Technologies de l'information et de la communication et données de santé :
pour un cadre juridique en phase avec les évolutions technologiques et les besoins du système de santé

Jeanne Bossi
Secrétaire générale de l'Agence des systèmes d'information partagés de santé[1]

Les données personnelles de santé sont confidentielles : pour protéger la vie privée des citoyens, la loi édicte des limitations strictes quant à leur gestion et à leur transmission. Cependant, les besoins d'échange et de traitement de ces données se font de plus en plus sentir, que ce soit pour le traitement des malades ou pour des études de santé publique. Des progrès techniques ont été réalisés pour faciliter ces échanges : création de référentiels et d'identifiants communs des acteurs. Pour aller plus loin, il faudra préciser le cadre juridique et définir une nouvelle gouvernance des données de santé.

Le développement des nouvelles technologies de l'information et de la communication dans les domaines sanitaire et médico-social peut constituer l'une des réponses aux problématiques que traverse actuellement notre système de santé : égalité d'accès aux soins dans un contexte économique contraint, conséquences du vieillissement de la population et de la dépendance, coordination du suivi médical tout au long du parcours de soins étendu au domaine médico-social et multidisciplinarité croissante de l'exercice médical.
Ces facteurs accroissent en effet le besoin d'échange de données de santé dans l'intérêt d'une meilleure prise en charge des personnes. Toutefois, les données personnelles de santé qui permettent d'identifier un individu sont également susceptibles de révéler l'intimité de la vie privée. A ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objectif de garantir leur confidentialité.
Comment alors permettre le développement des échanges de données de santé dématérialisés, nécessaires à l'amélioration du système de soins, sans toutefois renier les principes fondamentaux de la protection de la vie privée ? Au-delà de l'impulsion d'une politique publique volontariste, comment encadrer le développement spontané et très rapide des technologies dans le secteur des systèmes d'information de santé ?

Nous aborderons cette problématique en commençant par dresser un état des lieux du cadre légal qui régit actuellement l'échange et le partage de données de santé. Nous verrons ensuite comment ce cadre juridique est désormais complété par des référentiels permettant d'assurer la confidentialité des données. A la lumière de cet état des lieux, nous pourrons enfin déterminer les limites du cadre juridique actuel et proposer des pistes de réflexions pour faire face aux nouveaux enjeux soulevés par les évolutions simultanées des secteurs sanitaire et numérique.

1. L'ASIP-Santé est un groupement d'intérêt public fondé en 2009 pour renforcer la maîtrise d'ouvrage publique des systèmes d'information qui se développent dans le secteur de la santé et accompagner l'émergence de technologies numériques en santé.

Un cadre juridique qui doit s'adapter au partage des données de santé

Les données de santé font l'objet en France d'un encadrement juridique qui vise à protéger leur confidentialité.
Le cadre actuel de l'échange et du partage des données de santé s'articule autour de différents textes de lois qui traitent de leurs conditions d'utilisation et des moyens assurant leur confidentialité.
La gestion et le traitement des données de santé sont protégés par la directive européenne 95/46 du 24 octobre 1995 et la loi Informatique et Libertés du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
L'information préalable de la personne sur l'informatisation de ses données et, en particulier, l'information sur ses droits représentent toujours une garantie importante. Dans certains cas, le recueil du consentement peut être une protection supplémentaire de la personne.

