Dalloz IP/IT 2017 p.260

Le règlement européen et la protection des données de santé

Jeanne Bossi Malafosse, Avocat Associé - Cabinet DELSOL Avocats

L'essentiel
En introduisant une définition de la donnée de santé, le règlement européen sur la protection des données personnelles (1) traduit la réalité actuelle de la prise en charge sanitaire des personnes. Il reconnaît aux États membres la possibilité d'en adapter les conditions de traitement, ce que la France a initié au cours des dernières années.

Le règlement européen sur la protection des données du 27 avril 2016 sera applicable le 25 mai 2018. Il porte en lui des changements majeurs et modifie de façon substantielle l'approche du sujet de la protection des données personnelles tel que nous le connaissons en France avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Ce règlement instaure en effet le principe d'*accountability* aux termes duquel chaque acteur devra être en mesure de prouver à tout moment que les traitements qu'il met en oeuvre respectent les principes de protection des données personnelles. Associé à l'obligation d'intégrer en amont des projets les principes de protection des données (*Privacy by Design*) et à la suppression des formalités préalables, il instaure une nouvelle façon d'appréhender la protection des données personnelles.

Désormais l'application concrète des principes de protection des données personnelles sera uniformisée au sein de l'Union européenne et chaque acteur, quel que soit son secteur d'activité, devra les intégrer à ses projets.

Le secteur de la santé n'échappe pas à ce nouveau paradigme mais ses spécificités propres à chaque pays, continueront à le faire relever pour partie du droit national de chaque État membre.

En effet, aux termes du considérant 53 du règlement européen : « Les États membres devraient être autorisés à maintenir ou à introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. Toutefois, cela ne devrait pas entraver le libre flux des données au sein de l'Union lorsque ces conditions s'appliquent au traitement transfrontalier de ces données ».

Le règlement européen introduit toutefois dans le droit positif de chaque membre de l'Union européenne deux nouveautés majeures à l'heure de la dématérialisation croissante des données de santé et du *Big Data* qui se caractérisent par de nouvelles possibilités techniques d'analyse des données : une définition de la donnée de santé et la reconnaissance de la notion de finalité compatible (art. 6.4).

Ces deux éléments viennent en France s'accorder avec les nouvelles règles d'échange et de partage des données de santé et des conditions d'accès à celles-ci à des fins de recherche.

I - Le cadre juridique européen et national s'adapte aux différentes sources de production des données de santé

La nouvelle définition de la donnée de santé du règlement européen s'articule avec les nouvelles règles d'échange et de partage définies par le code de la santé publique.

A - Une nouvelle définition de la donnée de santé dans le règlement européen

Le nouveau règlement européen sur la protection des données personnelles du 27 avril 2016 définit ainsi plus largement la donnée de santé qu'il n'était coutumier de le faire (2). Celle-ci couvre désormais toutes informations relatives à l'identification du patient dans le système de soin ou le dispositif utilisé pour collecter et traiter des données de santé, toutes informations obtenues lors d'un contrôle ou d'un examen médical y compris des échantillons biologiques et des données génomiques, toutes informations médicales : par exemple, une maladie, un handicap, un risque de maladie, une donnée clinique ou thérapeutique, physiologique ou biologique, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un dispositif médical ou d'une exploration *in vivo* ou *in vitro.*

Cette nouvelle définition traduit un concept plus large de la donnée de santé prenant en compte le fait que la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples, professionnels de santé et personnels sociaux.

B - Une donnée également protégée

Les données de santé à caractère personnel (3) sont considérées par la loi Informatique et Libertés (art. 8, § I) comme des données dites « sensibles » dont la collecte et l'utilisation dans le cadre d'un traitement sont, par principe, interdits. Toutefois, le paragraphe II du même article procède à l'énumération limitative des cas dans lesquels leur traitement est admis. Les conditions posées diffèrent néanmoins selon la finalité poursuivie : recherche médicale, intérêt public, médecine préventive, évaluation des pratiques, etc.

L'article 9 du règlement européen, qui concerne le traitement portant sur des catégories particulières de données, reprend les mêmes finalités que l'article 8, paragraphe II, de la loi précitée.

Cette disposition doit être lue avec celle du I de l'article L. 1110-4 du code de la santé publique modifiée par la loi du 26 janvier 2016 portant modernisation de notre système de santé qui précise que : « I. - Toute personne prise en charge par un professionnel de santé, un établissement ou un des services de santé définis au livre III de la sixième partie du présent code, un professionnel du secteur médico-social ou social ou un établissement ou service social et

médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations le concernant.

Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne, venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé [...] ».

La définition très large des catégories de professionnels susceptibles d'intervenir désormais dans la prise en charge sanitaire d'une personne s'articule avec la définition de la donnée de santé du règlement.

Les conditions d'utilisation de ces données doivent ensuite être appréciées à l'aune des cinq grands principes de la protection des données personnelles (4) qui sont aujourd'hui traduits par le nouveau règlement européen sous la notion de *Privacy by Design*. Chaque acteur doit prendre en compte ces principes de protection dès la conception de son système à travers des mesures techniques et organisationnelles appropriées et à en être redevable (*Accountability*). Ce dernier principe conduit les responsables de traitement à être à même de démontrer la conformité des activités de traitement avec le règlement, y compris l'efficacité des mesures mises en place. Aux termes du considérant 74 du règlement, ces mesures doivent tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés de personnes physiques.

