Plateformes et bases de données en lien avec le dossier médical. Enjeux de la collecte de données personnelles pour la recherche médicale

Sandra Franrenet
Doctorante en Ethique de la Recherche

Introduction

L'informatique est devenue en quelques années un outil incontournable lié à l'essor des nouvelles technologies de l'information et de la communication (NTIC). Les professionnels de la santé, après avoir mis un certain temps à s'équiper[1], tentent aujourd'hui de rattraper leur retard : à l'instar des autres acteurs de la société, ils se sont à leur tour lancés dans ce processus en informatisant les données personnelles de leurs patients qui sont définies par la loi comme « *toute 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* » [1]. Interrogé à ce sujet en fin d'année 2005, le Sénat considère que l'informatisation du secteur de santé constitue un enjeu d'autant plus important qu'il devrait permettre « *d'améliorer l'exercice de la médecine par les professionnels de santé en leur apportant (…) un accès à des connaissances médicales validées (…)* » [2]. Désormais stockées sur un support facilement exportable, ces informations ont rapidement fait l'objet de mesures de protection législatives, censées réguler leur traitement ainsi que leur circulation. Parmi les principaux textes figure ainsi la loi du 6 janvier 1978 [1] relative à l'informatique, aux fichiers et aux libertés, ultérieurement modifiée à plusieurs reprises. Réglementée de manière complète et détaillée, l'informatisation offre aujourd'hui de nouvelles opportunités, en particulier pour la recherche. La Commission nationale de l'informatique et des libertés (CNIL) considère à ce titre que « *au sens de l'article 5 de la convention n° 108 du conseil de l'Europe, le traitement de données de santé à caractère personnel est légitime dès lors qu'il a pour finalités de permettre au professionnel de santé de mieux assurer le suivi médical des patients, de faciliter leur prise en charge par les organismes d'assurance maladie obligatoire, de participer aux actions de prévention et de veille sanitaire poursuivies par les autorités de santé et de contribuer aux travaux de recherche médicale* » [3]. L'incursion du monde de la recherche dans celui du soin constitue cependant un élément à double « tranchant » : s'il peut en effet se révéler très bénéfique à la fois sur les plans micro (le patient) et macro (la société), il pose en même temps certaines interrogations sur le plan de l'éthique. En effet, lorsqu'elles sont conservées dans leur dossier médical, les données médicales personnelles bénéficient du sceau du secret médical, garant de leur confidentialité. Transmises puis traitées pour la recherche, elles perdent *de facto* ce cadre privilégié pour se retrouver sur des plateformes ou bases de données informatiques.
Le présent dossier propose de faire un point sur cette situation en rappelant dans un premier temps le contenu de la réglementation relative à la collecte de données médicales personnelles puis en déterminant, dans un second, ses enjeux pour la recherche médicale

[1] Selon un rapport réalisé par le Sénat en novembre 2005 [2] seuls 30% des hôpitaux publics disposaient d'un système d'information réellement efficace à cette date et 20 à 25% d'un dossier patient électronique.

Réglementation relative à la collecte de données médicales personnelles pour la recherche

Compte tenu de leur caractère particulièrement sensible, les données médicales personnelles répondent à une législation très précise et très encadrée, a fortiori lorsqu'elles sont utilisées dans le cadre de la recherche.

o Particularité des données médicales personnelles

Comme l'affirme la Commission nationale de l'informatique et des libertés (CNIL) depuis une recommandation du 4 février 1997 [3], **les données de santé ne sont pas des informations comme les autres**. Revêtant un caractère directement ou indirectement nominatif dont le contenu relève de la vie privée, elles appartiennent désormais[2] à la **catégorie des données dites « sensibles »**, au même titre que celles qui font apparaître « *directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicales des personnes, ou qui sont relatives (…) à la vie sexuelle de celles-ci.* » Cette particularité, associée au développement rapide de l'informatique qui facilite leur dissémination, explique que le législateur leur confère une **protection accrue**. L'article 1er de la loi du 6 janvier 1978 modifiée [1] énonce à ce titre que l'informatique « *ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* » Néanmoins, « *nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé* » pour la recherche (article 55).

