COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 20 juin 2015 T-PD(2015)07

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

(T-PD)

Rapport de présentation visant à mettre à jour la Recommandation n° R (97) 5 du Conseil de l'Europe sur la protection des données médicales

Par Jeanne Bossi Malafosse
Cabinet DLA Piper France LLP

Direction Générale – Droits de l'Homme et Etat de droit

Sommaire

I- Introduction : le contexte de la protection des données de santé en 2015

Le développement du numérique au cours des dernières années a conduit à une véritable « datification » de nos sociétés. Les données sont partout. L'activité mondiale produira plus de données durant les deux prochaines années qu'elle n'en a produit depuis les débuts de l'informatique. Ces données constituent une matière première précieuse et un enjeu mondial de croissance qui représenterait pour l'Europe pas moins de 8% du PIB européen à l'horizon 2020.

Le secteur de la santé n'échappe pas à ces évolutions. L'informatisation croissante du secteur professionnel et notamment des activités de soins et de prévention, de recherche en sciences de la vie, de gestion du système de santé, et d'autre part l'implication croissante des patients caractérisent notamment ce nouvel environnement.

Les phénomènes de mobilité, le développement des objets et dispositifs médicaux connectés contribuent désormais à la croissance exponentielle du volume de données produit, le phénomène du "Big data" ne faisant que traduire les spécificités du traitement de grandes masses de données avec leurs exigences de rapidité de traitement, d'hétérogénéité des données et de création de valeur particulière.

Les données de santé représentent donc des enjeux singuliers et un potentiel de création de valeur et de contribution à la santé publique dont la concrétisation dépendra de la capacité des Etats à organiser le développement d'un écosystème facilitant leur exploitation tout en garantissant le respect de la vie privée et la confidentialité des données personnelles.

Les Etats sont en effet aujourd'hui confrontés à des enjeux majeurs pour lesquels le traitement des données de santé peut jouer et jouent déjà un rôle essentiel : des enjeux de santé publique face notamment au développement des maladies chroniques, des enjeux de qualité des soins, des enjeux de transparence et de démocratie sanitaire, des enjeux d'efficience du système de santé dans un contexte de croissance des dépenses de santé et de déficit chronique des comptes sociaux et des enjeux d'innovation et de croissance dans des domaines aussi variés et importants que la médecine personnelle et les technologies de l'information.

La e-santé, c'est-à-dire l'utilisation des technologies de l'information et de la communication dans le secteur de la santé, apparaît comme un formidable levier de qualité, de sécurité et d'efficience des soins, bien identifié par les pouvoirs publics. Les systèmes d'information et de façon générale, les technologies numériques seront au cours de cette décennie l'un des principaux supports de l'amélioration de la qualité, de l'organisation et de l'efficience des systèmes de santé.

Ces multiples enjeux se posent dans des termes très différents aujourd'hui par rapport à 1997, date de la Recommandation n° (97) 5 du Conseil de l'Europe sur la protection des données médicales.

En effet, le développement des nouvelles technologies de l'information et de la communication dans les domaines sanitaire et médico-social conjugué aux défis rappelés précédemment auxquels sont confrontées les sociétés a eu un effet systémique sur les organisations et le rôle des différents acteurs du soin.

Le besoin d'échange et de partage des données de santé dans l'intérêt d'une meilleure prise en charge des personnes est devenu primordial et modifie de façon considérable la nature même des relations entre soignants et soignés qui, il y a quelques années restaient fondés sur un colloque singulier sacralisé. Le patient est aujourd'hui actif et veut - même s'il n'en mesure pas toutes les conséquences - maîtriser son traitement, ses données et la façon dont elles sont traitées.

Bien sûr, les données personnelles de santé qui permettent d'identifier un individu sont toujours susceptibles de révéler l'intimité de la vie privée et, à ce titre, le droit doit continuer à leur reconnaître un statut particulier et imposer le respect de règles ayant pour objectif de garantir leur confidentialité. Le respect du secret professionnel (médical) est et doit rester au centre de cette garantie.

La future Recommandation du Conseil de l'Europe destinée à actualiser ou remplacer celle de 1997 devra prendre en compte ces évolutions : comment permettre le développement des échanges de données de santé dématérialisés, nécessaires à l'amélioration du système de soins et de la prise en charge des personnes, sans toutefois renier les principes fondamentaux de la protection de la vie privée ?

Cette nouvelle Recommandation devra également prendre en compte les principes de l'actuel projet de Règlement communautaire sur la protection des données personnelles qui prend d'ores et déjà en compte les évolutions majeures intervenues depuis la Directive 95/46 du 24 octobre 1995, en particulier le principe du *Privacy by design* qui impose de prendre en compte la protection des données dès la conception des systèmes amenés à en assurer le traitement.

