer activement.

• La pérennité des données :

Toutes les données doivent être sauvegardées et archivées de manière à assurer leur pérennité.

Pour ce faire, l'hébergeur doit s'assurer que les données n'ont pas été modifiées (hachage, signature ou autre), mettre en place un chiffrement et des moyens permettant d'assurer la conservation des données.

Sur ce dernier point, certaines mesures sont importantes, telles qu'une redondance des sauvegardes, des mesures de restauration en cas de perte d'une partie ou de la totalité des données. Des tests réguliers des sauvegardes doivent être effectués. Il faut également veiller à sauvegarder les données sur des supports ayant une longévité suffisante ; à titre d'exemple, la longévité des CD et DVD dépasse rarement 4/5 années.

Pour aller plus loin

Se référer au guide relatif à « la sécurité des données personnelles », fiche n°6 – Les sauvegardes et la continuité d'activité et fiche n°13 – L'archivage.

Informations complémentaires

L'ASIP Santé met à disposition sur son site Internet :

- **les référentiels de sécurité et d'interopérabilité (http://esante.gouv.fr/contenu/referentiels),**
- **les formulaires de constitution des dossiers de demande d'agrément (http://esante.gouv.fr/contenu/formulaires-du-referentiel-de-constitution-des-dossiers-de-demande-dagrement),**
- **la liste des hébergeurs de données de santé à caractère personnel agréés,**
- **une foire aux questions (FAQ) sur le référentiel de constitution de dossier.**

Fiche n°12 - L'Identifiant National de Santé : INS calculé – INS aléatoire

Jusqu'à présent, un patient se voyait attribuer un identifiant de santé différent dans chaque système de prise en charge. L'identifiant national de santé a pour vocation d'éviter la création de multiples identifiants locaux et de garantir ainsi une identification fiable, unique et pérenne des patients lors des échanges de données de santé qui les concernent. Ainsi, il facilite les échanges de données concernant chaque patient pour sa prise en charge. L'article L. 1111-8-1 du code de la santé publique prévoit la création d'un identifiant de santé des bénéficiaires de l'assurance maladie pris en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé.

Un Identifiant National de Santé (INS) : plusieurs étapes

Cet identifiant a vocation à être utilisé à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé et en particulier pour l'ouverture et la tenue du dossier médical personnel (DMP). Un décret, pris après avis de la CNIL, fixera le choix de cet identifiant ainsi que ses modalités d'utilisation. La CNIL n'en a pas été saisie à ce jour, bien que le principe d'un identifiant qui ne serait pas le NIR semble acquis

La mise en place de l'identifiant national de santé (INS) est prévue en deux étapes successives : un INS calculé (INS-C) puis un INS aléatoire (INS-A).

L'INS-C est un identifiant transitoire. Il permet d'ores et déjà l'identification des patients au niveau national ou régional. Ainsi, il facilite le déploiement d'échanges ou le partage de données de santé dans le cadre de projets régionaux ou nationaux. L'INS-C est composé de 20 chiffres et de 2 chiffres correspondant au code de détection d'erreur.

Le dossier de conception de l'INS-C est disponible sur le site de l'ASIP Santé depuis le 4 novembre 2009. Il permet sa mise en œuvre par les systèmes d'information de santé.

L'INS-A, non disponible actuellement, serait généré aléatoirement et attribué par un système central dès la création du NIR. Il serait accessible via un télé-service national aux professionnels de santé et aux établissements après lecture de la carte vitale du patient. Il serait composé de 10 chiffres aléatoires attribués par le système central de gestion des INS-A et de 2 chiffres correspondant au code de détection d'erreur.

Les caractéristiques de l'INS

L'identifiant national de santé (INS) est :

- attribué à chaque bénéficiaire de l'assurance maladie qu'il soit majeur ou mineur, français ou étranger ;
- fiable : il est généré à partir du NIR certifié par le RNIAM (Répertoire national inter régimes de l'assurance maladie) ;
- unique : un seul INS par bénéficiaire tout au long de sa vie ;
- un outil qui évite d'une part les doublons et de ce fait la création de plusieurs dossiers pour une même personne et d'autre part les collisions à savoir, le rattachement des données de santé d'une personne à une autre ;
- non signifiant : il ne permet pas de déduire des informations relatives à la personne.

L'INS-C est calculé par le logiciel du professionnel de santé ou de tout système d'information de santé (établissement de santé, réseau, …) à partir de traits d'identité figurant dans la carte d'assurance maladie du patient auxquels est appliqué un algorithme.

L'INS-C du patient peut être conservé dans le logiciel ou le système d'information du professionnel de santé. Il peut également être transmis à un autre professionnel qui n'est pas en contact direct avec le patient comme certains laboratoires d'analyse.

Fiche n°13 - Les recherches médicales : un cadre spécifique

La création de fichiers en matière de recherche médicale est soumise à une procédure particulière (chapitre IX de la loi du 6 janvier 1978 modifiée en août 2004).

Entrent dans ce cadre les études épidémiologiques, les registres des cancers, les recherches en pharmaco épidémiologie…

1. Les principes généraux et l'éthique

La loi Informatique et Libertés modifiée reconnaît un caractère sensible aux données de santé et pose le principe de l'interdiction de collecter et de traiter ces données (article 8).

D'une manière générale, la révélation d'une information médicale par un médecin constitue une rupture du secret médical, passible de sanctions pénales (article 226-13 du code pénal).

Des dérogations à ce principe d'interdiction sont prévues en particulier à des fins de recherche médicale. Une levée du secret médical est alors possible. Mais, elle est strictement encadrée.

2. Les garanties nécessaires

La levée du secret professionnel à des fins de recherche médicale est possible à condition que la personne concernée soit clairement informée de la finalité de la recherche, des catégories de données traitées, des modalités d'exercice de ses droits d'accès et de rectification et du caractère facultatif de sa participation.

La CNIL exerce une vigilance particulière en ce qui concerne l'information des personnes concernées dans la mesure où cette information conditionne l'exercice du droit d'opposition discrétionnaire reconnu par la loi (art 56). Les demandes de dérogation à l'obligation d'information font l'objet d'un examen au cas par cas. Le caractère rétrospectif d'une étude ne justifie pas, à lui seul, une dérogation à l'information des personnes.

L'utilisation, en matière de recherche, de données directement identifiantes est rare et doit être justifiée. Fréquemment, les chercheurs recourent à des tables de correspondance entre l'identité du patient et son numéro d'inclusion dans l'étude conservées par les investigateurs. La CNIL veille alors au strict cantonnement de cette table de correspondance.

En outre, le responsable du traitement est tenu de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Ainsi, la communication de données de santé directement ou indirectement identifiantes doit être sécurisée. La confidentialité, l'intégrité et l'authenticité des informations doivent être assurées. Si des échanges par messagerie électronique sont prévus, les pièces à transmettre doivent être chiffrées.

3. Une procédure spécifique : l'autorisation

Les fichiers ayant pour finalité la recherche dans le domaine de la santé sont soumis à autorisation préalable de la CNIL (article 53 de la loi du 6 janvier 1978 modifiée).

Sont concernés, les projets de recherche médicale qui nécessitent le recueil et la transmission à l'organisme de recherche de données directement ou indirectement identifiantes. Exemples : suivi longitudinal de patients atteints de diabète, rôle des facteurs de risque environnementaux et génétiques des cancers, étude des déterminants professionnels et sociaux de la santé, évaluation des résultats à long terme de l'implantation de tel dispositif médical…

Une procédure en deux temps :

- 1ère étape :
  une demande d'avis est adressée au Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS). Ce dossier comporte l'identité des responsables, le protocole de recherche, les avis rendus antérieurement par des instances scientifiques ou éthiques. Le Comité dispose d'un délai d'un mois pour notifier son avis.

- 2ème étape, après avis du CCTIRS :
  une demande d'autorisation doit être effectuée auprès de la CNIL. Ce dossier comporte : le formulaire de demande d'autorisation « recherche médicale », le dossier envoyé au CCTRIS et son avis, les modalités d'information des personnes (note, consentement). La Commission dispose d'un délai de 2 mois, éventuellement renouvelable une fois, pour notifier son autorisation. A défaut de décision dans ce délai, son silence vaut décision de rejet.