o Collecte des données

La collecte de données médicales personnelles appartient à un processus plus vaste dénommée « **traitement** ». Ce processus défini par l'article 2 de la loi du 6 janvier 1978 modifiée, concerne « *toute opération ou tout ensemble d'opérations portant sur de telles données (…) et notamment* (outre la collecte citée), *l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.* » Comme cela a été énoncé SUPRA, la CNIL considère que lorsqu'il a pour finalité de contribuer « *aux travaux de la recherche médicale* », ce traitement est « *légitime* » [3], mais suppose -lorsque les projets concernés nécessitent le recueil et la transmission à l'organisme de recherche de données directement ou indirectement nominatives et le recours à des moyens organisés- l'accomplissement de **formalités préalables** garantes de la protection des personnes.

[2] L'assimilation des données de santé aux données dites sensibles date de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. JO n° L 281 du 23 novembre 1995 pages 31 – 50. Cette directive a été intégrée en droit français par la loi modifiée du 6 janvier 1978 modifiée (article 8).

- **Formalités préalables**

Les formalités prévues par le législateur diffèrent selon que les données **médicales collectées à des fins de recherche permettent ou non une** identification directe des personnes. **Dans le premier cas**, les responsables de la recherche doivent respecter une **procédure en deux temps** garantissant une protection renforcée des individus concernés. Il leur est demandé d'effectuer une demande d'avis auprès du comité consultatif de la CNIL puis une demande d'autorisation auprès de la Commission. Dans le second cas, les responsables sont soumis à une **procédure simplifiée** homologuée et publiée par la CNIL [4]. L'organisme concerné n'a dans ce cas qu'à adresser à la Commission un engagement de conformité à la méthodologie de référence

- **Transmission des données nominatives**

Une fois la demande de traitement acceptée par la CNIL, les professionnels de santé sont autorisés à colleter puis transmettre au responsable de la recherche les données nominatives qu'ils détiennent dans le cadre d'un traitement automatisé. Si ces données permettent l'identification des personnes, elles doivent, sauf exception[3], être **codées** avant leur transmission. Le responsable doit ensuite veiller à leur **sécurité** et à leur **traitement**, ainsi qu'au **respect de la finalité de celui-ci** (article 55 de la loi du 6 janvier 1978 modifiée). La loi précise par ailleurs que les personnes appelées à mettre en œuvre ledit traitement ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au **secret professionnel**.

Enjeux relatifs à la collecte de données médicales personnelles pour la recherche

La collecte de données médicales personnelles pour la recherche se trouve facilitée lorsque ces données sont directement exportées du dossier patient vers des plateformes informatisées. Les chercheurs en contact avec ces informations peuvent ainsi bénéficier d'une fantastique base qui devrait permettre d'améliorer plus simplement, plus rapidement et à moindre coût les connaissances médicales. Mais si l'amélioration des connaissances constitue bien un enjeu fondamental pour la recherche, les chercheurs doivent en contrepartie faire face à d'autres types d'enjeux, tels que rassurer les individus sur l'utilisation et la sécurisation de leurs données ou encore leur délivrer une information claire, loyale et appropriée qui leur permettent de pouvoir pleinement consentir aux utilisations prévues.

- **Améliorer les connaissances médicales**

Les données médicales sur lesquelles les chercheurs ont l'habitude de travailler sont traditionnellement collectées dans le cadre de protocoles spécifiques (recherche sur des malades atteints de cancer ou par le VIH par exemple). Il résulte de cette manière de procéder une homogénéisation des informations capitalisées puisqu'elles proviennent d'un nombre généralement restreint de patients ayant des profils similaires (mêmes symptômes, mêmes diagnostics, mêmes traitements). Pour bénéficier de données hétérogènes, les

[3] Il peut être dérogé à l'obligation de coder les données lorsque leur traitement est associé à des études de pharmacovigilance ou a des recherches réalisées dans le cadre d'études coopératives nationales ou internationales ou encore si une particularité de la recherche l'exige (art. 55 de la loi du 6 janvier 1978 modifiée).

scientifiques doivent donc multiplier les protocoles de recherche, démarche qui les oblige à trouver des budgets ainsi que du temps pour recruter les participants.