II - Le cadre européen s'articule avec les nouvelles règles d'échange et de partage des données de santé définies par le code de la santé publique

A - L'équipe de soins

L'équipe de soins est désormais redéfinie et adaptée à la réalité du partage des données personnelles. À cet effet, le nouvel article L. 1110-4 du code de la santé publique précité tout en réaffirmant le secret redessine le régime de l'échange et du partage des données personnelles de santé en l'articulant avec une notion élargie d'équipe de soins (art. L. 1110-12).

L'équipe de soins, préalablement limitée à l'équipe d'un service hospitalier, est redéfini comme un ensemble : « [...] de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap ou de prévention de perte d'autonomie, ou aux actions nécessaires à leur coordination [...] ».

Cette nouvelle définition prend désormais en compte la réalité des prises en charge pluridisciplinaires par des structures multiples qui, jusqu'à présent, restaient bloquées par l'absence de fondement juridique harmonisé entre le secteur médical et le secteur médico-social (5).

À cette nouvelle définition de l'équipe de soins est associée une harmonisation des régimes d'information et de consentement. Au sein d'une équipe de soins est réservé le régime de l'information préalable de la personne concernée et de la reconnaissance de son droit d'opposition, l'exigence du recueil du consentement de la personne étant réservée lors du partage d'informations en dehors de cette équipe (6).

B - Un contexte fonctionnel clarifié

Le nouvel article L. 1110-4-1 du code de la santé publique issu de la loi n° 2016-41 du 26 janvier 2016, prenant la suite de la loi Hôpital Patients Santé et Territoires de 2009 consacre une assise législative unique aux référentiels de sécurité et d'interopérabilité que les responsables de systèmes d'information sont tenus de respecter. Ils sont définis par l'ASIP Santé et approuvés par voie d'arrêté pris par le ministre en charge de la santé après avis de la CNIL et publiés au *Journal officiel*.

Ces référentiels sont principalement les suivants :

- La certification de l'identité des professionnels de santé impliqués dans les systèmes d'information tout d'abord par l'inscription au répertoire partagé des professionnels de santé (RPPS).

La certification de l'identité des patients permet d'assurer l'identitovigilance au sein des systèmes d'information.

La loi précitée reconnaît désormais au numéro de sécurité sociale le caractère d'identifiant national de santé (INS) mettant ainsi fin à des années de discussion et d'hésitation autour de l'utilisation de cet identifiant qui a toujours eu une place particulière au sein de la loi Informatique et Libertés.

Notons que l'article 87 du règlement européen réserve aux États membres le soin de préciser les conditions spécifiques du traitement d'un numéro d'identification national ou de tout autre identifiant d'application générale. Il poursuit en indiquant que cet identifiant ne doit être utilisé que sous réserve des garanties appropriées pour les droits et libertés de la personne concernée tels que prévus par le règlement.

L'identifiant national de santé ou INS est visé à l'article L.1111-8-1 du code de la santé publique qui dispose que « ...I- Le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise les modalités d'utilisation de cet identifiant, notamment afin d'en empêcher l'utilisation à des fins autres que sanitaires et médico-sociales... ». Le décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé vient de préciser ces conditions.

- L'encadrement de l'activité des hébergeurs de données de santé à caractère personnel constitue un troisième référentiel important. Conçue initialement en 2002 pour maîtriser le développement d'activités nouvelles dues au développement d'internet dans le secteur de la santé, la procédure a été définie par le décret n° 2006-6 du 4 janvier 2006 qui définit les points constitutifs du contrat d'hébergement et les obligations de l'hébergeur et de son client.

La loi du 26 janvier 2016 est venue clarifier certains aspects de cette procédure et surtout, annoncer une évolution

de celle-ci vers un processus plus classique de certification. L'exigence du consentement de la personne dont les données sont hébergées est supprimée et le champ d'application de la procédure est précisé (7).

- Enfin la définition d'un cadre national d'interopérabilité des systèmes d'information mis en place par l'ASIP Santé dès sa création et à la suite d'une concertation avec l'ensemble des industriels spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de santé entre systèmes d'information, et contraint la mise en oeuvre de ces standards par des spécifications d'implémentation.

III - Une utilisation pour la santé publique prévue par les textes européens et français encore trop contrainte

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé crée dans la première partie du code de la santé publique, au sein du livre IV relatif à l'administration générale de la santé, un nouveau titre VI consacré à la mise à disposition des données de santé. Ces dispositions doivent bien sûr s'articuler étroitement avec celles de la loi Informatique et Libertés, notamment celles du nouveau chapitre IX également modifié et désormais relatif aux traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (art. 54 et s.) (8).