a. Les principes de la protection des données personnelles

Ces principes, définis dans la loi « Informatique et Libertés », se concentrent autour de cinq notions clés : une finalité de traitement déterminée et légitime, des données pertinentes (principe de proportionnalité), une durée de conservation déterminée à l'avance et dont la réalité est appréciée au regard de cette finalité (droit à l'oubli), le respect du droit des personnes et de leur information, et enfin la mise en place de mesures de sécurité de nature à garantir la confidentialité des données.
C'est le rôle de l'autorité administrative indépendante qu'est la Commission Nationale de l'Informatique et des Libertés de faire respecter ces principes.
Si l'article 8-1 de la loi Informatique et Libertés pose le principe de l'interdiction de la collecte et du traitement des données de santé à caractère personnel, le deuxième titre du même article procède à l'énumération limitative des cas dans lesquels leur traitement est admis. Les conditions posées diffèrent toutefois selon la finalité poursuivie : recherche médicale, intérêt public, médecine préventive, évaluation des pratiques… etc.
Parmi ces exceptions et cas particuliers, on retrouve les traitements mis en œuvre à des fins de coordination des soins et qui nécessitent le partage de données de santé, dont la CNIL a considéré qu'ils relevaient de l'intérêt public. Il s'agit là par exemple du régime juridique retenu pour le Dossier Médical Personnel (DMP) lancé en 2011 et déployé par l'Agence des systèmes d'information partagés de santé, ASIP Santé.
Le traitement des données personnelles est également admis dans le cas d'une expression du consentement exprès de la personne, sauf si la loi prévoit que l'interdiction ne peut être levée par ce consentement.
Dans certains cas en effet, le consentement de la personne est sans effet parce que la loi elle-même interdit la collecte et le traitement des données de santé. C'est le cas de l'interdiction pour le médecin d'une compagnie d'assurance d'accéder à un dossier médical ou à un employeur d'exiger d'un futur candidat des examens médicaux ou l'accès à son dossier médical.
Enfin, au-delà de l'affirmation de la spécificité des données de santé, la CNIL a toujours recommandé la mise en œuvre de mesures pratiques visant à informer le patient de ses droits et des modalités d'utilisation et de conservation de ses données, conformément aux articles 32, 39 et 40 de la loi informatique et libertés, et articles L.1111-2 et L. 1111-7 du code de la santé publique.
Ainsi, s'est-elle toujours attachée particulièrement aux mesures de sécurité qui doivent être mises en œuvre pour garantir aux données médicales la confidentialité exigée par la loi.[2]

2. Délibération n°01-011 du 8 mars 2001.

C'est ainsi que les traitements de données de santé à caractère personnel que nécessite l'hébergement de ces données doivent être réalisés dans le respect des dispositions de la loi du 6 janvier 1978 et de l'article L1111-8 du code de la santé publique introduit par la loi du 4 mars 2002 sur les droits des malades et la qualité du système de soins, qui disposent que les professionnels de santé ou les établissements de santé ou 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.
L'hébergement des données exige le consentement exprès de la personne concernée, doit respecter les dispositions de la loi Informatique et Libertés et le secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.
L'agrément est délivré pour trois ans par le ministre en charge de la santé après avis de la CNIL et du comité d'agrément des hébergeurs (CAH), dont l'ASIP Santé assure le secrétariat, après une évaluation des capacités des candidats, portant sur les aspects financiers, éthiques et de sécurité de leur activité. Il porte sur une prestation particulière, même si une mutualisation des services proposés est possible.
La liste exhaustive des hébergeurs agréés est disponible sur le site de l'ASIP Santé.

Tableau 1 : Bilan chiffré du Comité d'agrément des hébergeurs à mars 2014

- 188 dossiers ont été réceptionnés depuis le 1er juin 2009
- dont 16 dossiers de renouvellement d'agrément
- 82 dossiers ont été agréés
- 57 refus d'agrément ont été prononcés.

b. L'encadrement de l'échange et du partage des données de santé

Le droit commun de l'échange de données de santé à caractère personnel entre professionnels de santé est fixé à l'article L1110-4 du code de la santé publique. Cet article définit actuellement trois régimes d'échange et de partage des données de santé à caractère personnel :

- l'échange de données de santé entre plusieurs professionnels de santé qui prennent en charge un même patient en dehors d'un établissement de santé, sauf opposition ;
- le partage de données de santé entre professionnels de santé exerçant au sein d'un même établissement de santé, sauf opposition ;
- le partage de données de santé au sein d'une maison ou d'un centre de santé soumis au consentement.

En outre, le législateur a prévu le recueil du consentement de la personne concernée, sous différentes formes, dans le cadre des services nationaux de partage de données de santé que sont le dossier pharmaceutique (DP), le dossier médical personnel (DMP) et l'historique de remboursement.
Cette multiplicité de régimes juridiques est source d'incompréhension tant pour les usagers que pour les professionnels et ne garantit pas une protection efficace des droits des personnes concernées et de leurs données. Ils ne répondent pas à une logique de situation mais résultent d'une succession de textes intervenus au fil du temps et qui, souvent par simplicité, ont exigé de façon systématique un consentement.