Le recours à des plateformes de données

L'informatisation des données médicales personnelles offre un moyen de potentialiser les recherches en facilitant notamment le travail de collecte : en accédant à des plateformes informatiques en lien direct avec les dossiers médicaux d'un nombre considérable de patients, les chercheurs peuvent ainsi bénéficier d'une formidable base de données à moindre frais et en un temps record [5]. Le recours à ces informations constitue un enjeu fondamental pour la recherche puisqu'il permet d'améliorer les connaissances dans le domaine de nombreuses maladies et, *in fine* de mettre au point des thérapies effectives ainsi que des stratégies de prévention adaptées [6].

L'accès aux données

Mais pour travailler à partir de ces bases de données, encore faut-il que les chercheurs puissent y avoir accès. Or, l'article 45 du décret du 6 septembre 1995 portant code de déontologie médical énonce que les dossiers médicaux doivent être conservés sous la responsabilité des médecins qui assurent leur suivi. Cette mesure de sécurité résulte de la nature des données contenues. La particularité de ces informations, dites sensibles, et à ce titre protégées par le secret médical, explique par ailleurs que certains patients soient réticents à leur utilisation en dehors du cadre du colloque singulier par des individus que la loi appelle les « destinataires du traitement », c'est-à-dire « *toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.* »

La question à se poser en l'espèce est donc la suivante : qui doit précisément accéder à ces données ? Une étude menée récemment au Canada [7] propose, pour y répondre, d'établir un protocole précis qui détermine les personnes pouvant/devant avoir accès au dossier médical pour la recherche. Egalement intéressé par ce sujet, le Laboratoire d'éthique médicale et de médecine Légale (LEM)[4] de l'Université Paris Descartes a récemment interrogé une trentaine de patients pour savoir qui devrait, selon eux, consulter leur dossier dans le cadre de la recherche. Deux propositions leur ont été successivement faites : les médecins en charge de la recherche et/ou les chercheurs non médecins. Allant ensuite plus loin, le LEM a souhaité savoir si, toujours selon les patients interrogés, toutes les données contenues dans leur dossier médical devaient être accessibles pour la recherche ou au contraire si certaines devraient rester entre les mains des médecins qui les soignent. L'analyse (en cours) des entretiens semi-directifs permettra de mieux comprendre les attentes de ces personnes et ainsi déterminer un protocole adapté sur la manière de les recueillir et surtout de les exploiter. A défaut de réflexion sur ce sujet, les patients risquent d'exercer de manière récurrente leur droit d'opposition (Cf. INFRA), et ce même s'il est d'un usage plus limité lorsqu'il est associé à la recherche[5]. Pour l'heure, et dans le but d'éviter une telle défiance, il apparaît indispensable de

[4] Le LEM est l'un des principaux partenaires de ce projet dénommé INFORARE et financé par l'Agence Nationale de la Recherche (ANR) cité INFRA. Pour plus d'informations à ce sujet : www.ethique.inserm.fr.

[5] Selon l'article 56 de la loi du 6 janvier 1978 modifiée, pour que le droit d'opposition puisse être exercé dans ce cadre précis, il faut que les données fassent préalablement l'objet d'une levée du secret professionnel rendue nécessaire par le traitement

rassurer les patients quant à l'utilisation de leurs données et des procédures de sécurisation afférente.

- **Rassurer les individus sur l'utilisation de leurs données et leur sécurisation**

La collecte et l'utilisation des données médicales personnelles identifiantes peut, en soi, constituer une réelle source d'angoisse pour les individus concernés. Cette angoisse peut par ailleurs se trouver renforcée si lesdites données sont utilisées dans le cadre de recherche et transitent par des plateformes ou bases de données informatiques.

