http://www.ldh-france.org/
ldh@ldh-france.org

Droits Et Libertés face à l'Informatisation de la Société

http://www.delis.sgdg.org
contact@delis.sgdg.org

Audition du 24 janvier 2007 par la CNIL

Pour un identifiant santé qui préserve la protection absolue des données personnelles de santé

Contact : Ligue des Droits de l'Homme – 138 rue Marcadet 75018 Paris – Tél. 01 56 55 51 00

http://www.ldh-france.org/
ldh@ldh-france.org

Droits Et Libertés face à l'Informatisation de la Société
http://www.delis.sgdg.org
contact@delis.sgdg.org

Audition du 24 janvier 2007 par la CNIL

Pour un identifiant santé qui préserve la protection absolue des données personnelles de santé

Plan de l'argumentaire :
> Points de convergence entre l'ensemble des acteurs.
> Pourquoi le NIR ne peut être l'identifiant santé ?
> Qualités attendues d'un identifiant santé (NIS) et existence de solutions techniques répondant aux critères retenus.
> Réponses aux principales objections concernant le choix d'un NIS distinct du NIR.

1) Points de convergence entre l'ensemble des acteurs

Les données de santé sont parmi les plus sensibles (accès au travail, assurances, insertion sociale, secret professionnel,…) et les plus intimes (intériorisation, sentiment d'appartenance…) pour une personne.
Pour une très grande proportion des patients et pour l'ensemble des professionnels de santé, il faut que leur confiance soit totale dans la protection de la confidentialité des données stockées dans les dispositifs DMP et dans les autres dossiers de santé informatisés.
Pour une bonne gestion, il y a besoin d'un identifiant santé totalement fiable (assurant l'identification des données de santé de façon univoque pour une personne donnée).
Il s'agit donc de disposer d'un identifiant fiable dans le strict périmètre de la sphère des soins de santé, et lui seul.

2) Pourquoi le NIR ne peut être l'identifiant santé ?

*** Du point de vue du NIR :**

- L'énumération de l'ensemble des utilisations actuelles du NIR[1] illustre sa diffusion (au demeurant déjà trop large) dans plusieurs secteurs. Nous soutenons la demande du Collectif interassociatif sur la santé (CISS) adressée à la CNIL d'en faire un listing exhaustif actualisé. Le NIR est donc dans la main de divers acteurs (employeurs, assureurs santé, fisc…), directement et/ou potentiellement intéressés à connaître l'état de santé des personnes.
- Le NIR est un outil très fiable, voire le plus fiable, pour réaliser les rapprochements de données et interconnexions de fichiers, même si d'autres outils existent pour le faire.
- Le NIR est signifiant et facilite les tris de populations directs sur critère (fichiers de populations qui seront constitués avec les DMP de 60 millions de personnes stockés chez 3 ou 4 hébergeurs).

[1] Le secteur de la protection sociale au sens large : sécurité sociale dans toutes ses branches (santé, vieillesse, famille), organismes de prévoyance (CAF, organismes d'assurance maladie complémentaires, mutuelles), les organismes d'aide sociale (comme ceux gérant le RMI par ex. ou les ASSEDIC, l'ANPE) ; les employeurs du secteur public et privé dans le cadre de leurs relations avec la sécurité sociale uniquement (ils ne l'utilisent pas pour la gestion générale du personnel) ; les établissements de santé qui cependant ne l'utilisent pas pour gérer les dossiers médicaux ; L'INSEE, gestionnaire du RNIPP, donc du NIR, avec en particulier le fichier national électoral ; la sphère fiscale avec des conditions très restrictives ; les cas où la CNIL a autorisé de façon très ponctuelle la consultation du RNIPP ; ...