Les développements qui suivent ont pour objet de proposer de nouvelles orientations pour refondre le texte de la Recommandation de 1997. Ils se situent résolument dans une perspective où le numérique n'est plus une question mais une réalité. Ils sont nourris de l'analyse qui a été faite des questionnaires adressés aux Etats membres du Conseil de l'Europe dont la présentation est jointe en annexe et par l'analyse que l'on peut faire aujourd'hui de l'utilisation du numérique dans le secteur de la santé.

II- Orientations pour une nouvelle recommandation

1. Un nouveau champ d'application à définir

Les définitions qui introduisent l'Annexe à la Recommandation n° R (97) 5 doivent être revues et complétées. Si la définition de la donnée à caractère personnel est conservée, elle est complétée par d'autres définitions qui auront pour objet de préciser les termes utilisés dans la Recommandation et qui traduisent ainsi le nouveau champ d'application de ce texte.

1.1 La donnée de santé à caractère personnel

En premier lieu, l'expression "*données de santé*" serait dorénavant préférée à celle de "*données médicales*".

Il s'agit concrètement de données susceptibles de révéler l'état de santé de la personne. Cette indication serait conforme également à la définition d'une donnée de santé issue de la proposition de règlement du parlement européen et du conseil du 5 janvier 2012 sur la protection des données : «*toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne*». Elle traduit un concept plus large de la donnée de santé, qui aujourd'hui ne peut se limiter à la seule indication d'une maladie tant 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 du secteur social.

La donnée de santé à caractère personnel couvre donc en particulier toutes informations relatives à l'identification du patient dans le système de soins 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 les données génomiques, toutes informations médicales : par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, 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'une épreuve diagnostic in vitro.

Les données médico-sociales désignent toutes données produites par des professionnels exerçant dans le secteur social et médico-social, participant à la prise en charge sanitaire de la personne concernée par exemple en contribuant à caractériser son état de santé. Par souci de simplification, le terme de donnée de santé à caractère personnel couvre également celui de données médico-sociales.

Au surplus, le Groupe de l'article 29 a publié le 5 février 2015, à la demande de la Commission Européenne, un avis sur les critères à prendre en compte pour définir une donnée de santé, en particulier quand elles sont en relation avec le mode de vie et les applications de bien-être[1].

En deuxième lieu, les concepts "*d'anonymisation*" et de "*pseudonymisation"* nécessitent également d'être définis tant les techniques auxquelles ils renvoient sont répandues aujourd'hui en particulier pour la réutilisation des données de santé à des fins de recherche ou dans le cadre du Big data par exemple. L'anonymisation est le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification. Elle constitue un traitement ultérieur des données à caractère personnel. La pseudonymisation qui n'est pas une méthode d'anonymisation, réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée. C'est une mesure de sécurité utile.
Les données pseudonymisées continuent à permettre l'individualisation d'une personne concernée et la corrélation entre différents ensembles de données.[2]

Proposition n° 1

- Définir de façon large la donnée de santé pour y inclure toutes les informations susceptibles de caractériser l'état de santé d'un individu, les prestations de services de santé servies ainsi que l'environnement médico-social de la personne.

- Définir les notions d'"anonymisation" et de "pseudonymisation".

1.2 L'échange, le partage des données de santé à caractère personnel et les systèmes d'information

Il apparaît nécessaire de définir les notions d'échange et de partage de données de santé à caractère personnel tant ces notions traduisent désormais la réalité de l'exercice médical et permettent aux différents acteurs, professionnels comme patients de gérer les données de santé, les systèmes d'information constituant à cet égard les outils permettant le développement de l'échange et du partage.

Si le respect de la vie privée et le secret médical sont deux droits fondamentaux du patient, le secret médical s'impose à tous les professionnels de santé. Mais pour assurer la continuité des soins ou pour déterminer la meilleure prise en charge possible, les professionnels de santé ont désormais besoin d'échanger des informations sur les patients qu'ils prennent en charge. Cette notion de « secret partagé » est en général reconnue par la loi qui précise également les limites. Le patient doit toutefois toujours pouvoir refuser à tout moment que des informations qui le concernent soient communiquées à un ou plusieurs professionnels de santé.

L'échange de données pourrait être défini comme la communication d'informations à un (des) destinataire(s) clairement identifié(s) par un émetteur connu. L'utilisation d'une messagerie sécurisée en constitue un exemple.