Pour les catégories les plus usuelles de traitements qui ont pour finalité la recherche dans le domaine de la santé et portent sur des données ne permettant pas une identification directe des personnes concernées, la Commission peut homologuer et publier des méthodologies de référence en concertation avec le CCTIRS. A ainsi été publiée une méthodologie de référence pour les recherches biomédicales (MR001) : essais cliniques, études préalables à la mise sur le marché de médicaments. Dans cette hypothèse, une déclaration simplifiée (engagement de conformité) auprès de la CNIL suffit.

En pratique

L'ensemble des procédures en matière de recherche médicale peuvent s'effectuer en ligne sur le site de la CNIL : www.cnil.fr

4. Cas particuliers

Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients (dossier médical du patient) ne sont pas soumis aux présentes dispositions. Il en va de même pour les traitements qui permettent d'effectuer des études à partir de données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif (études mono-centriques).

Ainsi, les recherches médicales, qui ne nécessitent pas de transmission d'informations directement ou indirectement identifiantes à l'extérieur de la structure responsable du traitement, relèvent du régime de la déclaration normale, sauf s'il existe une rupture dans le secret professionnel.

Fiche n°14 - Les maladies à déclaration obligatoire

Certaines maladies infectieuses qui nécessitent une intervention urgente locale, nationale ou internationale 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).

Quelles sont les maladies concernées ?

Une trentaine de maladies sont concernées par la déclaration obligatoire (sida, choléra, rage…). L'objectif est de détecter et de déclarer ces maladies afin de mettre en place des dispositifs permettant de prévenir les risques d'épidémie, analyser l'évolution de ces maladies et adapter au mieux les politiques de santé publique.

La **liste** de ces maladies est disponible **sur le site de l'InVS** (http://www.invs.sante.fr/surveillance/mdo/).
L'inscription d'une maladie sur la liste des maladies à déclaration obligatoire fait l'objet d'une décision du ministre de la Santé rendue publique par décret.
Il s'agit de plusieurs maladies nécessitant :

- des mesures exceptionnelles au niveau international (peste, choléra, fièvre jaune…) ;
- une intervention urgente au niveau local, national ou international (tuberculose, rage, Infection invasive à méningocoque, poliomyélite, diphtérie…) ;
- une évaluation des programmes de prévention et de lutte menés pour en mesurer l'efficacité et les adapter (sida, tuberculose, tétanos …) ;
- une évaluation et un suivi (maladies graves) en raison de leur forte morbidité et de leur risque de séquelles (sida, légionellose …) ;
- un approfondissement des connaissances comme les maladies émergentes ou mal connues (maladie de Creutzfeldt-Jakob).

Les acteurs de la déclaration obligatoire

Le dispositif de surveillance des maladies à déclaration obligatoire repose sur trois types d'acteurs :

- les biologistes et les médecins libéraux et hospitaliers qui suspectent et diagnostiquent les maladies ;
- les médecins inspecteurs de santé publique des agences régionales de santé (ARS) et leurs collaborateurs qui sont chargés de réaliser la surveillance de ces maladies au niveau départemental ;
- les épidémiologistes de l'Institut de veille sanitaire (InVS) qui surveillent l'état de santé de la population.

Comment l'anonymat est-il garanti ?

Le dispositif de notification anonymisée des maladies à déclaration obligatoire a nécessité de nombreux travaux communs entre les services de l'Etat, les associations de défense des droits des personnes et les professionnels de santé. L'ensemble du dispositif ainsi que les fiches de notification ont été examinés par la Cnil et font l'objet d'un arrêté du ministre chargé de la Santé publié au Journal officiel.

La CNIL a considéré que l'anonymat des personnes était garanti par la technique d'anonymisation - double et irréversible - retenue par l'InVS qui 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 aux médecins inspecteurs de santé publique des agences régionales de santé (ARS), à charge pour eux de la transmettre à l'InVS qui procédera à une seconde anonymisation.

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

Les outils

L'InVS, via son site internet (http://www.invs.sante.fr/), met à la disposition des professionnels de santé les fiches de déclaration et des dépliants d'information.

Fiche n°15 - Le dépistage anonyme du VIH et des infections sexuellement transmissibles (IST)

Une levée de l'anonymat des personnes consultant les centres de dépistage anonymes et gratuits du VIH et Centres d'information, de dépistage et de diagnostic des infections sexuellement transmissibles est possible dans certaines conditions spécifiques.

Quelles sont les structures concernées ?

- Les Consultations de dépistage anonyme et gratuit du VIH (CDAG) et des hépatites virales B et C.
- Les Centres d'information, de dépistage et de diagnostic des infections sexuellement transmissibles (CIDDIST)

Le respect de l'anonymat des consultants régit l'activité de ces structures. Un code d'anonymat reporté sur une fiche est demandé au consultant à chaque consultation.

Pourquoi cette possibilité de lever l'anonymat des consultants ?

Les modalités de prise en charge des personnes séropositives et, en particulier, les traitements anti-rétroviraux et les trithérapies permettent de retarder, voire de faire régresser l'évolution de la maladie, en cas de traitement précoce. Or, les données épidémiologiques ont montré l'existence de retards dans le dépistage comme dans la prise en charge. La levée de l'anonymat est alors apparue comme un moyen d'améliorer et d'accélérer l'accompagnement du consultant dans le parcours de soins.

Le Conseil National du Sida et de la Haute Autorité de Santé a donc recommandé une dérogation au principe de l'anonymat.

Dans quel cas la levée de l'anonymat est-elle possible ?

Exclusivement dans l'intérêt thérapeutique du consultant, à savoir lorsque le consultant présente des signes cliniques apparemment significatifs d'une pathologie ou en cas de résultat biologique positif.

Les personnes pourront-elles toujours bénéficier d'un depistage anonyme ?

Oui. La levée de l'anonymat reste facultative.

Le consultant est informé de la possible levée de l'anonymat au moment de son accueil dans la structure par la remise d'une notice d'information, puis au cours de la consultation initiale avec le médecin. Il n'a pas à motiver sa décision et est libre de revenir à tout moment sur son choix. Il est également informé du fait que le choix de l'anonymat ne fait pas obstacle à sa prise en charge, à son orientation vers le système de soins et est sans incidence sur la gratuité des actes pratiqués.

Son consentement exprès à la levée de l'anonymat est recueilli par écrit et consigné par le médecin dans son dossier médical.

Quelles sont les informations recueillies ?

Elles concernent l'identité et les coordonnées du consultant (nom, prénom, adresse, numéro de téléphone) et sont recueillies par le médecin sur la base de ses déclarations.

Comment est garantie la sécurité des données ?

Les données d'identification sont consignées dans le dossier médical et ne sont accessibles qu'au seul personnel soignant habilité, dans le cadre de la prise en charge du consultant.

Combien de temps sont conservées les données ?

Tous les éléments d'identification de la personne sont supprimés en cas de retrait du consentement du consultant à la levée de l'anonymat.

Dans la mesure où la levée de l'anonymat vise à améliorer la prise en charge médicale des consultants et leur orientation dans le système de soins, la CNIL a demandé que les données d'identification soient détruites en cas de résultats négatifs ou une fois le patient effectivement entré dans le système de soins.

Fiche n°16 - Les cartes santé : carte Vitale, CPS

La carte Vitale est la carte d'assurance maladie en France. Elle identifie chaque bénéficiaire de l'assurance maladie et permet de connaître ses droits à remboursement des dépenses de santé.

La carte professionnelle de santé, CPS, authentifie le professionnel de santé, lui permet d'accèder à des données de santé et d'assurer la sécurité des documents qu'il transmet.

La CPS associée à la carte Vitale permet, notamment, dans le cadre de la médecine libérale, l'envoi sécurisé vers l'assurance maladie de feuilles de soins dématérialisées au travers d'un réseau appelé SESAM Vitale.

La carte d'assurance maladie : carte Vitale

La carte Vitale est une carte à puce de la taille d'une carte bancaire. Elle est envoyée par chaque régime d'assurance maladie à ses bénéficiaires de plus de 16 ans. Elle permet de justifier les droits du titulaire de la carte (ou de ses ayants droit, mineurs ou conjoint) à l'assurance maladie.