*** Du point de vue des données de santé :**

- Les données de santé sont parmi les plus sensibles et les plus intimes d'une personne (*« L'information médicale (...) est le sanctuaire de l'intimité la plus profonde de la personne humaine »*, Louise Cadoux, Sophie Vuillet Tavernier - CNIL 1998).
- Le secret médical est un élément fondamental de l'organisation de nos sociétés.
- La nécessité de partager certaines informations médicales entre professionnels de santé, dans le cadre de la coordination des soins, requiert l'accord du patient (rôle actif et éclairé des individus), et ne doit en aucune façon faire peser le moindre risque de rupture du secret médical qui couvre ces informations à l'égard de tiers, notamment de tout acteur extérieur à la sphère des soins (la déontologie professionnelle ne doit pas être mise en cause par un process technique).
- Le DMP et les autres dossiers médicaux informatisés, chez le médecin de ville, à l'hôpital, dans le cadre de réseaux (cancérologie, diabétologie…), doivent (pour être effectivement utiles au patient) et vont constituer une base de données personnelles de santé, sinon exhaustive, en tout cas très étendue pour chaque patient quant à son histoire de santé, stockées ad vitam aeternam (c'est l'objet même du DMP). De plus avec le DMP, on se trouvera en présence de véritables fichiers de santé de population avec le regroupement chez un nombre très restreint d'hébergeurs.
- On change de dimension (en changeant de quantitatif, on change de qualitatif) par rapport aux données de facturation qui seront certes de plus en plus médicalisées (avec les actes, les diagnostics dans le cadre de la T2A et de la médecine de ville), mais d'une part conservées dans plusieurs centaines de centres CPAM, donc largement réparties, et d'autre part pour la durée limitée aux contraintes de gestion de la facturation (les informations stockées concernent la prise en charge d'une année donnée et sont détruites 5 ans après la date de la prise en charge), cf. ci-après point 4) objection n°1.
- La sécurisation des flux et du stockage, ainsi que des accès à l'information personnelle de santé est régulièrement mise en défaut, ce qui n'est déjà pas acceptable dans le cadre des données de facturation, et a fortiori pour le DMP et les dossiers médicaux informatisés à vocation exhaustive.

➔ le NIR, outil très fiable pour les interconnections, est donc déjà disséminé dans divers secteurs d'activité, et son adoption comme identifiant santé ne peut garantir les deux critères que doit remplir un NIS qui seront exposés ci-après en 3).

3) Qualités attendues d'un identifiant santé (NIS) et existence de solutions techniques répondant aux critères retenus

*** Quelles qualités sont attendues pour le NIS ?**

- 1ère qualité : il doit répondre à la double condition de sécurité à apporter à la protection des données personnelles de santé que nous souhaitons promouvoir, à savoir que la protection est assurée à la fois par la technique (c'est le système de double hachage qui peut être pratiqué *n* fois, cf. ci-après) mais aussi par la conscience pratique qu'a la personne de l'appartenance et du caractère secret de ses propres infos médicales[2], condition à laquelle répond l'existence d'un NIS distinct du NIR et connu du patient.

- 2ème qualité : il doit permettre d'identifier de manière univoque l'ensemble des dossiers de santé informatisés pour une même personne, notamment son DMP.

[2] Cela renvoie au rapport Tricot, 1975, toujours d'une grande actualité :*" Il est des données personnelles qui méritent une protection renforcée : ce sont en tout cas celles qui sont relatives à la santé mentale et physique des personnes. Les traitements de ces données doit être effectué en utilisant des identifiants distincts du numéro national (aujourd'hui le NIR). Non comme on l'a dit, que cette précaution constitue un obstacle technique infranchissable, mais parce que la présence d'un identifiant spécial contribuera à rappeler à ceux qui participent à ces traitements qu'il y a des informations particulièrement secrètes qui ne peuvent être livrées qu'à un nombre restreint d'utilisateurs qualifiés".* Cette citation, qui fixe le cadre politique qui doit s'imposer aux techniciens est incontournable. Parmi les *"ceux qui participent aux traitements"* figurent dorénavant avec le DMP les patients eux-mêmes.

*** Il existe des solutions techniques pour prendre en compte les critères répondant à ces deux enjeux de qualité :**

- 1er temps, on génère un NIS « public » par anonymisation du NIR : parmi les approches techniques envisageables, nous indiquons ici celle qui repose sur le hachage du NIR qui pourrait être réalisée par un tiers de confiance qui générerait ainsi le numéro d'identifiant santé (NIS) qu'on pourrait ensuite distribuer au patient dans un premier temps puis dès que possible qu'on pourrait inclure dans la carte vitale, en reprenant le même schéma que celui initialement adopté par le GIP-DMP pour la création du NIS (mais en changeant le mode de génération du NIS puisque ce ne serait plus un tirage au sort mais le hachage du NIR).
- 2ème temps, ce NIS public fait l'objet d'une deuxième anonymisation : on procède à un deuxième double hachage à partir du NIS, dans le portail du DMP et des hébergeurs pour les dossiers des professionnels de santé, pour éviter que le NIS public soit chez les hébergeurs.