A contrario, le principe du "partage" de données consiste à rendre accessibles des informations à des tiers pas nécessairement identifiés au moment de la mise en partage et selon un principe d'habilitations. Le partage expose donc à des risques particuliers du fait de la conservation des

[1] Trois catégories ont été ainsi distinguées : "a) Les données traitées par l'application ou le dispositif est intrinsèquement / clairement des données médicales. En d'autres termes, les données fournissent des informations sur l'état de santé physique ou mentale d'un individu généré dans un contexte professionnel de la santé (par exemple, les fournisseurs de soins de santé) ; b) les données brutes du capteur traitées par l'application ou dispositif peuvent être utilisés indépendamment ou en combinaison avec d'autres données, pour tirer des conclusions sur l'état de santé ou des risques réels pour la santé d'un individu ; c) les données permettant de tirer des conclusions à propos de l'état de santé d'un individu (indépendamment du fait que ces conclusions sont exactes ou inexactes, légitimes ou illégitimes, suffisantes ou insuffisantes)".
[2] Cf Avis 05/2014 sur les Techniques d'anonymisation adopté par le 10 avril 2014 par le groupe de travail "Article 29" sur la protection des données.

données mais permet ainsi de mettre à la disposition de plusieurs professionnels fondés à en connaître des informations utiles à la coordination et à la continuité des soins ou à l'intérêt de la personne. Le principe d'un dossier médical électronique partagé en constitue un exemple.

Le partage et l'échange des données de santé à caractère personnel sont conditionnés d'une part par le développement de systèmes informatiques interopérables et d'autre part, par l'usage de référentiels communs entre professionnels.

Les systèmes d'information de santé qui constituent aujourd'hui le support dématérialisé de la circulation des données de santé doivent également être visés dans les définitions. En effet, le phénomène de numérisation qui s'observe dans le secteur de la santé comme dans les autres secteurs a modifié les règles d'urbanisation des systèmes d'information qui doivent désormais se caractériser par leur interopérabilité. L'interopérabilité est garante de l'expression des droits des personnes. Conserver des données de santé personnelles dans des formats propriétaires qui en interdirait l'accès peut constituer une restriction à l'exercice des droits.

Proposition n° 2

- Définir les notions d'échange et de partage des données de santé.

- Définir les termes d'urbanisation des systèmes d'information de santé et d'interopérabilité.

1.3 L'hébergement des données de santé et *le Cloud computing*

Le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données de santé sur internet est devenu aujourd'hui un moyen efficace de gérer les bases de données et d'assurer un stockage à moindre coût. Le terme de *Cloud Computing* est utilisé pour définir les différents modes de conservation sur internet de ces bases : Saas (*Software as a service*), Iaas (*Infrastructure as a service*) et Paas (*Plate-forme as a service*).

Ce terme doit être défini dans la Recommandation tant le traitement des données de santé aujourd'hui ne se développe pas aujourd'hui sans ces nouvelles infrastructures.

La reconnaissance du rôle joué par les plates-formes de services et de leur responsabilité dans le traitement des données qu'elles hébergent est à cet égard symptomatique et devra faire l'objet d'un développement dans la future Recommandation.

1.4 La santé mobile (dispositifs médicaux et objets connectés)

La santé mobile qui se développe depuis plusieurs années dans tous les pays (les réponses apportées au questionnaire le démontrent), correspond concrètement à l'utilisation d'objets connectés à des fins de gestion de données de santé. Ce développement revêt des formes diverses et recouvre plusieurs catégories d'applications qui elles-mêmes poursuivent des finalités d'usage très différentes. Du dispositif médical aujourd'hui réglementé au plan européen aux applications de "*msanté*" ou de "*quantified self*", il apparaît nécessaire de poser certains principes d'utilisation et de traitement des données de santé par ces objets connectés dont une des caractéristiques majeures est de démultiplier la quantité de données produites.

Traditionnellement en effet, le soin produit de la donnée - la visite chez le professionnel de santé génère un dossier médical. Désormais, ces outils vont produire des données qui vont impacter les soins.

En particulier, essayer de définir la frontière entre les applications de "bien-être" qui ne seraient pas soumises aux mêmes exigences que celles qui poursuivent clairement un objectif de prise en charge sanitaire semble utile pour mieux préciser les obligations des acteurs (Cf bas de page 1 sur les différentes catégories dégagées par le Groupe de l'Article 29).

Proposition n° 3

- Définir les termes d'hébergement/Cloud Computing.

- Définir les termes de "santé mobile" en distinguant les finalités de bien-être et de prise en charge sanitaire et les données produites par le patient lui-même et sous sa responsabilité de celles produites avec l'intervention de professionnels (de santé et du secteur médico-social).