La carte Vitale est identique pour tous les régimes d'assurance maladie et valable partout en France.

Les premières versions de la carte Vitale diffusées en 1998 à chaque assuré social (ouvrant-droit) étaient des cartes familiales (assurés et ayants droit). A partir de 2001 la carte Vitale a été distribuée aux ayants droit de 16 ans et plus. Les enfants de moins de 16 ans peuvent aujourd'hui être inscrits sur les cartes des deux parents à la demande de ces derniers.

Depuis novembre 2006, elle est progressivement remplacée par la nouvelle carte Vitale 2. Le visuel de celle-ci inclut une photographie du titulaire de la carte et un signe en relief afin de permettre l'identification de la carte par les mal-voyants.

Contenu de la carte Vitale

La carte d'assurance maladie comporte les données médico-administratives suivantes : les noms et prénoms du titulaire, sa photographie, son adresse, les données relatives au choix du médecin traitant, éventuellement les données relatives à la protection complémentaire, sa situation en matière d'accident du travail, de maladies professionnelles et aux derniers accidents ou maladies professionnelles reconnus, les données relatives à l'accès aux soins dans un autre État membre de l'Union européenne, les coordonnées d'une personne à prévenir en cas de nécessité, la mention indiquant que son titulaire a eu connaissance des dispositions de la réglementation sur le don d'organe.

Les informations relatives à l'exonération du ticket modérateur (longue maladie, 100%) contenues dans la carte ne sont accessibles qu'aux personnes titulaires d'une carte professionnelle de santé (CPS) ou d'une carte de professionnel d'établissement (CPE).

Mise à jour de la carte

Chaque année, le titulaire de la carte Vitale doit mettre à jour sa carte sinon il ne pourra pas bénéficier de la dispense d'avance de ses frais médicaux.

En cas de changement de situation, l'assuré doit mettre à jour sa carte. Il dispose d'un mois pour effectuer la mise à jour, après information par la caisse, de la prise en compte de son changement de situation. A défaut de mise à jour, la carte est temporairement inutilisable.

Carte Vitale et consentement

La carte Vitale constitue également une des clés d'accès à plusieurs applications contenant des données de santé. Ainsi, la loi prévoit que le patient accepte que le médecin accède à son historique des remboursements en lui remettant sa carte Vitale. L'accès au dossier pharmaceutique est subordonné à la remise de la carte.

Le rôle ambigu de la carte Vitale (transmission des feuilles de soins à l'assurance maladie et consentement pour l'accès à des données de santé) a été soulevé par la Cnil qui considère que la simple remise de la carte n'atteste pas de la réalité du consentement du patient.

La dématérialisation des feuilles de soins

L'envoi des feuilles de soins dématérialisées (factures des prestations de soins) vers l'assurance maladie repose sur la carte Vitale des bénéficiaires de l'assurance maladie et la CPS au travers du réseau sécurisé appelé SESAM Vitale (GIE SV).

L'assurance maladie obligatoire et la complémentaire sont raccordées au réseau SESAM Vitale via des portails d'échanges sécurisés de données.

Les données figurant dans les feuilles de soins électroniques sont celles nécessaires au paiement des prestations.

Ce mode de transmission permet de traiter plus rapidement les demandes de remboursements des frais médicaux et évite à l'assurance maladie un travail fastidieux de ressaisie des informations susceptibles de générer des erreurs.

CPS : l'atout sécurité

Tout professionnel de santé qui exerce une activité rendant nécessaire l'accès à un système d'information de santé peut disposer d'une carte émise par l'ASIP Santé.

La carte de professionnel de santé (CPS) est une carte à puce qui permet à son titulaire d'attester de son identité professionnelle et de ses qualifications auprès des systèmes informatisés de santé dans la cadre de l'accès aux données de santé à caractère personnel ou toute action effectuée sur celle-ci.

La CPS, délivrée par l'ASIP Santé, se généralise à l'ensemble des professionnels du secteur libéral de la santé et connaît une progression plus lente dans les établissements de soins (hôpitaux, cliniques, centres de santé…). Chaque catégorie de personnels concernée se voit attribuer une CPS.

Plusieurs types de cartes existent selon la profession exercée et le niveau de responsabilité du porteur : Carte de Professionnel de santé en Formation (CPF), Carte de Directeur d'Établissement (CDE) et une Carte de Personnel d'Établissement (CPE), Carte de Personnel Autorisé (CPA) et la Carte de Professionnel de Santé (CPS) pour les professions à Ordre ou réglementées.

• Authentification
Cette carte possède un certificat d'authentification, protégé par un mot de passe, ce qui assure que la personne souhaitant se connecter aux logiciels est un professionnel de santé habilité.
Ces cartes ne peuvent être lues que par un lecteur homologué par le GIE Sesam Vitale.

• Définition du tableau des habilitations
L'ASIP Santé tient à jour un tableau regroupant les professionnels de santé disposant d'une CPS. Ce tableau permet de savoir quels sont les professionnels de santé habilité, leur fonction et si la carte a été désactivée ou non. Il est donc important de signaler toute perte ou vol de carte à l'ASIP Santé.

• Signature électronique
Un certificat de signature électronique est également inclus dans la carte. Il permet au professionnel de santé de signer les documents et informations qu'il crée, ce qui assure leur intégrité c'est-à-dire que les documents n'ont pas été modifiés par une personne autre qu'un professionnel de santé.

• Chiffrement des données / chiffrement de transport
Via les certificats, les professionnels de santé peuvent également chiffrer les données. Ce chiffrement assure la confidentialité des données lors de leur transport, notamment les pièces jointes d'un message électronique (Cf. Fiche n°5 relative à la messagerie électronique et à la télécopie).

• La nouvelle carte CPS
Depuis février 2011, les professionnels de santé se voient équipés progressivement d'une nouvelle CPS dotée de nouvelles fonctionnalités (la CPS 3). Elle est délivrée de façon systématique à tout professionnel de santé inscrit au Répertoire Partagé des Professionnels de Santé (RPPS), donc inscrits au tableau pour les professions à ordre. Des évolutions de la CPS ont été opérées pour mieux répondre aux besoins de sa généralisation : la CPS intègre les standards industriels ainsi que les fonctionnalités sans contact (lecture sans contact mieux adaptée aux contraintes de fonctionnement des établissements de santé).
Une convergence entre la CPS et la Carte Ordinale (carte professionnelle d'identification des médecins inscrits à l'Ordre) est effectuée. Une carte unique permettrait à la fois d'identifier le professionnel et d'assurer des communications sécurisées.
Les Ordres professionnels souhaitent également une convergence entre la CPS et la future carte européenne de professionnels de santé afin de faciliter la libre circulation des praticiens.

Fiche n°17 - L'éducation thérapeutique du patient : ou comment mieux gérer sa maladie

L'éducation thérapeutique (ETP) s'inscrit dans le parcours de soins du patient et a pour objectif de le rendre plus autonome en facilitant son adhésion aux traitements prescrits et en améliorant sa qualité de vie

L'éducation thérapeutique du patient : de quoi s'agit-il ?

L'éducation thérapeutique du patient (ETP) est un processus prévu par l'article 84 de la loi portant réforme de l'hôpital et relative au patient à la santé et aux territoires, dite HPST. Il est destiné à aider le patient et son entourage à mieux comprendre sa maladie afin de mieux la prendre en charge, en coopération avec les soignants et ainsi maintenir ou améliorer sa qualité de vie.

Elle comprend des activités organisées de sensibilisation, d'information, d'apprentissage et d'accompagnement psychosocial.

L'ETP prend trois formes :

- **Les programmes d'éducation thérapeutique** concernent une ou plusieurs des trente affections de longue durée (ALD 30) exonérées du ticket modérateur, ainsi que l'asthme, les maladies rares ou des problèmes de santé publique considérés comme prioritaires au niveau régional.
  Ils comportent quatre phases successives :
  - orientation du patient vers le programme d'éducation thérapeutique le plus adapté à sa situation en concertation avec son médecin traitant ;
  - réalisation d'un diagnostic éducatif permettant d'identifier les besoins (entretien individuel) ;
  - participation à des séances d'éducation thérapeutique animées par un ou plusieurs professionnels ;
  - évaluation individuelle finale du bénéficiaire du programme.