➔ à l'issue de ces deux temps, les dossiers santé et le DMP sont identifiés de façon parfaitement univoque à partir d'un NIS lui-même conçu de façon univoque à partir du NIR : l'alimentation et la consultation des dossiers de santé est réalisée sans risque d'erreur sur la personne concernée, mais on ne peut pas remonter au NIR ni au NIS à partir de ces dossiers et des données de santé qui y sont stockées.

(Le problème de la correspondance NIS-NIR sur la carte vitale, mais surtout dans le dossier médical du patient sur le logiciel métier du professionnel de santé, peut être minimisé par le fait d'indexer respectivement le NIR et les données facturation d'une part, le NIS et les données santé d'autre part, dans des bases de données distinctes. L'éclatement des informations sur les ordinateurs des professionnels de santé, et le stockage d'une petite partie des informations de chaque patient, nous place dans la situation de fichiers très partiels. De toutes façons l'objectif est principalement de ne pas retrouver le NIR dans des systèmes de stockage de données personnelles de santé exhaustives et chaînées sur toute la durée d'une vie, c'est-à-dire chez les hébergeurs et notamment ceux du DMP).

NB. Pour les patients ne disposant pas de NIR, un NIS peut aussi être généré de façon aléatoire, puis soumis au même processus que décrit ci-dessus.

4) <u>Réponses aux principales objections concernant le choix d'un NIS distinct du NIR</u>

*** Objection n°1 : « *Le NIR est déjà associé aux données de santé, dans le cadre des réformes sur la facturation , par ex. la T2A à l'hôpital et plus généralement les actes et diagnostics »* :**

Les tenants du NIR comme identifiant santé expliquent que le NIR va être utilisé, dans le cadre de la tarification à l'activité (T2A), lors de la transmission des factures. Ceci signifie que les établissements devront créer des fichiers dans les établissements de santé, qui comprendront à la fois les données PMSI et le NIR. Par conséquent, la question de l'utilisation du NIR comme identifiant santé et en particulier l'ajout du NIR dans les dossiers médicaux des établissements ne se poserait plus puisqu'elle est déjà réglée.

Cet argument appelle les éléments de réponse suivants :

- La T2A n'implique pas que le NIR soit présent dans les dossiers médicaux mais seulement que le DIM fasse le rapprochement entre le NIR et les données PMSI, juste avant l'envoi des données de facturation. Bien sûr, ceci supposera qu'un fichier contenant à la fois le NIR et les données PMSI sera stocké au DIM (sous la responsabilité du médecin responsable du DIM). La question de savoir si ce fichier sera stocké également aux affaires financières des établissements n'est pas encore tranchée et nous paraît non conforme à la législation actuelle. Par ailleurs, la T2A ne suppose pas que le NIR soit accolé à toutes les données de santé de l'établissement mais uniquement aux données PMSI.

Le fait que co-existent dans les établissements de santé, sous la responsabilité du DIM, le NIR et les données PMSI (diagnostics et actes codés), nous inquiète encore plus sur la sécurité des données sauvegardées par les établissements. Tous les acteurs reconnaissent que la sécurité des données de santé n'est absolument pas assurée dans les établissements hospitaliers. Le fait que cette sécurité ne soit pas assurée, ne peut qu'inquiéter

concernant la possibilité d'utiliser le NIR dans les établissements de santé accolé à l'ensemble des données de santé.

En l'état actuel de la sécurité des données dans les établissements de santé, la mise en place du dispositif, dans le cadre de la tarification à l'activité, d'une facturation basée sur les données PMSI ne peut qu'être remise en question et, au mieux, différée jusqu'à ce que les établissements aient atteint un niveau de sécurité suffisant, sauf à envisager un autre dispositif, incluant le hachage du NIR dans la transmission des données de facturation vers les caisses d'assurance maladie.

A notre connaissance, il n'existe pas de texte réglementaire statuant sur les modalités techniques de rapprochement du NIR avec les données PMSI dans les établissements de santé, permettant ainsi la transmission avec des données de facturation (précisant comment le rapprochement va être fait, qui va le faire et qui va transmettre les données à l'assurance maladie). Ces questions devraient être traitées avant toute mise en œuvre du projet.