c. La nécessaire prise en compte du parcours de soins

On l'a vu, le législateur a étendu la notion d'équipe de soins aux maisons et centres de santé : les professionnels peuvent partager les informations concernant les personnes qu'ils prennent en charge, sans toutefois que le législateur ait imposé la condition de l'appartenance à la même équipe de soins.
Or, on peut regretter que cet élargissement se limite à ces seules structures d'exercice regroupé, dans la mesure où la distinction qui a pu être faite entre une donnée de santé et une donnée médicosociale[3] trouve aujourd'hui ses limites dans la nécessité d'une prise en charge globale de la personne, qu'elle fasse appel au secteur sanitaire ou médicosocial.
Les textes de loi intervenus récemment insistent pourtant sur la nécessité d'une coordination des acteurs, en particulier à l'aide de systèmes d'informations. Ils consacrent également des modèles d'exercice collectif de la prise en charge au sein de structures de groupe. On peut citer la loi "Hôpital, patients, santé, territoires" (HPST) de juillet 2009 qui consacre l'exercice collectif au sein de maisons et centres de santé ou la création des maisons pour l'autonomie et l'intégration des malades d'Alzheimer, ou plus récemment l'article 48 de la loi du 17 décembre 2012 de financement de la sécurité sociale pour 2013, qui prévoit des expérimentations de collaboration entre structures médico-sociales et sanitaires dans le cadre de l'optimisation du parcours de santé des personnes âgées en risque de perte d'autonomie (PAERPA).
Plus globalement, aucun système d'information de santé aujourd'hui ne devrait se développer sans prendre en compte cette dimension dès sa conception.
Il faut donc tendre aujourd'hui vers une homogénéité des règles applicables (information préalable, droit d'opposition, consentement exprès) au partage des données de santé autour de la notion de parcours de soins, en élargissant la notion actuelle d'exercice en équipe à l'ensemble des professionnels de santé impliqués dans la prise en charge du patient.
La personne prise en charge doit pouvoir bénéficier d'un suivi utile, documenté et rendu accessible à l'ensemble de la communauté des professionnels qui seront appelés à la prendre en charge.
Si tous ces textes posent des principes forts pour assurer la protection des données personnelles de santé, la difficulté de leur application concrète et en particulier l'inadaptation des moyens prévus pour assurer la sécurité et la confidentialité des données face au développement de systèmes d'information organisés de façon non concertée ont rendu indispensables la normalisation et la sécurisation du partage de l'information.
C'est précisément cette idée qui a mené à la création de l'ASIP Santé, en 2009 : il s'agit d'instaurer un pilotage stratégique et cohérent des systèmes d'information de santé au niveau national, et de définir le cadre fonctionnel et de sécurité pour l'échange et le partage des données de santé.

Des référentiels désormais accessibles

Ce cadre fonctionnel est constitué par un ensemble de dispositifs techniques, normes et référentiels dans les champs de l'interopérabilité (capacité des systèmes à échanger des informations) et de la sécurité.

3. Lire aussi sur le sujet : BOSSI, Jeanne « Le cadre juridique du partage d'informations dans les domaines sanitaire et médicosocial. État des lieux et perspectives » in Médecine et Droit Vol 2013 – Janvier 2013 – Elsevier Masson – P5 – 8
http://www.em-consulte.com/article/785892/article/le-cadre-juridique-du-partage-dinformations-dans-l

Le cadre national d'interopérabilité des systèmes d'information de santé (CI-SIS)

Mis en place par l'ASIP Santé dès sa création et à la suite d'une concertation avec l'ensemble des industriels, ce référentiel spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de santé entre SIS[4], et contraint la mise en œuvre de ces standards par des spécifications d'implémentation.
L'interopérabilité est définie comme la capacité que possède un produit ou un système informatique à fonctionner avec d'autres produits ou systèmes existants ou futurs. C'est la possibilité qu'ont des systèmes à fonctionner en synergie, à « communiquer », ce qui implique d'utiliser un langage (interopérabilité sémantique) et des référentiels techniques (interopérabilité technique) communs.
Les spécifications et outils du CI-SIS sont modulaires et répartis en trois couches : une couche de contenus interopérables, qui concentrent les moyens de l'interopérabilité sémantique – c'est-à-dire, la structuration et la signification de l'information échangée entre les SI de santé – une couche de services d'interopérabilité et une couche de transport qui représentent quant à elles le socle d'interopérabilité technique du référentiel.
Ainsi, le programme « Santé connectée », lancé par la Haute Autorité de Santé et l'ASIP Santé en novembre 2013[5], vise à amener progressivement les professionnels de santé à saisir et utiliser des données standardisées en cours de consultation. Pour ce faire, le projet définit des règles de langage communes (nomenclatures) pour le poste de travail qui seront intégrées dans le CI-SIS.
La version actuelle du référentiel CI-SIS est la version 1.3 publiée le 18 octobre 2012. En outre, le cadre d'interopérabilité est en évolution constante au gré de l'implémentation de nouveaux volets et des commentaires que les utilisateurs peuvent remonter à l'ASIP Santé via son site web, esante.gouv.fr.