  Exemple de programmes d'éducation thérapeutique : la prise en charge du diabète ou de l'obésité.

- **Les actions d'accompagnement** ont pour objet d'apporter une assistance et un soutien aux malades ou à leur entourage dans la prise en charge de la maladie. Ces actions doivent être conformes à un cahier des charges national dont les modalités sont à définir par arrêté.

- **Les programmes d'apprentissage** ont pour objet l'appropriation par les patients de gestes techniques permettant l'utilisation d'un médicament le nécessitant. Ils sont conçus en cohérence avec les actions de santé publique menées par les autorités sanitaires, les organismes d'assurance maladie et les établissements de santé. Ils sont conçus et mis en œuvre conformément aux recommandations formulées par les autorités compétentes et notamment l'Agence française de sécurité sanitaire des produits de santé (AFSSAPS) et la Haute autorité de santé.

  Exemple de programmes d'apprentissage : l'utilisation d'un médicament pour le traitement de la sclérose en plaques.

Les modalités de mise en œuvre

- Des dispositions communes aux programmes et actions d'éducation :
  - interdiction de tout contact direct entre un malade, ou son entourage, et une entreprise exploitant un médicament ou un dispositif faisant l'objet d'un programme ;
  - le consentement préalable du patient est requis avant toute inclusion dans un programme ou une action. Il dispose d'un droit discrétionnaire de retrait ;
  - l'adhésion ou non du patient ne peut avoir de conséquence sur le remboursement des soins et prestations dont il bénéficie ;
  - le médecin traitant est informé de l'adhésion de son patient et tenu informé des principales étapes.

- Les programmes d'éducation thérapeutique :

  Ces programmes doivent répondre à un cahier des charges national défini par arrêté. En application du décret relatif aux conditions d'autorisation des programmes d'éducation thérapeutique du patient, ils sont soumis à l'autorisation du directeur général de l'Agence régionale de Santé (ARS) compétente. Le directeur général de l'ARS dispose d'un délai de deux mois, à réception d'un dossier complet, pour délivrer l'autorisation.

  L'autorisation est délivrée pour une durée de 4 ans, renouvelable 2 mois avant expiration. L'autorisation est par ailleurs caduque si le programme n'est pas mis en œuvre dans les 12 mois suivant l'autorisation, ou s'il n'est pas mis en œuvre pendant 6 mois consécutifs.

- Les actions d'accompagnement :

  Un arrêté doit définir un cahier des charges auquel doivent répondre les actions d'accompagnement.

- Les programmes d'apprentissage

  Les programmes d'apprentissage sont soumis à une autorisation délivrée par le directeur de l'AFSSAPS après dépôt d'un dossier comportant notamment une autorisation de la CNIL (cf. article R.1161-16 du CSP).

  Avant de statuer, l'AFSSAPS recueille deux avis : celui d'une association concernée par la pathologie et celui de la Commission chargée du contrôle de la publicité.

  L'autorisation est délivrée pour une durée de trois ans, renouvelable 6 mois avant expiration.

Comment déclarer ?

La mise en place de ces programmes et actions implique des formalités préalables auprès de la CNIL.

Les traitements relatifs aux programmes d'éducation thérapeutique doivent

préalablement à leur mise en œuvre faire l'objet d'une autorisation de la CNIL en application des dispositions de l'article 25-I-1°de la loi informatique et liberté (traitement à des fins de santé publique associé au traitement de données de santé). Les demandes d'autorisation adressées à la Commission doivent comporter l'autorisation de l'ARS compétente.

Toutefois, lorsque ces programmes sont mis en œuvre par un établissement de santé pour ses propres patients, le régime applicable est celui de la déclaration normale (sauf si l'accès au dossier s'opère via internet).

Les traitements relatifs aux programmes d'apprentissage doivent préalablement à leur mise en œuvre faire l'objet d'une autorisation de la CNIL en application des dispositions de l'article 25-I-1°de la loi informatique et liberté (traitement à des fins de santé publique associé au traitement de données de santé). Le décret relatif aux programmes d'apprentissage (art. R.1161-24 CSP) prévoit que la demande d'autorisation est présentée par l'opérateur choisi.

Pour aller plus loin

- décret n° 2010-904 du 2 août 2010 relatif aux conditions d'autorisation des programmes d'éducation thérapeutique du patient ;
- arrêté du 2 août 2010 relatif au cahier des charges des programmes d'éducation thérapeutique du patient et à la composition du dossier de demande de leur autorisation ;
- arrêté du 2 août 2010 relatif aux compétences requises pour dispenser l'éducation thérapeutique du patient ;
- décret n° 2010-1031 du 31 août 2010 relatif aux programmes d'apprentissage et pris en application de l'article L. 1161-5 du code de la santé publique.

Fiche n°18 - Les nouveaux modes de rémunération des professionnels de santé

Aujourd'hui, les professionnels de santé libéraux sont payés à l'acte. Ce type de rémunération n'encourage pas les prises en charge pluridisciplinaires des patients. Le ministère chargé de la santé a donc souhaité développer des modes alternatifs au paiement à l'acte des professionnels de santé dans les structures pluridisciplinaires (réseaux de santé, maisons et centres de santé…).

Les nouveaux modes de rémunération : de quoi s'agit-il ?

L'offre de soins dite de 1er recours est en pleine mutation. Les jeunes professionnels de santé choisissent souvent de se regrouper dans des structures pluridisciplinaires pour exercer de façon différente leur activité. Les modes d'exercices regroupés favorisent les échanges et une prise en charge médicale plus globale des patients. Pour permettre, dans ce cadre, le développement de services innovants en matière de prévention, d'éducation pour la santé, d'accompagnement et d'orientation dans le système de soins ou de prise en compte des aidants familiaux, des nouveaux modes de rémunération des professionnels de santé ont été prévus à l'article 44 de la loi de financement de la sécurité sociale pour 2008.

Cet article permet d'expérimenter des rémunérations alternatives au paiement à l'acte ou pouvant le compléter.

Ces nouvelles formes de rémunération évitent au patient de payer un ticket modérateur (reste à charge) et de faire l'avance des frais. Le forfait est payé directement par l'organisme auquel est affilié le patient et éventuellement sa complémentaire santé.

Ces nouveaux modes de rémunération tiennent compte de l'atteinte d'objectifs notamment de santé publique.

Les conditions à remplir

Les sites souhaitant bénéficier de ces nouveaux modes de rémunération répondent aux critères suivants :

- l'exercice au sein de la structure est pluri-professionnels et de premier recours avec au moins deux médecins généralistes et un professionnel paramédical ;
- un projet de santé formalisé décrit le mode de fonctionnement de la structure et prend en compte les besoins de santé du territoire ;
- témoigner d'un exercice coordonné des professionnels de la structure (réunion pluri-professionnelles…) ;
- témoigner d'une prise en charge globale du patient : prévention et suivi ;
- assurer la continuité des soins ;

- mettre en place un dispositif de partage d'informations sécurisé ;
- la structure doit être le lieu d'exercice principal des professionnels qui y exercent ;
- elle doit accueillir et encadrer des professionnels de santé en formation.

Le montant du forfait

Le versement du forfait est conditionné à l'atteinte d'objectifs fixés dans la convention signée avec l'Agence Régionale de Santé (ARS).

Les objectifs concernent les points suivants : dépistage des cancers, prévention de la grippe saisonnière, lutte contre l'hypertension, prise en charge du diabète, prévention de l'obésité, prévention du risque cardiovasculaire, dépistage Alzheimer, prescription par les paramédicaux, lombalgie chronique, continuité des soins, partage d'informations, organisation des pratiques, bon usage des médicaments génériques, diminution du recours à l'hospitalisation et bon usage des transports sanitaires.

Pour chaque objectif, des indicateurs sont fournis pour évaluer l'atteinte ou non des objectifs.

Pour plus d'informations, se rendre sur le site de chaque ARS (agence régionale de santé).