- Le fait que le NIR soit accolé aux données médicales PMSI (diagnostics et actes codés) dans les caisses primaires de l'assurance maladie, ne peut d'aucune manière servir de justification de l'inclusion du NIR dans les bases de données des hébergeurs du DMP.

En effet,
(i) D'une part, il ne s'agit pas des mêmes données : diagnostics et actes codés du PMSI contre diagnostics et actes en clair du DMP ; données réparties entre les différentes CPAM et données regroupées pour chaque individu dans la base de données, chez une poignée d'hébergeurs (prenant alors la valeur de données de population).

(ii) De plus, les données stockées par les caisses primaires sont des données dites glissantes c'est-à-dire qu'elles ne concernent que la prise en charge d'une année donnée et sont détruites 5 ans après la date de la prise en charge (même si cette durée est déjà longue pour assurer la confidentialité des données de santé, on n'est pas dans une logique d'info longitudinale). Au contraire, les données du DMP seront conservées pendant toute la vie du patient. Il est même question à l'heure actuelle de les conserver au moins 30 ans après le décès, voire plus. On a donc un film de l'état de santé du patient depuis sa naissance.

(iii) Enfin les données de l'assurance maladie sont stockées sous responsabilité médicale. Elles sont anonymisées (hachées) au niveau de chaque centre de traitement informatique (CTI) local avant d'être regroupées au niveau national, afin d'être utilisées pour les traitements statistiques de l'assurance maladie, dans le cadre du système national d'information de l'assurance maladie (SNIIR AM), où elles sont hachées une deuxième fois.
L'anonymat porte sur le numéro de sécurité sociale de l'assuré ainsi que sur la date de naissance du patient et sur le sexe du patient : il s'agit d'un algorithme de hachage appelé FOIN, qui est le même que celui utilisé par les établissements hospitaliers pour l'anonymisation du numéro de sécurité sociale dans le cadre du PMSI.

En effet, à l'heure actuelle, les établissements hospitaliers publics et privés stockent séparément les données PMSI de santé (diagnostics et actes) et les données de facturation (dont le NIR). Le rapprochement du NIR et des données PMSI est effectué sous la responsabilité du médecin responsable du département de l'information médicale (DIM) qui va procéder à l'anonymisation du numéro de sécurité sociale, à partir du logiciel FOIN.

Les données transmises à l'administration des hôpitaux par le DIM sont alors anonymisées et cette administration peut ensuite adresser ses données à l'Agence Régionale de l'Hospitalisation (ARH) qui les transmettra ensuite au ministère. Un système de double clé de hachage permet d'être sûr que le numéro d'anonymat obtenu dans les établissements hospitaliers de santé ne sera pas le même que celui utilisé pour le stockage de données au niveau national.

- L'ensemble des acteurs s'accordent sur le fait qu'il faut impérativement exiger un renforcement de la sécurité des données médicales dans les établissements de santé et chez les professionnels libéraux.

Malgré la recommandation de la CNIL d'utiliser la carte de professionnel de santé dans les établissements de santé, la majorité des établissements de santé ne l'utilisent toujours pas. La mise en place des mesures de sécurité légitimement exigées par la CNIL semble nécessiter des moyens organisationnels et financiers importants ainsi que des délais qui sont incompatibles avec le démarrage du DMP au 1er juillet 2007. Il est notable par ailleurs que, dans le cadre des expérimentations qui sont déjà en cours, la CNIL a eu l'occasion de mener des opérations de contrôle dans les établissements concernés et de constater l'insuffisance des mesures de sécurité mises en place (informations non publiées).

En conclusion, la prétendue justification de l'utilisation du NIR au motif de l'existence de la procédure T2A est dépourvue de fondement et de pertinence.

*** Objection n° 2** : ***« Les usagers du système de santé et les professionnels de santé veulent un système simple, ils connaissent et utilisent le NIR et n'accepteront pas un NIS »*** *:*

- Les « experts » parlent ici à la place des acteurs de terrain :
  > Depuis début décembre, plus de 11 000 personnes ont signé la pétition « Pas touche à mon numéro de sécu » dont de très nombreux professionnels de santé parmi des citoyens de tous milieux.
  > Les principales associations de malades chroniques se sont exprimées pour rejeter le NIR comme clé d'accès au DMP et réclamer un *identifiant unique et fiable de patient (IUFP)* distinct du NIR (cf. audition du CISS devant la Cnil le 13/12).
  > Le Conseil national de l'Ordre des médecins aurait, de source informée, adopté une position convergente dans le cadre de discussions avec les autorités concernées.
  Ainsi l'argument est démenti par les représentants de ceux dont il est censé exprimer le point de vue.