Se prononçant sur cette question dans un avis relatif aux problèmes éthiques rencontrés par l'informatisation de la prescription hospitalière et du dossier du patient [8], le Comité Consultatif National d'Ethique (CCNE) rappelle que « *l'histoire de l'informatique atteste qu'en dépit des précautions prises par les concepteurs de programmes, des possibilités de subtilisation de données confidentielles existent. De façon générale, le sentiment que plus les données sont numérisées, plus elles sont facilement exploitables par des tiers (sinon des organismes de contrôle) n'est pas dépourvu de fondement.* » Certaines études [9] sont venues préciser que les angoisses les plus récurrentes concernent le mésusage des données par des pirates informatiques *(hackers)*. Ces inquiétudes, par ailleurs consolidées par un certain battage médiatique, renforcent la croyance générale selon laquelle les supports informatisés ne sont pas suffisamment sécurisés, et *de facto* la peur que les données médicales puissent tomber entre les mains d'employeurs, de compagnies d'assurance [6] ou de tout autre type d'interlocuteur qui ne devraient absolument pas y avoir accès.

Le mésusage des données

Parmi ces « autres interlocuteurs » figurent de nombreuses entreprises commerciales ayant une activité médicale, comme CEDEGIM pour ne citer qu'elle. Société privée fournissant des logiciels de médecine générale, « *elle s'est fait une spécialité d'informatiser plus ou moins gratuitement les cabinets médicaux, en échange d'un accès anonymisé nocturne aux bases de données tirées directement des dossiers médicaux des patients Son activité de base est la collecte des données médicales, grâce à un réseau de communication interactive avec les médecins, reposant sur les réseaux Thalès et Heraclès dont elle est propriétaire. Elle revend ensuite ces données sous forme de statistiques aux laboratoires. (…°). Ce n'est pas le seul exemple puisque la société IMS Health, organisme implanté au niveau international, réalise également des études sur les consommations médicales à la demande principalement des laboratoires. Grâce à un module implanté dans un certain nombre de logiciels (…), elle réceptionne les résumés de chaque consultation médicale. Elle a ainsi accès aux pathologies codées, aux dates et aux motifs d'arrêts en longue maladie (ALD), à l'ordonnance, mais aussi à des renseignements permettant une réidentification facile comme le numéro national du médecin traitant ainsi que la date de naissance, le sexe et le régime du patient. Il s'agit donc d'un simulacre d'anonymisation.* » [10]. Pourtant, comme le constate le Conseil de l'ordre dans un rapport réalisé en juin 2000 [11], « *il serait vain de combattre une tendance aussi irréversible que celle de la commercialisation des données personnelles et de l'interdire d'une manière globale et définitive »* et de recommander d'imposer des règles précises *« qui permettent* ***d'obtenir des données statistiques agréées à un niveau suffisant pour qu'elles perdent leur caractère de données personnelles et puissent devenir dans certains cas des données publiques commercialisables*** *comme le sont les fichier de certaines administrations,*

au risque que certains patients refusent à leurs médecins de communiquer des informations qui les concernent. (…). »

Cet extrait permet de rebondir sur un élément très important : le lien de confiance unissant les patients à leur médecin Il ressort ainsi d'une étude canadienne rendue publique en mars 2008 [12] que la relation unissant le malade à son praticien n'est qu'exceptionnellement emprunte de défiance puisque, sur les 2392 personnes interrogées, seuls 4% pense que leur médecin a pu communiquer certaines de leurs données médicales sans les informer ni leur demander de consentir ; ce chiffre tombe à 3% lorsqu'il s'agit de l'hôpital ou la clinique dans lequel ils ont reçu des soins. Les enquêteurs ont également demandé aux participants si, à leur connaissance, certaines de leurs données médicales identifiantes ou concernant leur santé utilisées dans le cadre d'une recherche donnée avaient pu être communiquées à d'autres personnes que celles appartenant à l'équipe de la recherche. Là encore, seuls 2% ont répondu par l'affirmative, mais 38% n'ont pas été capables de répondre. Ensuite interrogés sur leur réaction en cas de communication « impropre » de leurs données (sans information ni consentement), 77% ont répondu qu'ils se sentiraient trahis par les chercheurs. Ce sentiment de trahison est évidemment très néfaste pour la recherche et donc pour l'amélioration des connaissances en général.