Comment déclarer ?

La déclaration normale de gestion des patients permet de mettre en place la gestion administrative et médicale des patients.

Les traitements mis en œuvre à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins sont soumis à une autorisation préalable de la CNIL conformément au chapitre X de la loi du 6 janvier 1978 modifiée (cf. fiche n°20 : Comment déclarer ?).

Fiche n°19 - La vente en ligne de médicaments et de produits de santé

Le développement d'internet et la création de sites destinés à la revente de médicaments ou de produits, tant en France que dans d'autres pays soulèvent des interrogations nouvelles.

Un cadre législatif encore inexistant

La Cour de Justice de l'Union européenne considère qu'il convient de distinguer les produits soumis à prescription obligatoire et les autres (décision de 2003 de la Cour de Justice de l'Union européenne). Les Etats membres de l'Union européenne peuvent interdire la vente en ligne des médicaments soumis à prescription obligatoire. La France n'a pas encore légiféré sur ce point.

Toutefois, on peut considérer qu'en France, la vente en ligne de médicaments pourrait être assimilée à de la publicité, ce qui est interdit ou strictement limité par le code de la santé publique (art. R. 4235-57 et suivants).

Les produits de santé en ligne

En France, l'Ordre des pharmaciens considère que tous les médicaments soumis à une prescription obligatoire sont exclus de la vente en ligne.

La situation des autres médicaments ou produits n'est pas totalement tranchée. Mais la prudence s'impose dans la mesure où aucun texte ne définit les modalités et les conditions d'une telle vente en ligne.

Le monopole des officines pour la vente en ligne des médicaments

Les officines bénéficient d'un monopole de vente des médicaments. Par conséquent, la vente en ligne de médicaments ne peut se réaliser que par l'intermédiaire d'un pharmacien, lequel est responsable de la vente.

> ***Attention***
>
> **La vente de médicaments en dehors d'une pharmacie est passible de poursuites pour exercice illégal de la pharmacie.**

Les dispositifs médicaux (fauteuil roulant, canne…) ne sont pas soumis au monopole de vente par des pharmaciens. Cependant, la distribution des dispositifs médicaux (lunettes, audioprothèses, fauteuil roulant, canne…) est règlementée. Des restrictions de fait sont à signaler. Ainsi, pour les dispositifs implantables (ex : stimulateurs cardiaques, implants dentaires) destinés à être utilisés par un professionnel de santé, la vente directe n'apparaît pas pertinente. Il en va de même pour les dispositifs sur mesure ou nécessitant une adaptation pour répondre aux besoins du patient (ex : lunetterie).

Les obligations des pharmaciens

Le pharmacien est soumis à une obligation de conseil qui consiste à vérifier que le produit est adapté au patient. Or, à distance, cette obligation de conseil est difficile à remplir.

La traçabilité des médicaments doit être assurée pour la gestion des retours de produits (rappel de médicaments, pharmacovigilance), cette obligation apparaît difficile à mettre en œuvre dans le cadre de la vente en ligne.

Dans l'hypothèse de produits devant être maintenus au froid (ex. vaccins), des difficultés de conservation et de distribution des produits doivent être signalés dans le cadre de la vente en ligne.

Quelques problèmes concrets

Le consentement du patient

Dans certaines hypothèses, le consentement du patient doit être recueilli (ex. dossier pharmaceutique). Cette condition est difficilement compatible avec la vente en ligne.

L'ordonnance électronique

Les textes d'application relatifs aux spécifications techniques de l'ordonnance électronique ne sont toujours pas parus à ce jour (art. R. 161-45 et R. 161-48 du code de la sécurité sociale).

Le remboursement des médicaments

Le problème de transmission de la demande de remboursement à l'assurance maladie demeure.

Fiche n°20 - Comment déclarer auprès de la CNIL : secteur santé

Les données de santé sont des données sensibles (article 8 de la loi) dont le traitement est en principe interdit, sauf exceptions. La dérogation la plus utilisée est celle prévue pour la gestion administrative et médicale des patients mis en œuvre par les professionnels et établissements de santé (art. 8-II-6°). Pour le reste, les formalités applicables varient en fonction du traitement concerné.

La gestion administrative et médicale des patients : déclaration simplifiée

• Les procédures simplifiées

- Normes simplifiées (NS)

Plusieurs mesures de simplification ont été prises par la CNIL dans le secteur santé :

- la NS n° 50 : gestion des cabinets médicaux et paramédicaux ;
- la NS n° 52 : gestion des pharmacies libérales ;
- la NS n° 53 : gestion des laboratoires d'analyses ;
- la NS n° 54 : gestion des centres d'optique.

- Autorisation unique (AU)

Certains traitements de données personnelles sensibles qui visent une même finalité et des catégories de données et de destinataires identiques, sont autorisés par la CNIL au travers de décisions-cadre, appelées autorisations uniques (AU).

• AU-013 : traitements concernant la pharmacovigilance des médicaments.

- Méthodologie de référence (MR-001)

Afin de simplifier les procédures en matière de recherche médicale, une méthodologie de référence a été adoptée le 5 janvier 2006 pour les traitements opérés dans le cadre des recherches biomédicales.

• MR 001 : traitements de données opérés dans le cadre des recherches biomédicales.

Pour tous ces traitements, une déclaration simplifiée, en conformité à l'un de ces textes, suffit. Une démarche s'effectue en ligne sur le site internet de la CNIL (www.cnil.fr).

• Le régime de droit commun : la déclaration

Pour les traitements qui ne relèvent pas d'une procédure spécifique, le principe est la déclaration normale.

Le régime de la déclaration normale est applicable aux **fichiers de gestion administrative et médicale** mis en œuvre par les professions de santé au sein des établissements de soins privés ou publics ou des centres de soins dès lors qu'ils sont nécessaires pour établir des diagnostics médicaux, administrer des soins ou des traitements, gérer des services de santé ou mettre en œuvre des actions de médecine préventive (art. 8-II-6° de la loi).

Exemples : gestion administrative des patients (facturation), gestion du

dossier médical au sein de l'établissement.

Relèvent également de la déclaration normale les traitements suivants :
- gestion du PMSI ;
- étude mono-centrique sur une pathologie ;
- gestion de la médecine du travail ;
- enquête de satisfaction ;
- gestion des campagnes de dépistage des cancers par les associations…

Le correspondant informatique et libertés : dispense de déclaration

Chaque responsable de traitement a la faculté de désigner un CIL. Cette désignation permet un allègement des formalités. Il dispense de déclarer à la CNIL la majorité des traitements, sauf les traitements relevant du régime de l'autorisation ou de la demande d'avis.

Le correspondant est cependant chargé d'inscrire sur un registre qu'il tient à jour les traitements mis en œuvre par l'organisme (Voir III : Le correspondant informatique et libertés (CIL) : un vecteur de diffusion de la culture informatique et libertés).

Les traitements relevant d'un régime d'autorisation

- Sont soumis à une **autorisation** de la CNIL prévue par l'article 25 de la loi du 6 janvier 1978 modifiée certains **traitements justifiés par un intérêt public comportant des données de santé**. C'est le cas de la mise en place d'un **dossier médical partagé** dans le cadre d'un réseau de soins, du DMP, du dossier pharmaceutique (DP), des applications médicales gérées par les services médicaux des caisses, des programmes d'apprentissages, télémédecine…

  Le site de la CNIL permet d'effectuer en ligne les demandes d'autorisation ou de télécharger le formulaire. La CNIL dispose d'un délai de deux mois (éventuellement renouvelable une fois), pour se prononcer sur la demande. En l'absence de réponse, la demande est considérée comme rejetée.

- Relèvent également d'une procédure d'autorisation :
  - les traitements mis en œuvre par des organismes privés qui utilisent le NIR (sauf si un texte le permet déjà) ou qui comportent des données biométriques ;
  - les traitements qui comportent des appréciations sur les difficultés sociales des personnes (données subjectives) ;
  - les traitements de données génétiques ;
  - les traitements portant sur les infractions condamnations ;
  - les traitements statistiques de données sensibles de l'INSEE et des services statistiques ministériels ;
  - les traitements de données sensibles qui recourent, à bref délai, à une anonymisation ;

- les traitements ayant pour objet l'interconnexion de fichiers différents ;
- et les traitements susceptibles d'exclure les personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

• **Les fichiers mis en œuvre à des fins de recherche médicale** sont soumis au régime de l'autorisation préalable prévu au chapitre IX de la loi du 6 janvier 1978 modifiée.