Les dispositifs d'identification des acteurs

Ces dispositifs sont majeurs et sans eux, aucun partage ou échange de données de santé à caractère personnel ne peut être réalisé de façon sécurisée.
S'agissant des professionnels de santé, leur identification repose sur la mise en place du Répertoire partagé des professionnels de santé (RPPS).
Créé par l'Arrêté du 6 février 2009, ce répertoire permet, à partir de données d'identification transmises par les autorités d'enregistrements (ordres professionnels, ARS[6]) de certifier les identités et d'attribuer un numéro RPPS à chaque professionnel de santé (Ordonnance n° 2009-1586 du 17 décembre 2009 relative aux conditions d'enregistrement des professions de santé).
Le RPPS contient à ce jour les médecins, pharmaciens, sages-femmes et chirurgiens-dentistes et doit se substituer à terme au répertoire ADELI[7], pour les professionnels de santé réglementés par le code de la santé publique. Les masseurs-kinésithérapeutes et les pédicures-podologues devraient y figurer prochainement.

Attestant de cette identité, le professionnel de santé peut alors devenir titulaire d'une Carte de Professionnel de Santé (CPS) ou d'un dispositif équivalent qui permet de l'identifier lors de l'échange et du partage de données tout en sécurisant leur transfert par des protocoles de sécurité spécifiques.

4. Systèmes d'information de santé
5. Cf « Programme Santé Connectée DataSet de Bonnes Pratiques DSBP », présentation du 21 novembre 2013 : http://fr.slideshare.net/esante_gouv_fr/20131121-jni-hasinterop
6. Agence Régionale de Santé
7. ADELI signifie Automatisation DEs LIstes. C'est un système d'information national sur les professionnels relevant du code de la santé publique.

La Carte CPS est une carte d'identité professionnelle électronique et une clé d'accès pour le professionnel de santé. Elle contient les données d'identification de son porteur (identité, profession, spécialité) mais aussi ses situations d'exercice (cabinet ou établissement).
L'usage de la carte de professionnel de santé (CPS) est en principe rendu obligatoire pour la conservation et la transmission par voie électronique d'informations médicales à caractère personnel. Cette obligation découle des dispositions de l'article L 1110·4 du code de la santé publique et du décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique, communément appelé « décret confidentialité» (articles R 1110-1 à R 1110-3 du code de la santé publique).
Initialement cantonnée à la télétransmission des feuilles de soins électroniques, la CPS permet aujourd'hui d'identifier le professionnel de santé lors de la consultation ou de la création du Dossier Médical Personnel (DMP) de ses patients, à la messagerie sécurisée de santé (MS Santé), réaliser des actes de télémédecine… les applications potentielles sont encore nombreuses.
Cependant, la dématérialisation accrue des données de santé qui accompagne les nouveaux modes d'exercice de la médecine amène à rechercher d'autres moyens d'accès aux données de santé qui permettent de conserver le même niveau de sécurité que celui apporté par l'usage de la CPS là où l'usage de celle-ci s'avère impossible ou mal adapté. Le législateur lui-même en a acté le principe puisque l'article L1110-4 a été complété par la loi n° 2009-879 du 21 juillet 2009 dite « loi HPST » qui introduit à côté de l'utilisation de la CPS tout autre « dispositif équivalent agréé par l'organisme chargé d'émettre la carte de professionnel de santé », rendant ainsi caduques les dispositions du décret de 2007.
Des dispositifs sont d'ores et déjà reconnus comme alternatifs : couple login/ mot de passe associé à un mot de passe à usage unique (OTP[8]) ou certificats logiciel par exemple. Ils devraient être consacrés dans le cadre des travaux de la Politique générale de sécurité des systèmes d'information actuellement menés par les pouvoirs publics.
L'identification des patients, qui garantit que ces données sont appariées de façon certaine à une même identité et qu'elles ne sont pas susceptibles d'être mal utilisées, est assurée quant à elle par l'Identifiant National de Santé, (INS) prévu par L'article L.1111-8-1 du code de la santé publique, qui postule qu'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 défini à l'article L. 6321 est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé. » Un décret fixe le choix de cet identifiant ainsi que ses modalités d'utilisation.
Dans l'attente de la détermination de cet identifiant, l'ASIP Santé a mis en place dès 2009 une première version de l'INS afin de ne pas retarder le déploiement du cadre d'interopérabilité et permettre la sécurisation de l'accès au DMP. Un INS dit « INS-C » est ainsi calculé localement à partir des traits d'identité contenus dans la carte vitale. Il comporte des imperfections tenant essentiellement à l'absence de carte d'assurance maladie individuelle qui permettrait d'identifier de façon autonome les ayant-droits. Néanmoins, il est apparu plus sécurisant pour le patient d'améliorer les conditions de son identification alors que la situation actuelle reste très insatisfaisante pour le déploiement des systèmes d'information partagés de santé.
Le déploiement actuel des SI de santé autour du patient et de la notion de parcours de soins impose en effet de faire le choix d'un identifiant simple, pérenne, fondé sur des outils de certification déjà existants et reconnus et, dans un contexte budgétaire très contraint, de privilégier l'efficacité à des solutions coûteuses. Le numéro de sécurité sociale, ou « NIR »[9], présente ces caractéristiques.