La sécurisation des données

Pour rassurer les individus quant au risque de mésusage de leurs données médicales personnelles identifiantes, il est impératif que les destinataires (les chercheurs en l'espèce) leur apportent des garanties portant « *non seulement sur la fiabilité intrinsèque du système, c'est-à-dire sa capacité pour satisfaire de manière reproductible à ses objectifs et à ses fonctions, mais aussi sur la sécurité de son emploi dans l'environnement médical, administratif et informatique où il sera mis en œuvre. Sécuriser un système d'informations requiert une analyse des nombreux risques auxquels il est exposé et le choix de solutions organisationnelles ou techniques qui permettent d'assurer sa confidentialité, son intégrité et sa disponibilité* » [13]. Respectivement coordinateur et partenaire du projet INFORARE[6], le Laboratoire de Biostatistique et d'Informatique Médicale de la faculté de médecine de Dijon et la start-up HC Forum® sont en train de développer une plateforme informatique hautement sécurisée visant à organiser le partage d'information entre la partie soin et la partie clinique qui permet notamment aux chercheurs d'effectuer des études génétiques à partir des informations contenues dans leur dossier. Pour assurer la sécurité du système, le projet repose sur une technique de hachage à sens unique permettant de rendre les données des patients anonymes en transformant de manière irréversible les variables d'identification. Cette procédure est par ailleurs couplée avec le Standard Hash Algorithm (SHA), algorithme du domaine public le plus sûr vis-à-vis des tentatives de déchiffrement, également appelées « attaque par dictionnaire ». Nonobstant la performance de ce système de sécurisation des données, il ne paraît néanmoins pas possible de garantir qu'il est absolument protégé contre tout risque d'attaque. Aucun système informatique ne peut à ce jour tenir d'un tel discours. Aussi, pour pallier cela, il est non seulement impératif de délivrer une information claire, loyale et appropriée sur l'usage qui sera fait des données et des moyens de sécurisation mis en place, mais aussi de mentionner les droits et recours en cas de mésusage avéré.

[6] Cf. note de bas de page n°4.

- **Délivrer une information claire, loyale et appropriée**

Tant d'un point de vue éthique que juridique, il est essentiel que les personnes dont les données personnelles sont collectées puissent consentir à ce qu'elles soient utilisées dans le cadre de la recherche. Ce consentement ne revêt cependant de valeur que s'il est « éclairé », c'est-à-dire donné après la délivrance d'une information claire, loyale et appropriée qui permette au participant de bien distinguer son parcours de soin de celui de la recherche.

Distinguer le soin de la recherche

L'utilisation de données médicales personnelles pour la recherche peut être à l'origine de confusion pour les patients qui peuvent alors croire que ces dernières sont en fait utilisées dans le cadre de leur parcours de soin. Cette confusion, appelée « *Therapeutic Misconception* » par les anglo-saxons, a été décrite en 1982 par le Pr. Appelbaum et collaborateurs [14]. Etudiée depuis par de nombreux auteurs, cette notion peut être définie comme un événement survenant lorsque les participants ne comprennent pas qu'ils participent à une recherche ayant pour but de produire des connaissances généralisables, mais pensent au contraire qu'ils participent à un protocole dont ils pourront tirer bénéfice pour leur santé [15]. Il est donc évident que les personnes placées dans une telle situation ne pourront inévitablement pas comprendre la plupart des conséquences de leur décision [16]. Le développement des dossiers médicaux informatisés ne va, quant à lui, pas arranger cette situation, mais au contraire renforcer le flou existant entre recherche et soin. Une étude menée en 2005 a ainsi montré que beaucoup de patients ignoraient totalement que leurs données médicales personnelles informatisées pouvaient être utilisées dans le cadre de la recherche, et ce malgré l'existence d'une notice d'information affichée dans la salle d'attente du cabinet [17]. Aussi, pour éviter aux patients de faire la confusion, Lidz et Appelbaum [16] proposent de mettre le focus sur la distinction entre soin et recherche et sur les raisons qui expliquent pourquoi les deux sont différents. A défaut, les participants ne seront pas en mesure de donner un consentement éclairé.