Une procédure spécifique en deux temps est prévue pour ces traitements qui supposent une levée du secret professionnel, sauf pour la recherche conforme à la méthodologie de référence (MR-001) soumise à une déclaration simplifiée. Le Comité consultatif (CCTIRS) doit être saisi pour avis préalablement à la demande d'autorisation auprès de la CNIL.

Les personnes concernées doivent être informées de la finalité du traitement, des données traitées, des destinataires, des modalités d'exercice des droits d'accès, de rectification, de leur droit d'opposition discrétionnaire reconnu par la loi. Les demandes de dérogations à l'obligation d'information font l'objet d'un examen au cas par cas. L'utilisation de données directement identifiantes est rare et doit être justifiée.

Le formulaire et la notice sur les formalités en matière de recherche sont disponibles sur le site de la CNIL. La demande d'autorisation peut être effectuée en ligne.

• **Les fichiers mis en œuvre à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins** sont également soumis au régime de l'autorisation préalable définie au chapitre X de la loi du 6 janvier 1978 modifiée.

Les traitements de données de santé indirectement identifiantes (sans nom, prénom ou NIR), notamment issues des fichiers des professionnels de santé, des systèmes d'information hospitaliers (PMSI), ou des caisses de sécurité sociale, transmises et exploitées à des fins d'évaluation des pratiques de soins et de prévention doivent faire l'objet d'une autorisation préalable de la CNIL.

Le formulaire et la notice relatifs à ces traitements sont disponibles sur le site de la CNIL. **La demande d'autorisation peut être effectuée en ligne.**

• Le cas particulier des **transferts de données hors de l'union européenne**

On parle de transfert lorsque des données personnelles (ex. : nom, téléphone, n° d'étude…) sont transférées depuis le territoire européen vers un pays situé en-dehors de l'Union européenne.

Ces transferts sont interdits sauf :

- si le transfert a lieu vers un pays reconnu comme «adéquat» par la Commission européenne. C'est le cas du Canada, de la Suisse, de l'Argentine, des territoires de Guernesey, de Jersey et de l'Île de Man (consulter le tableau accessible via le site de la CNIL) ;
- si des Clauses Contractuelles Types, approuvées par la Commission européenne, sont signées entre deux entreprises ;
- si des Règles internes d'entreprises (BCR) sont adoptées au sein d'un groupe ;
- si dans le cas d'un transfert vers les États-Unis, l'entreprise destinataire a adhéré au Safe Harbor ;
- si l'une des exceptions prévues par l'article 69 de la loi Informatique et Libertés est invoquée.

Les sanctions encourues en cas de non respect des règles en matière de transferts sont de 300 000 euros d'amende et de 5 ans d'emprisonnement. (Articles 226-16, 226-16 A et 226-22-1 du Code pénal).

Un pays reconnu comme « adéquat » est un pays garantissant un niveau de protection des données personnelles équivalent a celui fixé par la directive européenne.

Pour en savoir plus, consulter le site de la CNIL, rubrique « *Le transfert de données à l'étranger* »

En pratique

L'ensemble des procédures et des formulaires sont accessibles sur le site de la CNIL :

www.cnil.fr, rubrique « Déclarer »

Modèles d'affichettes d'information

Cabinet médical et paramédical

Ce cabinet dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients, à assurer la facturation des actes et la télétransmission des feuilles de soins aux caisses de sécurité sociale.

Les informations recueillies lors de votre consultation feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique réservé à l'usage de votre professionnel de santé.

Votre professionnel de santé traitant se tient à votre disposition pour vous communiquer ces renseignements ainsi que toutes informations nécessaires sur votre état de santé*.

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

**Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Lieu de soins

Ce lieu de soins dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à assurer la facturation des actes et, le cas échéant, la télétransmission des feuilles de soins aux caisses de sécurité sociale.

Les informations qui vous sont demandées feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique.

Vous pouvez accéder aux informations vous concernant auprès de votre professionnel de santé*.

**Loi n°78-17 du 6 janvier 1978 modifié een 2004 relative à l'informatique, aux fichiers et aux libertés*

Opticien

Votre opticien dispose d'un système informatique destiné à gérer plus facilement ses ventes (facturations, remboursements).

Les informations qui vous sont demandées feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique réservé à l'usage de votre opticien, et le cas échéant, de votre caisse de sécurité sociale et de votre organisme d'assurance maladie complémentaire.

Vous pouvez accéder aux informations vous concernant auprès de votre opticien*.

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

Pharmacie

Cette pharmacie est équipée d'un système informatique destiné a assurer sa gestion et la délivrance des médicaments (facturation, tiers-payant, suivi des remboursements, tenue de l'ordonnancier), ceci dans le strict respect du secret professionnel auquel sont astreints les pharmaciens.

Sauf opposition justifiée de votre part, certains renseignements vous concernant, recueillis sur la base de l'ordonnance qui vous a été délivrée, de votre carte d'assuré social ainsi que, le cas échéant, de votre carte d'assurance maladie complémentaire (mutuelle ou assurance), feront donc l'objet d'un enregistrement informatique.

L'usage en est exclusivement réservé, dans la limite de leurs attributions, à votre pharmacien, votre caisse de sécurité sociale, votre organisme d'assurance complémentaire.

Ces données pourront être traitées, de façon totalement anonyme, à des fins statistiques professionnelles.

Conformément aux dispositions de la loi Informatique et Libertés*, vous pouvez obtenir communication auprès de cette pharmacie des informations vous concernant et, le cas échéant, en demander la modification.

** Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Service hospitalier

Ce service hospitalier dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à réaliser, le cas échéant, des travaux statistiques à usage du service.

Les informations recueillies lors de votre consultation ou de votre hospitalisation, feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique. Ces informations sont réservées à l'équipe médicale qui vous suit ainsi que pour les données administratives, au service de facturation.

Conformément aux dispositions de la loi Informatique et Libertés*, vous pouvez obtenir communication des données vous concernant en vous adressant au responsable de cet établissement ou *(indiquer le service concerné ou la personne désignée à cet effet).*

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

**Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Laboratoire d'analyses médicales

Ce laboratoire d'analyses médicales dispose d'un système informatique, réservé à l'usage de son personnel habilité, pour lui permettre de gérer plus facilement la facturation des actes pratiqués ainsi que l'édition des résultats d'analyses.

Les renseignements nécessaires à l'établissement de la facturation ne sont transmis qu'aux patients et, dans le cas des procédures de tiers payant, aux organismes de sécurité sociale dont ils relèvent ainsi que, le cas échéant, à leur organisme d'assurance maladie complémentaire.

Vous pouvez accéder à ces informations en vous adressant au directeur de ce laboratoire*.

Conformément aux dispositions de l'arrêté du 2 novembre 1994, les résultats d'analyses ne peuvent être transmis qu'au patient, au praticien prescripteur et, à la demande du patient, au médecin désigné par lui.

** Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Cabinet dentaire

Ce cabinet dentaire dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à assurer la facturation des actes et la télétransmission des feuilles de soins aux caisses de sécurité sociale.

Les informations recueillies lors de votre consultation feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique réservé à l'usage de ce cabinet.

Vous pouvez avoir accès à votre dossier en vous adressant à votre chirurgien-dentiste*.

**Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés*

Modèle de formulaire de collecte de données personnelles

…… *(Veuillez indiquer l'identité du responsable du traitement)*

« Les informations recueillies font l'objet d'un traitement informatique destiné à …..... *(Veuillez préciser la finalité)*. Les destinataires des données sont : …… *(précisez)*.

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à …… *(Veuillez préciser le service et l'adresse)*.

[Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.]