2. Le cadre juridique du traitement des données de santé à caractère personnel

2.1 Les principes de protection des données à caractère personnel

Il doit être rappelé que les données de santé à caractère personnel ne peuvent être traitées que dans les cas déterminés par le droit interne et, en tout état de cause, dans le respect du secret professionnel, de la vie privée des personnes et de la confidentialité de ses informations.

Les principes qui commandent la protection des données personnelles tels qu'exprimés dans la Convention du Conseil de l'Europe du 28 janvier 1981 et explicités dans la Directive 95/46 du 24 octobre 1995 doivent également être respectés. Ils doivent être rappelés dans le corps du projet de Recommandation comme un cadre général et obligatoire : une finalité de traitement déterminée et légitime, des données pertinentes, une durée de conservation des données limitée, la mise en place de mesures de sécurité de nature à garantir la confidentialité des données et le respect du droit des personnes et de leur information.

Mais aujourd'hui, au regard d'un contexte qui a profondément évolué, ces cinq règles d'or de la protection des données doivent pouvoir s'adapter au décloisonnement des échanges entre professionnels et patients et à la notion de parcours de soins qui caractérise aujourd'hui davantage la prise en charge que le traditionnel colloque singulier entre un professionnel et un patient, même si celui-ci persiste.

S'il apparaît encore nécessaire de lister les différentes finalités pour lesquelles les données de santé peuvent être collectées et traitées, il convient aussi de prendre en compte le fait que le développement des objets connectés par exemple démultiplie le nombre de donnés produites et pour des finalités qu'il n'est pas toujours facile de déterminer à l'avance.

Les principes traditionnels de protection des données ne sont pas toujours aisément applicables aujourd'hui à ce phénomène de "datification", le Big Data en constituant un exemple concret. [3]

Il apparaît donc important de préciser, à côté des finalités classiques de traitement des données médicales, la capacité des Etats à prévoir un usage non déterminé à l'avance dès lors qu'il respecte les principes de confidentialité et de vie privée des individus et sous le contrôle de l'autorité de protection des données nationale.

A titre d'illustration, la possibilité aujourd'hui offerte par le Big Data de pouvoir identifier des problèmes de santé publique non déterminés à l'avance mais dont la connaissance est rendue désormais possible par l'analyse d'une plus grande quantité de données doit être permise.

[3] "Le Big Data, (« grosses données »), désigne des ensembles de données qui deviennent si volumineux qu'ils en deviennent difficiles à traiter avec les seuls outils de gestion de base de données ou les outils classiques de gestion de l'information.

Le Big Data désigne aussi l'ensemble des technologies, infrastructures et services permettant la collecte, le stockage et l'analyse de données recueillies et produites en nombre croissant, grâce à des traitements automatisés et au recours aux technologies de l'intelligence artificielle " (Rapport de l'Institut Montaigne sur Big data et objets connectés 2015).

De la même façon la notion de responsable de traitement doit prendre aujourd'hui en compte l'absence de frontières physiques aux transferts de données et la nouvelle responsabilité indéniable des plates-formes internet dans la réalisation d'un traitement ainsi que le fait que les finalités d'un traitement et ses modalités sont désormais souvent définies par des personnes multiples.

En tout état de cause, il appartient toujours aux autorités de protection des données nationales de s'assurer du respect de ces principes et de diffuser toutes recommandations de nature à faire respecter le principe du "*Pivacy by design*".

2.2 La reconnaissance d'un secret professionnel partagé

Les politiques de santé actuelles conduites en Europe en particulier, insistent sur la nécessité d'une coordination des acteurs intervenant tout au long du parcours de soins du patient, en particulier à l'aide de systèmes d'informations. Ce parcours présente un périmètre qui n'est pas restreint aux soins et qui s'articule autour de la prévention, du sanitaire, du médico-social et du social. Il présente une dimension à la fois temporelle (organiser une prise en charge coordonnée et organisée du patient) et spatiale (organiser cette prise en charge sur un territoire, dans la proximité de son domicile).

Ce décloisonnement entre les acteurs du secteur sanitaire et ceux du médico-social s'incarne dans la création de nouvelles structures d'exercice collaboratif et de nouveaux modes d'exercice qui doivent pouvoir se fonder sur la reconnaissance juridique d'un secret partagé.

Le développement des dossiers médicaux électroniques et des plates-formes collaboratives requiert cette avancée dont le principe est d'ores et déjà acquis dans nombre de pays. La France par exemple s'apprête à voter un texte de loi élargissant de façon substantielle la notion d'équipe de soins pour permettre aux professionnels des secteurs sanitaire, médico-social et social d'échanger et de partager sans violer le secret professionnel et mettre en cause leur responsabilité. Bien sûr, ce secret partagé doit être limité aux patients communs pris en charge et dès lors que ces derniers ne s'y opposent pas.