La nature du consentement éclairé

Le consentement constitue une phase préliminaire de la recherche qui a fait l'objet de plusieurs tentatives de définition. Mais que recouvre t-il exactement si ce n'est, a priori, l'expression de l'accord d'un individu face à une action proposée ? [18] Réfléchissant à cette étape-clé, Eike-Henner W. Kluge (département de philosophie de l'Université de Victoria au Canada) considère que le consentement n'est pas en soi un « état » mais au contraire un « processus » dynamique qui comporte plusieurs critères [19]. Parmi ceux-ci, la signature donnée par le participant pour confirmer son adhésion à la recherche est considéré comme étant le moins important. Lui donner la possibilité de choisir –participer ou ne pas participer- est en revanche jugé beaucoup plus intéressant sur le plan de l'éthique [19]. Est-ce à dire cependant qu'il faut rechercher son consentement à chaque fois que les chercheurs ont besoin d'utiliser ses données ? Si l'on s'appuie sur le Code International d'Ethique Médicale de l'Association Médicale Mondiale (AMM) [20], les individus concernés par un dossier médical électronique devraient être tenus informés de l'existence de systèmes, programmes ou dispositifs de collecte et/ou de la communication de données à leur sujet, et à ce titre donner un consentement éclairé avant la construction dudit dossier ainsi que lors de l'utilisation, du stockage, de la communication, de la manipulation et du traitement des données contenues.

En France, la loi exige que le consentement des personnes dont les informations médicales sont collectées soit recueilli puisqu'elles appartiennent à la catégorie des données dites « sensibles ». Cette décision implique que les chercheurs qui souhaitent utiliser les informations contenues dans le dossier médical, pour un protocole précis, doivent au préalable demander l'autorisation des personnes concernées (sauf s'ils sont dans l'impossibilité de les retrouver).
Pour contourner cette obligation, certains professionnels exerçant Outre-Atlantique optent pour un système appelé « blanket consent », autrement dit consentement blanc, qui consiste à demander aux participants un consentement global en début de recherche qui, *de facto*, les autorise à utiliser les données pour tout type de recherche englobée dans le protocole. Cette façon de procéder n'est cependant pas nécessairement toujours appréciée par les participants. L'étude nationale canadienne mentionnée SUPRA [12] a ainsi montré que seul 1% des personnes interrogées étaient d'accord pour que leurs données soient utilisées par les chercheurs sans consentement contre 38% qui souhaitaient donner un consentement pour chaque utilisation. De même, un projet mené récemment en Nouvelle-Zélande a montré que seuls 20% des patients hospitalisés pour des soins cliniques primaires étaient d'accord pour partager leurs données (non anonymisées) avec des chercheurs alors que ce chiffre passait à 55% si ces derniers leur en demandaient l'autorisation [21]. Réfléchissant à partir d'un autre angle de vue, Eike-Henner W. Kluge [19] estime pour sa part que les données contenues dans un dossier médical électronique peuvent être accessibles et traitées sans passer préalablement par le consentement informé tant que les données sont anonymisées et utilisées dans une forme statistique et que les personnes qui y ont accès sont des représentant dûment accrédités par les responsables de la recherche. S'appuyant sur une étude réalisée en 2004 par Coiera et Clarke [22] qui a permis d'identifier quatre formes de consentement (*General consent*, *General consent with specific denial*, *General denial with specific consent*, et *General denial*) Kulynych et Korn [6] ont à leur tour proposé un modèle hybride dans lequel la manière dont le consentement obtenu varie selon l'utilisation qui est faite des données. Ce modèle implique d'intégrer des mécanismes à la fois flexibles et sophistiqués, tel que l'*e-consentement*, dans les futurs systèmes d'information afin qu'ils puissent être adaptés pour répondre aux préférences des patients. Nonobstant le système retenu, il est impératif qu'il soit accompagné d'une information adaptée répondant aux principes de l'éthique médicale.

Le contenu de l'information délivrée
L'article 57 de la loi du 6 janvier 1978 modifiée énonce que « *les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :*

1° De la nature des informations transmises ;
2° De la finalité du traitement de données ;
3° Des personnes physiques ou morales destinataires des données ;
4° Du droit d'accès et de rectification institué aux articles 39 et 40 ;
5° Du droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement[7]. »

[7] Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.