Pour aller plus loin

Consulter les modèles de mentions légales sur le site de la CNIL : http://www.cnil.fr/vos-responsabilites/informations-legales

Modèle de demande de droit d'accès à son dossier médical

Expéditeur :

Monsieur le Directeur
Service du droit d'accès
ADRESSE

Recommandée avec accusé de réception

Objet : Demande de droit d'accès à mon dossier médical

Madame, Monsieur,
Docteur (ou Monsieur le Directeur),

En application des dispositions de l'article 43 de la loi n° 78-17 du 6 janvier 1978 modifiée en août 2004, je vous prie de bien vouloir m'adresser l'ensemble des données dont vous disposez concernant ma santé, qu'elles soient sous forme papier ou sur support informatique (dans cette dernière hypothèse, avec indication de la signification des codes, sigles ou abréviations éventuellement utilisés).

Pour faciliter le traitement de ma demande, je vous précise que [à compléter]...

Je vous prie d'agréer, Docteur (Monsieur le Directeur), l'expression de mes salutations distinguées.

Signature :

Modèle de clause de confidentialité en cas de sous-traitance

Les supports informatiques fournis par la ……. et tous documents de quelque nature qu'ils soient résultant de leur traitement par la société ……. restent la propriété de …..

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226.13 du code pénal). Conformément aux articles 34 et 35 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la société ….. 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.

La société …….. s'engage donc à respecter et à faire respecter par son personnel, de façon absolue, les obligations suivantes :

- ne prendre aucune copie des documents et supports d'informations confiés par la société et utilisés par la société à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du présent contrat ;

- 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, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de 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 ;

ou à :

- restituer intégralement les supports d'informations selon les modalités prévues au présent contrat.

A ce titre, également, la société ….. ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché. Les supports d'informations qui lui seront remis devront être traités sur le territoire français métropolitain.

La ….. se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société…..

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

La ……. 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.

Tableau récapitulatif : quelle déclaration pour quel fichier ?

Si vous avez désigné un Correspondant Informatique et Libertés (CIL), seuls les traitements figurant dans les champs grisés doivent faire l'objet de formalités auprès de la CNIL.

VOUS ÊTES :	Finalité du fichier	Formalités déclaratives	A savoir…
Professions libérales de santé médicales et paramédicales*	Paie	AUCUNE	Dispense de déclaration n°1
	Gestion administrative et médicale des patients	NS n°50	Obligation d'utiliser la Carte Professionnelle de Santé
	Gestion du personnel (cabinets médicaux)	NS n°46	
Pharmacie	Gestion courante de la pharmacie et dossier pharmaceutique (DP)	NS n°52	Obligation d'utiliser la CPS
	Vidéosurveillance dans un lieu ouvert au public, partie de pharmacie accessible au public	Autorisation préfectorale	
	Vidéosurveillance dans un lieu privé avec enregistrement d'images (ex. : les réserves, locaux réservés au personnel)	DN	Affichage pour information des personnes
	Gestion du personnel	NS n°46	
	Paie	AUCUNE	Dispense de déclaration n°1
Laboratoires d'analyses de biologie médicale	Gestion courante du laboratoire	NS n°53	Obligation d'utiliser la CPS
	Gestion du personnel	NS n°46	
	Paie	AUCUNE	Dispense de déclaration n°1
	Site internet « vitrine »	AUCUNE	Dispense de déclaration n°6
	Vidéosurveillance dans un lieu ouvert au public, partie de pharmacie accessible au public	Autorisation préfectorale	
Opticiens	Gestion administrative des clients	NS n°54	
	Gestion du personnel	NS n°46	
	Vidéosurveillance dans un lieu privé	DN	Affichage pour information des personnes
	Paie	AUCUNE	Dispense de déclaration n°1

** Médecins, infirmières libérales, orthophonistes, kinésithérapeutes…*

Etablissements de soins publics ou privés OU Centres d'examen de santé gérés par les organismes de sécurité sociale ou les collectivités territoriales (dispensaires…)	Gestion administrative (facturation…)	DN	
	Gestions des repas	DN	
	Gestion du dossier médical	DN	
	Gestion des urgences, du laboratoire, du service de radiologie…	DN	
	Frappe de comptes rendus et de courriers médicaux au sein par un prestataire en Europe	DN	Une clause de confidentialité devra également être signée avec le prestataire
	Constitution d'une cohorte mono centrique de patients	DN	
	Paie	AUCUNE	Dispenses de déclaration n°1 et 2
	Gestion des fichiers de fournisseurs comportant des personnes physiques	AUCUNE	Dispenses de déclaration n°4
	Vidéosurveillance dans un lieu ouvert au public	Autorisation préfectorale	Affichage pour information des personnes
	Autocommutateur	NS 39	
	Gestion des contrôles d'accès aux locaux	NS n°42	
	Gestion du personnel	NS n°46	
	Utilisation de services de téléphonie fixe et mobile sur les lieux de travail	NS 47	
	Dispositifs biométriques contrôle d'accès	AUTORISATION UNIQUE	AU n°007 (contour de la main) AU n°008 (empreinte digitale) AU n°019 (réseau veineux) AU n°027 (Biométrie pour les ordinateurs portables)
	Site internet « vitrine »	AUCUNE	
	Enquêtes de satisfaction	DN	
	PMSI	DN	
	Programme d'éducation thérapeutique (Mono centrique)	DN	Si le programme concerne uniquement les patients de l'établissement
	Gestion des risques	AUTORISATION	

	Recherches médicales supposant une levée du secret médicale	AUTORISATION recherche	Après avis du Comité Consultatif
Institut de Recherches médicales Laboratoires pharmaceutiques	Recherches biomédicales (essais cliniques)	Engagement de conformité à la méthodologie de référence : MR001	Un seul par organisme pour toutes les études présentes et à venir qui relèvent de la méthodologie de référence
	Pharmacovigilance	Autorisation Unique 013	
	Autres recherches médicales supposant une levée du secret médicale	AUTORISATION recherche	Après avis du Comité Consultatif
	Autorisation temporaire d'utilisation de médicaments (ATU)	DN	
Registre des cancers	Mise en place du registre	AUTORISATION recherche	Après avis du Comité Consultatif
Dossier médical partagé	Réseaux de santé avec un dossier médical partagé	AUTORISATION	
	Dossier médical personnel (DMP)	AUTORISATION	
	Dossier pharmaceutique déposé par le CNOP	AUTORISATION	
Hébergeur de données de santé	Hébergement de données de santé	Avis de la CNIL + agrément du Ministère	
Organismes d'assurance maladie	Gestion de l'accueil	DN	
	Gestion des remboursements	DN	
	Campagne de dépistage des cancers	DN	
	Campagnes de prévention	DN	
	Gestion des adhérents des complémentaires santé	DN	
	Accès aux données détaillées des feuilles de soins électroniques anonymisées par les complémentaires santé	AUTORISATION	
	Lutte contre la fraude avec la collecte de données relatives aux infractions, condamnations	AUTORISATION	

	Web médecin ou historique des remboursements	AUTORISATION	
	Gestion du service médical de l'assurance maladie	AUTORISATION	
	Télé-service de l'administration avec un identifiant national	AVIS	
Autres	Evaluation des pratiques de soins et de prévention (sans nom, sans NIR)	AUTORISATION ÉVALUATION	
	Programmes d'éducation thérapeutique	AUTORISATION	
	Programme d'apprentissage thérapeutique	AUTORISATION	
	Interconnexions	AUTORISATION	
	Traitement appelé à faire l'objet à bref délai d'un procédé d'anonymisation	AUTORISATION	

Vous pouvez retrouver ce tableau et ses mises à jour sur le site de la Cnil : www.cnil.fr

LÉGENDES :

NS : Norme Simplifiée. Si votre traitement correspond à une NS, vous n'avez qu'un engagement de conformité à effectuer en ligne sur le site internet de la CNIL : www.cnil.fr

DN : Déclaration Normale. Si votre traitement correspond à une DN, vous devez remplir en ligne le formulaire de déclaration normale.

AU : Autorisation Unique. Si votre traitement correspond à une AU, vous n'avez qu'un engagement de conformité à une autorisation unique à remplir. Cette procédure simplifiée se fait en ligne sur le site Internet de la CNIL.