Proposition n° 4

- Rappeler les grands principes de protection des données de santé à caractère personnel tout en intégrant à travers le principe du "*privacy by design*" la notion de conformité à un cadre permettant d'adapter les finalités de collecte et de traitement des données et la détermination du ou des responsable(s) de traitement.

- Reconnaître un secret professionnel partagé entre professionnels de santé qui prennent en charge les mêmes patients.

3. Un cadre fonctionnel sécurisé adapté à la nouvelle urbanisation des systèmes d'information de santé

3.1 Les référentiels d'interopérabilité

Le traitement des données médicales fait appel aujourd'hui à de nouvelles architectures informatiques de gestion (mode Saas par exemple) ou de conservation (Cloud). Ce nouvel environnement informatique doit permettre la communication dans le respect des principes définis juridiquement.

Certains référentiels techniques, de sécurité et organisationnels doivent ainsi être définis par les autorités de chaque Etat pour garantir aux citoyens que leurs données de santé sont bien gérées en respectant leur confidentialité et leur vie privée.

Ces référentiels ont besoin d'une assise juridique pour pouvoir s'imposer et permettre l'interopérabilité technique et sémantique des systèmes d'information sans laquelle il ne peut y avoir d'échange et/ou de partage efficaces.

Ils se fondent sur des normes et standards internationaux qui permettent aux produits ou systèmes informatiques présents et futurs de communiquer, donc d'utiliser un langage commun (interopérabilité sémantique) et des référentiels techniques communs (interopérabilité technique).

Les spécifications et outils du cadre d'interopérabilité des systèmes d'information de santé 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[4].

Sans rentrer dans ce détail, la future recommandation sur le traitement des données de santé devra y faire référence.

Proposition n° 5

- Rendre opposable le principe de la conformité aux référentiels d'interopérabilité.

- Laisser aux Etats l'organisation de leur mise à jour.

3.2 Les référentiels de sécurité

La confidentialité des données personnelles de santé est consubstantielle au principe du secret professionnel (médical) et constitue un des principes essentiels de la protection des données à caractère personnel.

La sécurité informatique qui permet d'assurer le respect de cette confidentialité représente aujourd'hui un enjeu d'autant plus impérieux que la multiplication des échanges permet à un nombre accru de personnes d'accéder aux données. Les politiques d'habilitations et de traçabilité sont essentielles pour assurer la protection des données et empêcher qu'elles ne soient communiquées à des tiers non autorisées.

La dématérialisation des échanges dans le secteur de la santé a entrainé une modification de la nature des mesures prises pour assurer cette sécurité.

Au-delà des mesures classiques de sécurité physique et logique toujours importantes, la politique de sécurité qu'il incombe au responsable de traitement de mettre en place repose également aujourd'hui sur des référentiels de sécurité dont les pouvoirs publics doivent assurer la juste application.

Ces référentiels sont en général organisés selon leur type et leur cible d'application.

Il s'agit :

- de référentiels organisationnels définissant l'organisation de la sécurité et exposant les bonnes pratiques à destination des professionnels de santé ;
- de référentiels techniques décrivant les modalités d'authentification des patients, des acteurs de santé et l'imputabilité des documents par exemple davantage destinés aux industriels ;
- de référentiels spécifiques destinés aux responsables de traitement dans le cadre d'applications particulières comme les objets connectées ou les règles de maintenance ;
- de référentiels juridiques qui visent à informer sur la réglementation des situations d'exercice particulières.

Le fondement juridique donné à ces référentiels doit être suffisamment élevé dans la hiérarchie des

[4] Les standards internationaux les plus répandus sont les standards IHE "*Integrating the Healthcare Enterprise*"/HL7 "*Health Level Seven*" qui correspondent respectivement à la production de profils de standards existants pour répondre à de usages déterminés et au développement de standards d'interopérabilité dans le domaine de la santé. Sur le fondement de ces référentiels sont définis des formats de document médical électronique CDA "*Clinical Document Architecture*".

normes pour s'imposer mais le détail des mesures techniques doit pouvoir être adapté aux évolutions des techniques informatiques et à l'état de l'art.

- Ainsi les référentiels d'identification des acteurs apparaissent indispensables pour assurer la qualité des professionnels de santé. Le recours à des annuaires professionnels régulièrement mis à jour à partir des données certifiées par une autorité dont c'est la mission, doit être privilégié.

Il doit en être de même pour le patient dès lors que les données qui sont enregistrées et utilisées s'inscrivent dans une relation de soins et qu'il est dès lors impérieux que des données de santé ne soient pas attribuées à un mauvais patient. La nécessité d'une identification fiable et pérenne est un gage de sécurité important pour suivre le patient tout au long de son parcours de soins.