Ces informations sont techniquement délivrées par voie d'affichage ou remises en main propre aux personnes concernées. Dans le cas cependant où les données personnelles ont été initialement recueillies pour un autre objet que le traitement -comme c'est le cas lorsqu'elles ont été collectées pour être enregistrées dans le dossier médical et qu'elles sont ensuite utilisées dans le cadre de la recherche- « *il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées. Les dérogations à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point.* »

Plusieurs études menées de l'autre côté de l'Atlantique pour évaluer l'opinion publique en matière d'information relative à l'utilisation des données médicales personnelles pour la recherche ont montré que les participants sont plutôt enclin à accepter le principe, à condition néanmoins d'en être au moins tenu informé (à défaut de donner un consentement). Illustrant ce constat, le projet canadien mentionné SUPRA [7] a clairement mis en exergue que, si peu de répondants sont totalement opposés à l'utilisation de leurs données personnelles pour la recherche (4%), la majorité d'entre eux semble cependant vouloir garder un certain niveau de contrôle sur leur utilisation. Pour cela, encore faut-il qu'ils reçoivent régulièrement une information de la part de l'équipe de recherche. Le CCNE énonce à ce titre que « *l'adhésion des patients à la proposition d'une nouvelle forme de prise en charge (qu'elle soit ou non informatisée) est largement tributaire du contenu de l'information qui leur aura été communiquée. Par exemple, si une information transmise au patient porte uniquement sur quelques risques mineurs et avérés, il est clair qu'elle n'aura pas le même retentissement émotionnel que si elle inclut aussi les risques potentiels. Par exemple, le risque d'une panne d'électricité pourrait être signalé (en même temps que les mesures de sécurité qui sont prises pour y remédier) si le service a déjà eu l'occasion de pâtir d'un tel dysfonctionnement. En revanche, la panne de secteur généralisée qui entraînerait la perte des données sauvegardées dans un établissement de santé voisin constitue un risque purement potentiel qu'il ne semble pas opportun de spécifier au patient* » [8]. Cet avis montre qu'en dehors de l'information « légale » qui doit être obligatoirement donnée à chaque patient dont les données sont utilisées pour la recherche, il est important d'adapter le contenu du message en fonction des profils des personnes et des particularités de chaque protocole. Un mémoire de recherche de Master 2 réalisé pour le compte du laboratoire d'éthique médicale a d'ailleurs montré que « *seule une communication « holistique » et donc non standardisée peut (…) répondre au principe éthique du respect du participant qui consiste à lui transmettre une information selon un processus qui lui convient* » [23].

Conclusion

La collecte de données médicales personnelles pour la recherche est un processus qui devrait être facilité, dans les années à venir, avec l'instauration du dossier médical personnel (DMP). « *Institué par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, c'est en quelque sorte un porte-documents* (informatique) *contenant : **des données générales** (antécédents médicaux et chirurgicaux, l'historique des consultations, les vaccinations, les allergies etc.), **des données de soins** (résultats d'analyses, les comptes rendus médicaux, les dispensations médicamenteuses, etc.), **des données de prévention** (les facteurs de risques*

individuels, etc.), ***des données image*** *(radios, scanners, etc.),* ***un espace d'expression personnelle*** *permettant de porter des informations personnelles à la connaissance des professionnels de santé (position sur le don d'organes, par ex.)* (ainsi que) *les éléments du dossier pharmaceutique (DP)* » [24]. Actuellement à un stade encore embryonnaire compte tenu des obstacles techniques qu'il reste à résoudre avant sa mise en place, le DMP finira tôt ou tard par voir le jour. L'accélération de l'informatisation des données, qu'elles soient médicales ou non, constitue donc une tendance irréversible à laquelle acteurs et citoyens doivent dès à présent se préparer. Et parmi les nombreuses difficultés qu'il reste à prendre en compte, il semble que, pour l'heure, le principal défi consiste à trouver un équilibre solide entre la protection des données médicales personnelles des individus d'une part, et la nécessité d'améliorer la qualité des soins et les connaissances médicales via la recherche d'autre part [5].