MR-001 : Méthodologie de référence : si votre traitement entre dans le cadre de cette méthodologie, un simple engagement de conformité sur le site de la CNIL suffit.

AUTORISATION : Le formulaire et la procédure en ligne de demande d'autorisation sont disponibles sur le site de la CNIL.

AUTORISATION RECHERCHE MEDICALE : Le formulaire et la procédure en ligne de demande d'autorisation recherche sont disponibles sur le site de la CNIL.

AUTORISATION ÉVALUATION DES PRATIQUES DE SOINS : Le formulaire et la procédure en ligne de demande d'autorisation évaluation sont disponibles sur le site de la CNIL.

Soyez vigilant

Une procédure simplifiée ne vous dispense pas de connaître et de respecter la loi Informatique et Libertés. Vous devez lire les textes pour lesquels vous vous engagez : vous êtes le responsable du traitement. Tous les textes (normes simplifiées, autorisations uniques…) sont disponibles sur le site de la CNIL : www.cnil.fr

Lexique

Demande d'autorisation	Certains traitements du fait de la nature des données traitées ou de la finalité poursuivie relèvent de la procédure de l'autorisation. Ils sont définis à l'article 25 de la loi du 6 janvier 1978 modifiée : les traitements de données sensibles qui présentent un motif d'intérêt public (réseaux de santé, le DMP), les traitements mis en œuvre par des organismes privés qui comportent le numéro de sécurité sociale ou des données biométriques, les traitements portant sur des données génétiques, des données relatives aux infractions, condamnations ou mesures de sûreté, les traitements qui excluent les personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, les traitements ayant pour objet l'interconnexion de fichiers, les traitements comportant des appréciations sur les difficultés sociales des personnes.
Déclaration normale (DN)	C'est la procédure la plus courante, applicable à la majorité des traitements qui ne soulèvent pas de difficultés au regard de la protection des données.
Demande d'autorisation « recherche médicale » (DR)	Les traitements ayant pour fin la recherche dans le domaine de la santé sont soumis à une autorisation préalable de la CNIL spécifique (Article 53 de la loi du 6 janvier 1978 modifiée). Sont concernés les projets de recherche médicale qui nécessitent le recueil et la transmission à l'organisme de recherche de données directement ou indirectement identifiantes.
Demande d'autorisation « évaluation des pratiques de soins » (DE)	Les traitements de données de santé indirectement identifiantes (sans nom, prénom ou NIR), notamment issues des fichiers des professionnels de santé, des systèmes d'information hospitaliers (PMSI), ou des caisses de sécurité sociale, transmises et exploitées à des fins d'évaluation des pratiques de soins et de prévention doivent faire l'objet d'une autorisation préalable de la CNIL.
Dispense de déclaration	Décision de la CNIL (délibération) qui dispense un traitement courant de toutes formalités devant la CNIL (ex. : paie du personnel).
Données anonymes	Informations qui ne permettent pas d'identifier directement ou indirectement une personne physique même par regroupement.
Donnée à caractère personnel	Toute information reliée à une personne physique qui peut être identifiée, directement ou indirectement.

Donnée identifiante	Information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.
Données sensibles	Elles sont énumérées à l'article 8 de la loi du 6 janvier 1978 modifiée : origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci… Leur traitement est en principe interdit. Des dérogations existent.
Droit d'accès	Le droit d'accès vous permet de savoir si un fichier comporte des informations qui vous concernent, en contrôler leur exactitude et lorsque c'est nécessaire, les faire rectifier. En matière de santé, l'article L 1111-7 du code de la santé publique réaffirme le secret médical et le droit d'accès direct aux personnes sur les données les concernant (se référer à la fiche n°2 « Le droit d'accès au dossier médical »).
Droit d'opposition	Permet à un individu de s'opposer à ce que des informations le concernant fassent l'objet d'un traitement.
Fichier	Tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.
Finalité	Objectif du fichier. La ou les finalités doivent être déterminées, explicites et légitimes. Ex. : le traitement mis en place par un médecin peut avoir plusieurs finalités : gestion des RDV, gestion du dossier médical des patients, l'édition des feuilles de soins… Il ne doit pas servir à des fins commerciales.
Mentions d'information	Mentions indiquant le droit à l'information et le droit d'accès aux personnes concernées.

Méthodologie de référence	La méthodologie de référence est l'équivalent d'une autorisation unique, mais applicable aux traitements mis en œuvre dans le cadre de la demande d'autorisation « recherche médicale » (chapitre 9 de la loi). La CNIL a adopté une méthodologie de référence (MR-001), applicable aux traitements de données mis en œuvre dans le cadre de recherches biomédicales (exemples : recherche préalable à une autorisation de mise sur le marché d'un médicament, essai clinique).
Norme simplifiée (NS)	Norme pour une catégorie courante de traitement.
NIR	Numéro d'inscription au Répertoire national d'identification des personnes physiques ou numéro de sécurité sociale. Pour plus d'informations, se référer à la fiche n°3 « Numéro de Sécurité sociale ».
Responsable de traitement	L'autorité, l'organisme, le service qui détermine les finalités du traitement et les moyens (notamment informatiques) nécessaires à sa mise en œuvre (ex : le promoteur d'une recherche).
Sous traitant	Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. Le sous-traitant n'a pas de déclaration à faire à la CNIL.
Traitement automatisé de données personnelles	Toute opération informatisée (ou mécanographique) de collecte, enregistrement, organisation, conservation, modification, extraction, consultation, utilisation, communication, rapprochement, interconnexion, verrouillage, effacement, destruction.

Sigles

AFSSAPS : Agence française de sécurité sanitaire des produits de santé

ALD : Affection Longue Durée

ANAP : Agence nationale d'appui à la performance des établissements de santé et médico-sociaux

ANSSI : Agence nationale de la sécurité des systèmes d'information

ARS : Agence Régionale de Santé

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

CAH : Comité d'agrément des Hébergeurs de données de santé

CCAM : Classification commune des actes médicaux

CCMSA : Caisse Centrale de la Mutualité Sociale Agricole

CCTIRS : Comité Consultatif sur le Traitement de l'Information en matière de Recherche dans le domaine de la Santé

CETAF : Centre technique d'appui et de formation des Centres d'examens de santé

CépiDC : Centre d'Epidémiologie sur les Causes Médicales de Décès

CIM : Classification internationale des maladies de l'OMS

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

CNOM : Conseil National de l'Ordre des Médecins

CNOP : Conseil National de l'Ordre des Pharmaciens

CNR : Comité National des Registres

CPAM : Caisse primaire d'assurance maladie

CPP : Comité de Protection des Personnes

CPS : Carte de professionnel de santé

DMP : Dossier Médical Personnel

DP : Dossier Pharmaceutique

FOIN : Fonction d'occultation des informations nominatives

HAS : Haute Autorité de Santé

HCSP : Haut Conseil de la Santé Publique

IDS : Institut des Données de Santé (IDS)

INCa : Institut National du Cancer

INS : Identifiant National de Santé

Insee : Institut national de la statistique et des études économiques

INSERM : Institut national de la santé et de la recherche médicale

InVS : Institut de veille sanitaire

IRDES : Institut de Recherche et de Documentation en Economie de la Santé

MSA : Mutualité Sociale Agricole

NIR : Numéro d'inscription au Répertoire national d'identification des personnes physiques

ORS : Observatoire Régional de Santé

PMSI : Programme de médicalisation des systèmes d'information

PS : Professionnel de santé

RNIAM : Répertoire National Inter régimes de l'Assurance Maladie

RNIPP : Répertoire National d'Identification des Personnes Physiques

RPPS : Répertoire Partagé des Professionnels de Santé

SNIIRAM : Système National d'Information Interrégimes de l'Assurance Maladie

Une difficulté ? Une hésitation ?

Plus d'informations sur **www.cnil.fr,**

Une permanence de renseignements juridiques
par téléphone est assurée tous les jours
de 10h à 12h et de 14h à 16h
au **01 53 73 22 22**

Vous pouvez en outre adresser toute demande
par télécopie au **01 53 73 22 00**

Document Imprimé sur papier 100% recyclé

www.cnil.fr

8 rue Vivienne - CS 30223
75083 Paris cedex 02
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00