- Le développement de l'activité d'hébergement des bases de données de santé à caractère personnel impose également de s'assurer des conditions dans lesquelles ces données sont conservées et mises à disposition des utilisateurs. Des risques particuliers liés en particulier à la localisation des données, à la perte de maîtrise du système d'information et à la mutualisation des ressources doivent être donc identifiés.

Il s'agit d'organiser le dépôt et la conservation des données de santé dans des conditions de nature à garantir leur pérennité et leur confidentialité et de les mettre à la disposition des personnes autorisées.

Il appartient aux Etats de s'assurer du respect de ces principes et de mettre en œuvre les garanties nécessaires.

Proposition n° 6

- Rappeler l'importance des mesures de sécurité dans le traitement de l'information de santé.

- Rendre opposables les référentiels d'identification des acteurs, professionnels et patients.

- Organiser l'activité d'hébergement des donnés de santé.

4. Les droits de la personne

4.1 Un droit à l'information revisité par *l'empowerment*

Le respect des droits des personnes est au cœur de la protection des données personnelles. Le droit à l'information au moment du recueil des données, de leur enregistrement ou de leur communication, le droit d'accès direct aux données de santé et le droit de rectification doivent être garantis par tous les Etats à leurs citoyens.

Quelle que soit la situation d'exercice du professionnel de santé, le patient doit être informé de son état de santé et de la nature des soins qui lui sont prodigués. Cette règle, illustre les principes traditionnels d'information et de confiance qui caractérisent la relation singulière entre le médecin et plus généralement tout professionnel de santé, tenu au respect du secret, et le patient.

Le contenu de l'information doit porter sur la finalité du traitement (administration de soins, recherches, etc.), le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse, l'identité du responsable du traitement et des destinataires des données. En outre, le patient doit être informé de l'existence et des modalités d'exercice de ses droits et, le cas échéant, des transferts de données vers des pays hors Union européenne.
Toute personne doit également conserver la possibilité de s'opposer, pour des motifs légitimes, au traitement de ses données de santé. Des exceptions peuvent être prévues par les législations internes aux Etats membres dans la mesure où un autre intérêt légitime le justifie.

Dans le cadre de l'information préalable aux soins, on soulignera que la personne doit également être éclairée sur les types de techniques auxquelles il est recouru (télémédecine, hébergement dans le cloud, etc.).

Chaque professionnel de santé informe le patient, dans la limite de ses compétences et de façon adaptée, utile et pertinente au regard de son état de santé et de sa capacité de compréhension.

Les cas dans lesquels le professionnel de santé peut déroger à cette obligation d'information préalables sont limitativement énumérés et laissés à l'appréciation du professionnel lui-même : cas de l'urgence, cas dans lesquels il y a impossibilité d'informer la personne.
La volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respectée, sauf lorsque des tiers sont exposés à un risque de transmission.

Alors que le projet de règlement européen sur la protection des données en cours d'adoption consacre à travers le renforcement du droit à l'effacement des données et à la portabilité de celles-ci, quel que soit le responsable de traitement, la notion *d'empowerment*, c'est-à-dire la maîtrise par la personne de ses données à toutes les phases du cycle de vie de la donnée, cette notion revêt une dimension particulière dans le secteur de la santé.

En effet, le développement des objets connectés qui permettent aux patients d'être plus actifs dans leur prise en charge médicale donne au droit à l'information tel qu'il est présenté une nouvelle dimension.

Le responsable du traitement n'est plus le seul à détenir l'information et à en diffuser le contenu au patient. La reconnaissance du droit d'accès direct aux données médicales et la maîtrise technique qu'ont désormais certains patients, à travers les outils numériques, de leurs données rend la relation plus équilibrée.

4.2 Le recueil du consentement

Il s'agit ici de traiter du consentement au traitement des données de santé et non du consentement aux soins qui reste, sous réserve de quelques exceptions, une exigence incontournable.

Le consentement ne doit être que la traduction d'un accord à voir utiliser, partager et échanger des données de santé dans des conditions de sécurité assurées et précédé d'une information claire.

Son exigence ne doit pas masquer ou dédouaner la personne tenue de le recueillir du respect de mesures de sécurité ou de l'effort d'information qui sont la vraie protection de la personne aujourd'hui.

Les efforts ne doivent pas se concentrer de façon disproportionnée sur le recueil de ce consentement quelle que soit sa forme mais sur ce qu'il recouvre comme exigences. Si le consentement est une protection juridique il n'est pas obligatoirement une garantie éthique.