- Aucun argument sérieusement étayé ne vient à l'appui de cette assertion :
  > Si on pousse la logique de l'argument à fond, on devrait adopter la notion d'identifiant universel des données personnelles, justement rejetée depuis 30 ans par les démocrates avec le refus d'un numéro national d'identification et l'affaire Safari.
  > La pratique quotidienne montre que, à l'inverse de l'argument ici discuté, les personnes se satisfont parfaitement de manier divers numéro d'identification en fonction de finalités distinctes et ne font par exemple aucune confusion entre leur numéro de carte bleue (secteur bancaire) et le n° de sécu (secteur droits sociaux), personne n'a réclamé que le second vienne se substituer au premier.

- Il faut retourner l'argument :
  > en ré-insistant ici sur la double condition de la protection des données personnelles de santé que nous souhaitons promouvoir, à savoir que la protection est assurée à la fois par la technique (c'est le système de double hachage, cf. ci-avant) mais aussi par la conscience qu'a la personne de l'appartenance et du caractère non public de ses propres informations médicales, condition à laquelle correspond l'existence d'un NIS distinct du NIR et connu du patient (avec in fine un deuxième hachage dans le portail du DMP).
  > Cela renvoie au rapport Tricot, 1975, op. cité (note 2 page 2).

Donc la solution retenue pour l'identifiant santé doit prendre en compte qu'un NIS connu par le patient renforce sa capacité à participer activement à la protection de ses propres données, avantage bien supérieur à l'inconvénient allégué sur la source de complication qui serait liée à la dualité d'usage d'un NIR et d'un NIS.

*** Objection n° 3 :** ***« Choisir le NIR, c'est économiser du temps et de l'argent et cela permettra de mettre en œuvre le DMP au plus tôt, au bénéfice des patients »*** *:*

- Sur l'aspect financier :
  > rappelons ici le caractère fantaisiste des chiffres avancés dans l'exposé des motifs du PFLSS, soit 500 millions d'€, chiffre qui n'est étayé par aucune étude publiée, à comparer au coût de 1 à 1, 5 milliard d'€ avancé pour l'ensemble du déploiement du DMP.
  > le coût de gestion d'un NIS, qui pourrait être dérivé du NIR mais sans retour possible, est négligeable par rapport aux budgets en jeu pour le DMP.

> l'existence de ce coût financier est à mettre en regard avec le bénéfice social attendu du DMP, donc de l'objectif de succès de cette entreprise qui repose sur la confiance des patients, laquelle serait gravement ébranlée si on choisit le NIR, argument déjà développé.

- Sur l'aspect délai :

> le retard éventuel de démarrage du DMP est lié à de nombreux facteurs juridiques, institutionnels, techniques, parmi lesquels l'instauration d'un NIS n'a pas de raison d'être pas le plus prépondérant (cf. l'article du *Quotidien du médecin* du 21/12/2006).
> un retard de quelques mois, pour une entreprise d'une telle ampleur, avec constitution de dossiers de santé informatisés portant sur des décennies d'évènements de santé, est une contrainte acceptable, au regard des bénéfices que le NIS apportera en matière de protection des données personnelles de santé.

*** Objection n° 4 :** ***« Le NIR n'est pas le seul outil permettant de réaliser des interconnexions, il y en d'autres sur le marché »***

- En réalité le NIR est un outil très fiable, voire le plus fiable, pour réaliser les rapprochements de données et interconnexions de fichiers, même si d'autres outils existent pour le faire (cf. argument développé en 2). Par ex. le risque de doublons avec nom, prénom, sexe, date de naissance est notoirement plus élevé qu'avec le NIR où il est négligeable.

- Cet argument n'est pas recevable: la multiplicité de dangers n'est pas un argument pertinent pour s'abstenir de traiter chaque danger distinctement et séparément.
En d'autres termes le fait que l'utilisation du NIR dans le DMP comme identifiant fasse courir un risque majeur pour les libertés individuelles et collectives doit être dénoncé et combattu, comme est dénoncée et combattue par les associations et organismes signataires, notamment et par exemple l'utilisation d'identifiants biométriques dans les fichiers, faisant courir un autre risque majeur d'interconnexions attentatoires aux libertés.