8. One-time password http://fr.wikipedia.org/wiki/Mot_de_passe_unique
9. Numéro d'inscription au répertoire national d'identification des personnes physiques

En outre, l'utilisation du NIR permettrait de disposer de données de santé fiables directement issues des processus de soins et qui viennent nourrir les bases de données médico-administratives permettant ensuite aux chercheurs de distinguer les éléments utiles à la définition d'une politique de santé publique efficace.
Enfin, cette solution réglerait la question d'un identifiant commun aux secteurs sanitaire et social qui reste un frein à la coordination des soins, notamment dans la prise en charge des maladies chroniques et de la dépendance.
En tout état de cause, le NIR est utilisé comme identifiant permettant d'éviter les doublons et collisions, et ne saurait être utilisé, du fait de son caractère prédictible et non confidentiel, comme clef d'accès aux systèmes d'information. La question est donc à nouveau posée[10] et la CNIL devrait être saisie.

Et demain ? Vers une nouvelle conception des Systèmes d'Information de Santé

Ces réflexions et l'expérience désormais acquise en matière d'échange et partage dématérialisés de données de santé permettent de dégager une vision prospective des principes qui devront à l'avenir guider leur développement.
Tout d'abord, au-delà de l'élargissement de l'accès des données de santé au secteur médico-social et de la mise en place d'une loi sur le secret professionnel partagé, il faut aller vers une redéfinition de la notion de donnée de santé, telle qu'elle semble prônée par les instances européennes. La proposition de règlement du parlement européen et du conseil du 5 janvier 2012[11] sur la protection des données définit ainsi la donnée de santé comme « toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne »
Cette définition élargie doit guider une rénovation des textes permettant une communication plus aisée des informations dans une optique d'amélioration de la coordination des soins, sans pour autant déroger aux principes fondamentaux de la protection de la vie privée et de l'intimité des personnes.
Une définition unifiée permettrait également d'aller vers la mise en place d'une véritable gouvernance des données de santé qui régisse tous les aspects de leur utilisation : coordination des soins, comme on l'a vu, mais également utilisation secondaire.
On parle d'utilisation secondaire des données de santé lorsque les données collectées sont utilisées à des fins de statistiques ou pour la recherche et la mise au point d'indicateurs utiles au pilotage des politiques publiques.
L'utilisation secondaire des données personnelles de santé peut prendre diverses formes, et couvrir des domaines très différents : études épidémiologiques, recherches « biomédicales », activités observationnelles (dont la veille sanitaire), bases médico-administratives.
Or, la France dispose de bases de données médico-sociales et économiques nationales centralisées, couvrant de façon exhaustive et permanente l'ensemble de la population dans divers domaines stratégiques pour la santé publique et la recherche, qui « constituent un patrimoine considérable, vraisemblablement sans équivalent au monde. »[12] : Le PMSI[13] et le SNIIRAM[14] en sont les exemples les plus connus.