Se posent ainsi les questions de sa forme, des modalités de son recueil et des cas dans lesquels il doit être recueilli. Lorsqu'il est exigé, il doit être clair et univoque, explicite et préalable et/ou concomitant à la collecte et à l'enregistrement de l'information.

Il doit rester réversible et maîtrisé par le patient et, puisque son expression peut être aujourd'hui dématérialisée, la traçabilité des accès aux donnes de santé constitue le moyen technique du respect de ses droits et est une garantie essentielle.

Des exceptions à l'obligation du recueil du consentement, quand il est exigé, doivent être prévues et relèvent de l'appréciation du professionnel de santé. L'urgence ou l'impossibilité compte tenu de l'état du patient de recueillir son consentement peuvent être des exceptions qui peuvent être gérées par la désignation d'une personne de confiance par le patient qui se prononcera à sa place.

Proposition n° 7

- Renforcer les droits des patients sur leurs données de santé en intégrant la notion "d'empowerment".

- Limiter le recueil du consentement aux cas où le droit interne le prévoit expressément.

5. La réutilisation des données de santé

Les données de santé à caractère personnel collectées pour une finalité déterminée et légitime peuvent faire l'objet dans certains cas d'une réutilisation à d'autres fins. En général, le droit interne des pays prévoit des garanties particulières.

Il s'agit de couvrir les finalités de recherche dans le domaine de la santé sous toutes ses formes : épidémiologiques, biomédicales, statistiques, historiques etc ….

Ces ré-utilisations possibles sont essentielles à la santé publique puisque c'est à partir des résultats de ces recherches que les Etats sont en mesure d'identifier des problèmes particuliers de santé et de prendre les mesures nécessaires pour y remédier et/ou pour définir leur politique de santé.

La finalité dite secondaire des données de santé est l'amélioration de la santé publique.

Elle est traditionnellement menée à partir de recherches dans le domaine de la santé dont les modalités sont précisées par les législations nationales et soumises aux principes de protection des données personnelles.

Mais on constate aujourd'hui avec les potentialités du Big data et la démultiplication des données induites par l'usage des objets connectés, quels qu'ils soient, que les critères classiques de ré-utilisation qui se fondent sur les principes de protection des données personnelles, nécessitent d'être appréciés à l'aune de ce nouvel environnement.

Les données de santé sont produites par des sources très variées et il est important pour les chercheurs et les observateurs de pouvoir les rapprocher d'autres sources de données (environnementales, climatiques, sociales par exemple).

Les débats sur l'ouverture des bases de données conjugués aux nouvelles potentialités qu'offre le Big data doivent conduire à créer un environnement juridique favorable à l'utilisation secondaire des données de santé au bénéfice de la prévention des risques et à l'amélioration de la santé publique.

A cet égard, si les principes de protection des données de santé à caractère personnel doivent être réaffirmés, ils ne doivent pas être appliqués et/ou interprétés comme freinant une utilisation secondaire des données de santé sauf à ne pouvoir profiter de la connaissance que peut apporter tant aux acteurs économiques qu'aux pouvoirs publics, l'analyse des masses de données produites aujourd'hui.

Et sur ce point, les techniques d'anonymisation telles que définies précédemment ne sont pas suffisantes tant l'individualisation des comportements est riche d'enseignements.

Les techniques de pseudonymisation qui permettent cette individualisation et l'établissement de corrélations entre des ensembles de données doivent être favorisées, appréciées au regard des risques réels de ré-identification et ne pas être soumises par les Etats membres à des contraintes excessives.

Proposition n° 8

- Adapter au nouveau contexte de démultiplication des données de santé l'encadrement permettant une utilisation secondaire de ces données à des fins d'amélioration de la santé publique.

III- Annexes

1. Analyse des réponses au questionnaire adressé aux Etats membres

Summary of Compilation of Replies on Medical Technologies and Data Protection Issues:
Recommendation No. (97) 5 on the protection of medical data

The Consultation Committee of the Convention for the protection of individuals with regard to automatic processing of personal data issued a Questionnaire on Medical Data to the member States of the Council of Europe. The compilation of replies that has been sent to us for review is not exhaustive since it comprises a total of 36 replies some of which are incomplete (re identified by the following caption). Furthermore, only 20 States out of 47 have answered the Questionnaire, namely: Albania, Austria, Belgium, Bosnia, Croatia, Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Monaco, Norway, Poland, Portugal, Serbia, Slovakia, Macedonia, Switzerland and Uruguay. This being said, we can only assume that the following restitution is as accurate as possible and will formulate in a separate paper recommendations on that basis.

1. Mobile Health and Electronic Health Record

- Does EHR exist in your country?