Le sujet très porteur de l'ouverture des bases de données de santé, en particulier celles détenues par les pouvoirs publics, indispensable à un développement des nouvelles méthodes de recherche induites par les techniques du *Data Mining*, doit donc maintenant compter avec ces nouvelles dispositions.

Une première analyse de celles-ci - qui nécessiteront d'être appréciées à nouveau dans quelque temps à la lumière de leur mise en oeuvre pratique - conduit selon le prisme choisi, soit à y voir une simplification des procédures qui pourrait notamment être déduite de la fusion des chapitres IX et X de la loi Informatique et Libertés (9), soit au contraire un vrai parcours d'étapes réduisant considérablement la portée des deux objectifs initiaux, celui de la simplification et celui de l'ouverture des bases de données.

Une procédure d'autorisation unique à étapes multiples est ainsi en cours de mise en place faisant intervenir le nouvel Institut national des données de santé créé par l'article L. 1462-1 du code de la santé publique qui reçoit les demandes d'autorisation (10), le nouveau Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, ou les Comités de protection des personnes selon les cas et la CNIL.

La mise en place du Système national des données de santé (SNDS) (11), dont les conditions d'accès sont également définies par la loi instaure d'ores et déjà une procédure plus contraignante prévue pour les organismes d'études et de recherches poursuivant un but lucratif, notamment (12) les personnes produisant ou commercialisant des produits à finalité sanitaire, les établissements de crédit, les entreprises exerçant une activité d'assurance directe ou de réassurance et les intermédiaires d'assurance.

La CNIL dispose de moyens de simplification (méthodologies de référence, autorisations uniques et référentiels de sécurité).

Perspectives

Il serait toutefois souhaitable, afin de prendre en compte les besoins accrus des acteurs de disposer de données, d'aligner les procédures entre acteurs publics et privés dès lors qu'un intérêt de santé publique est poursuivi et que des garanties appropriées sont prises et de s'inscrire dans un processus de contrôle fondé sur les principes qui commandent désormais la protection des données personnelles dans l'ensemble des pays de l'Union européenne (*Privacy by Design* et *Accountability*).

Ces évolutions apparaissent aujourd'hui essentielles pour que la donnée de santé produite à l'occasion du soin puisse contribuer à nourrir en temps réel la recherche et ainsi contribuer à élever le niveau de la santé publique.

Le Conseil de l'Europe s'apprête également à réviser sa Recommandation sur la protection des données de santé et les dispositions du projet de texte actuellement en discussion viendront utilement enrichir une doctrine commune de développement de systèmes d'information en santé respectueux de la protection des données personnelles.

Mots clés :
DONNEES A CARACTERE PERSONNEL * Protection * Règlement (UE) 2016/679 du 27 avril 2016 * Données de santé

(1) Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avr. 2016 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.

(2) Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la dir. 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques ; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro* (consid. 35).

(3) Conformément à l'art. 2 de la loi Informatique et Libertés, le caractère « personnel » de la donnée de santé comme de toute donnée tient au fait que cette donnée permet une identification, de façon directe ou indirecte, de la personne physique à laquelle elle se rattache, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

(4) Une finalité de traitement déterminée et légitime, des données pertinentes (principe de proportionnalité), une

durée de conservation déterminée, le respect du droit des personnes et de leur information et la mise en place de mesures de sécurité de nature à garantir la confidentialité des données.

(5) V. Le cadre juridique des données de santé confronté à l'exigence du partage, Méd. et Droit, 2013.

(6) Définition des conditions de l'expression du consentement du patient (y compris dématérialisé) pour le partage d'informations entre des professionnels de santé ne faisant pas partie de la même équipe de soins - Décr. n° 2016-1349 du 10 oct. 2016.

Conditions d'échange et de partage d'informations entre professionnels de santé et non professionnels de santé du champ social et médico-social - Décr. n° 2016-994 du 20 juill. 2016.

Cahier des charges d'organisation d'une équipe de soins dans le cadre d'un parcours de soins - Arr. du 25 nov. 2016.

(7) Ainsi, « toute personne qui héberge des données de santé à caractère personnel, recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime ».

(8) Le chap. X de la loi Informatique et Libertés est dès lors supprimé.

(9) Chap. IX : Traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé.

Chap. X : Traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention.

(10) À l'exception des recherches biomédicales interventionnelles et non interventionnelles.

(11) Le SNDS est composé des bases de données suivantes :

- les données issues des systèmes d'information mentionnés à l'art. L. 6113-7 CSP, c'est-à-dire des données produites dans le cadre du programme de médicalisation des systèmes d'information (PMSI) qui traduisent l'activité des établissements de santé, publics ou privés ;

- les données du Système national d'information interrégimes de l'assurance maladie (SNIIRAM) produites par les organismes gérant un régime de base d'assurance maladie (CSS, art. L. 161-28-1) ;

- les données sur les causes de décès mentionnées à l'art. L. 2223-42 CGCT ;

- les données médico-sociales du système d'information mentionné à l'art. L. 247-2 CASF qui rassemble les données produites par les maisons départementales des personnes handicapées sous l'autorité de la Caisse nationale de solidarité pour l'autonomie ;

- un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants.

(12) Art. L. 1461-3, II.