10. La CNIL, dans un contexte très différent, a estimé dans son avis du 20 février 2007 que le NIR (ou « numéro de Sécurité sociale ») n'apportait pas les garanties de confidentialité suffisantes pour être l'identifiant du secteur de la santé. Cf « Conclusions de la Commission Nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de Sante » Avis rendu le 20/02/2007 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR.pdf
11. Règlement du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) CE – 25 janvier 2012 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF
12. Pour une meilleure utilisation des bases de données nationales pour la santé publique et la recherche, rapport du Haut Conseil de la Santé Publique – collection documents, mars 2012
13. Programme de médicalisation des systèmes d'information http://fr.wikipedia.org/wiki/Programme_de_m%C3%A9dicalisation_des_syst%C3%A8mes_d'information
14. Système national d'information inter-régimes de l'assurance maladie http://www.sante.gouv.fr/IMG/pdf/CNAMTS___Le_SNIIRAM_et_les_bases_de_donnees_de_l_assurance_maladie_en_2011.pdf

Construites de façon dédiée, elles portent toutefois en elles leurs propres limites. Soit parce qu'elles ignorent le sujet de la santé publique, soit en raison de leur finalité précise et organisée (cohortes), l'accès à ces bases est aujourd'hui techniquement hétérogène et difficile. Il nécessite plusieurs avis préalables d'instances qui complexifient l'accès et participent ainsi à une absence de transparence réelle.
En outre, la validité scientifique des données auxquelles on accède peut être discutée (conditions de collecte, durée de conservation…).
L'accès aux données contenues dans ces bases et surtout l'utilisation d'autres sources de données plus proches de la réalité de l'administration des soins devraient révolutionner notre approche de l'épidémiologie, de la veille sanitaire et des politiques de santé publique qui en découlent (Fig.1).