Bibliographie

[1] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF du 7 janvier 1978. Page 227. Version consolidée au 22 décembre 2007.
[2] Sénat, Rapport d'information n° 62 sur l'informatisation dans le secteur de la santé. Session ordinaire 2005-2006.
[3] CNIL, Délibération n°97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. JO du 12 avril 1997. www.cnil.fr
[4] Renseignements pratiques sur les formalités préalables à la création d'un fichier de recherche médicale. Edition août 2007. www.cnil.fr
[5] Norman M. Bradburn, Medical Privacy and Research, The Journal of Legal Studies, Vol. 30, No. 2, The Regulation of Managed Care Organizations and the Doctor-Patient Relationship, (Jun., 2001), pp. 687-701.
[6] Kulynych J., Korn D, The Effect of the New Federal Medical-Privacy Rule on Research, The new England Journal of Medecine, Volume 346:201-204, January 17 2002, Number 3.
[7] Willison J, Schwartz L, Abelson J, Charles C, Swinton M, Northrup D, Thabane L, Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?, J Am Med Inform Assoc. 2007;14:706 –712. DOI 10.1197/jamia.M2457.
[8] CCNE, Avis n°91 sur les problèmes éthiques rencontrés par l'informatisation de la prescription hospitalière et du dossier du patient, 16 février 2006.
[9] Chhanabhai P., Consumers Are Ready to Accept the Transition to Online and Electronic Records If They Can Be Assured of the Security Measures, MedGenMed. 2007; 9(1): 8. Published online 2007 January 11
[10] Picard S., Pellet J., Brulet JF., Trombert B., Les aspects juridiques et éthiques de la protection des données issues du dossier médical informatisé et utilisées en épidémiologie: un point de la situation, Santé publique 2006, volume 18, n°1, pp. 107-117.
[11] « La commercialisation des informations médicales est-elle déontologiquement correcte ? » Rapport adopté par le Conseil national de l'Ordre des médecins lors de la session des 29 et 30 juin 2000.
[12] How the Public Views Privacy and Health Research, Results of a National Survey Commissioned by the Institute of Medecine Committee on "Health Research and the Privacy of Health Information : The HIPAA Rule". Original Report – November 2007: Revised and expanded – March 2008.
[13] Allaert FA, Dusserre L, Leclercq B, La sécurité des systèmes d'information médico-hospitaliers, Informatique et Santé, 1997 (9) : 149-157.
[14] Appelbaum PS, Roth LH, Lidz C, 1982, The Therapeutic Misconception: Informed Consent in psychiatric Research. Int. J. Law Psychiatry 5:319–329.
[15] Henderson G, Churchill L, Davis A, Easter M, Grady C, Joffe S, Kass N, King N, Lidz C, Miller F, Nelson D, Peppercorn J, Bluestone Rothschild B, Sankar P, Wilfond B, Zimmer C, Clinical Trials and Medical Care: Defining the Therapeutic Misconception, Plos Medecine, November 007, Volume 4, Issue 11, e324.
[16] Lidz W, Appelbaum P, The therapeutic Misconception : Problems and Solutions, Medical Care 2002, Volume 40, Number 9, Supplement, pp 55-63.
[17] Willison D, Keshavjee K, Nair K, Goldsmith C, Holbrook A, Patient consent preferences for research uses of information in electronic medical records : interviews and survey data. BMJ, Volume 326, 15 February 2003.

[18] Singleton P, Wadworth M, Consent for the use of personal medical data in research, BMJ 2006;333;255-258.
[19] Eike-Henner W. Kluge, Informed consent and the security of the electronic health record (EHR): some policy considerations, International Journal of Medical Informatics (2004) 73, 229—234.
[20] IMIA Code of Ethics for Health Information Professionals, 2002, http//:www.imia.org.
[21] Whiddett R, Hunter I, Engelbrecht J, Handy J. Patients' attitudes towards sharing their health information. Int J Med Inform. 2006;75:530–41.
[22] Coira E, Clarke R, e-Consent- the design and implementation of consumer consent mechanisms in an electronic environment, J. Am. Inf. Assoc. 11 (4), 2004, 129-140.
[23] Franrenet S, Regard des associations de patients sur le processus d'information dans la recherche biomédicale. Mémoire de Master 2 de recherche en éthique médicale. Paris Descartes. 2007. www.ethique.inserm.fr.
[24] Grivel P, Le Dossier Médical Personnel (DMP) : un dossier mal programmé.