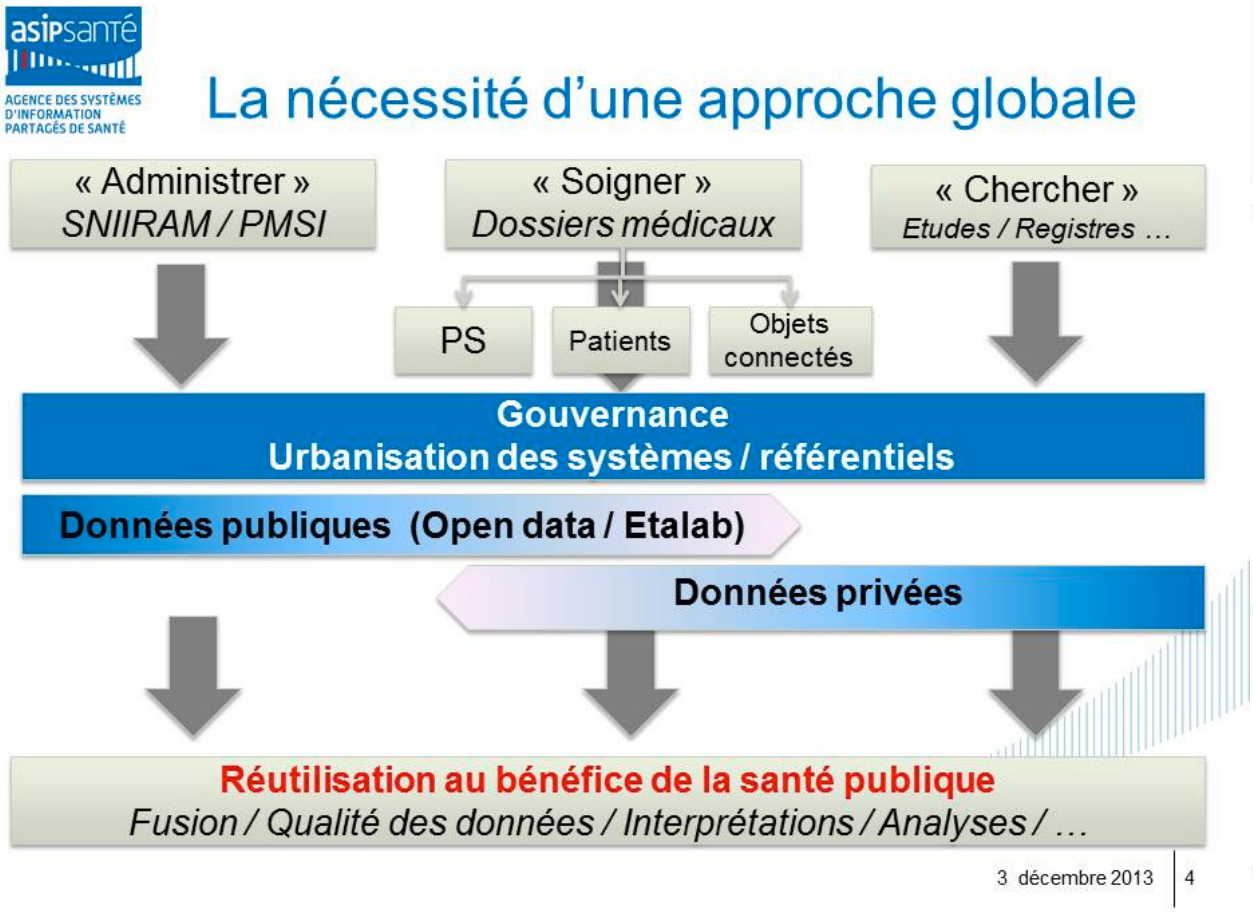

Figure 1. proposition de schéma d'organisation de recueil des données de santé pour leur utilisation secondaire à des fins de santé publique.

Les différentes bases de données de santé, ici médico-sociales avec le SNIIRAM et le PMSI, de soins avec les dossiers médicaux type DMP, et épidémiologiques (recherche) obéissent à des règles de traitement spécifiques et ne partagent pas encore des principes d'urbanisation communs qui pourraient les rendre interopérables (cadre d'interopérabilité). Toutes ces données pourraient être recueillies et compilées, croisées si besoin de façon agile et rapide, dans le respect de principes éthiques communs (anonymisation, finalité, durée de conservation…), afin de servir d'indicateurs en temps quasi réel pour l'évaluation des politiques de santé publique.

Pour faire face à ces problèmes et exploiter enfin tout le potentiel de la « e-santé » pour l'amélioration du système de soins, il sera nécessaire de définir une nouvelle gouvernance des données de santé.
Le Haut conseil pour la santé publique propose deux modèles[15] de gouvernance, en précisant toutefois qu'une entité créée ad hoc ne se substituerait pas aux autorités délivrant les autorisations règlementaires d'accès aux données :

- Gouvernance décentralisée : chaque organisme public gestionnaire de bases de données fixe des règles explicites d'accès (incluant une politique tarifaire et la possibilité de refuser l'accès à ses données) et met en place un « guichet » destiné à traiter les demandes et accompagner les demandeurs.
- Gouvernance centralisée : une structure centrale gère un guichet unique et fait office d'interface entre les demandeurs et les organismes gestionnaires de bases de données, selon des règles homogènes et sous le contrôle d'une instance de gouvernance unique.

Cette gouvernance devra s'accompagner d'une prise en compte de la dimension de santé publique dès la conception des systèmes d'information partagés de santé. Par exemple, en prévoyant dans l'architecture des projets, à côté de la fonction de production de soins, une fonction destinée à produire de la connaissance et une fonction de retour d'information permettant de valoriser les personnes qui les produisent, les professionnels de santé.

Conclusion

Les dispositifs juridiques et techniques mis en place pour prévenir toute utilisation abusive des données personnelles de santé et encadrer leur gestion par un tiers traduisent l'importance attachée par le législateur à la sécurité du traitement de ces données.
Toutefois, l'explosion récente des outils électroniques de partage et d'échange de données, et les usages qui en découlent doivent être pris en compte par les pouvoirs publics afin de fournir un cadre juridique et technique adapté, capable de protéger les droits des personnes mais aussi d'accompagner une vraie révolution technologique qui doit être mise au service de la santé publique.

15. Pour une meilleure utilisation des bases de données nationales pour la santé publique et la recherche, rapport du Haut Conseil de la Santé Publique – collection documents, mars 2012 – P 40