	AL	AU	BE	BO	CR	ES	LA	LIT	HU	GE	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
No EHR									√			√	√					√		
Under Construction		√		√				√						√		√				
EHR	√		√		√	√	√			√	√				√		√		√	√

Few States have specific definition enshrined in dedicated health or e-health regulation. When such regulation does not exist, States rely on general data protection law. When applicable, EHR is restricted to health data.

- Are there specific mHealth regulations in your country?

There does not seem to be any m-Health regulation enacted to date in the concerned States.

- Who is granted access to EHR?

	AL	AU	BE	BO	CR	ES	LA	LIT	HU	GE	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Authorized medical staff	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√	√
Competent Authorities			√		√	√	√	√			√			√				√		√
Pharmacists (stricter access)		√	√				√			√	√			√						

More generally, the Data Controller is responsible for purpose limitation and for information security. Some States provide different levels of authorization. For instance, Croatia has 4 levels of authorizations (no access, limited access, full access, special access).

- Do you use anonymisation technique?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√	√			√	√	√		√	√	√			√					
No	√				√								√							

- How are patients identified in the EHR?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
By name and surname	√									√	√									
Identification Number		√	√			√	√	√		√	√		√		√			√		√

- How long is the data kept?

Concerning data retention, there is often no specific storage period defined for EHR. However conservation time varies depending of the type of records and methods. For instance in Albania, health records are stored 30 years, discard reports 50 years, imaging diagnostic methods 10 years, recipes pharmacies 2 years except for narcotic and psychotropic 5 years.

- Where are the records stored?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Centralized system	√					√	√						√		√	√	√	√		
Decentralized system		√	√	√					√		√	√								√

- Is the system based on an opt-in approach?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Opt-in	√		√						√		√						√		√	
Opt-out		√		√	√	√	√	√		√		√	√		√	√				√

- Are patients able to withdraw their consent?

In every State, withdrawal of consent is possible at any given moment.

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

- Is outsourcing common?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√				√		√				√		√		√	√		√	
No	√		√		√		√			√	√									

For instance, Austria uses outsourcing within the autonomy and responsibility of the health service providers as long as the storage is based in the EU. Lithuania enables outsourcing only if it is executed on legal basis of agreements.

2. Cloud computing, Data mining and Profiling

- Is your legal framework providing for a regulation of Cloud Computing?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Specific provisions		√																		

Cloud computing is not specifically regulated, except in Austria where legislation stipulates that health data which are saved by means of cloud computing have to be encrypted state-of-the-art. Most often, cloud computing is regulated by non-binding guidelines issued by National Data Protection Authority.

- Is your legal framework providing for a regulation of Data Mining?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Specific provisions						√					√									

- Is your legal framework providing for a regulation of Profiling?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Specific provisions						√					√									

Few States have implemented provisions in relation to data mining and profiling. In Italy, private entities can mine medical data obtaining the consent from data subject or using irreversibly anonymized data.

3. RFID and wireless communication technologies

- Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
No specific regulation	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√

- Is RFID applied in hospitals?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√	√		√	√													√	

RFID regulation does not seem to exist yet but are sometimes used by health professionals. For now, only guidelines from some National Data Protection Authorities have been published.

4. Applications (Mobile)

- Is your legal framework providing for a regulation of Apps and Mobile apps?

No, except in Estonia where Apps and Mobile apps with medical purpose are considered as medical devices, regulated by Medical Devices Act, there is no specific regulation for Apps in the concerned States.

- Is it allowed or do institutions use apps to gather medical data?

According to the compilation of replies, apps are used in Croatia, Italy, and Switzerland. Most often, the same rules apply as for other IT equipment's dealing with medical data.

- Is there any requirement to implement privacy by design?

Not in general. In Albania, there are requirement to implement the development of Privacy by design in medical equipment but based on the standards of the medical device (soft law).

5. Medical Devices and Wearable Devices

- Is your legal framework providing for a regulation of Medical Devices?

Not for the concerned member States. However in EU Member States due to EU regulation, all medical devices should wear CE marking of conformity.

- Does the concept of Medical device in your country encompass apps or services and apparels in the realm of eHealth and mHealth?

It appears that eHealth and mHealth devices and apps are not currently considered as medical devices and therefore are not subject to the same requirements.

There are currently no binding rules as to the difference between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. For instance, the only EU legal framework for now is the Commission's guidelines "on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices".

Examples of soft law or regulation in that field are rare. In Estonia, apps are considered as medical devices by Ministry of Social Affairs in Estonia. In Austria, identification of medical devices with bar codes is used.

6. Internet of Things

- Is your legal framework providing for a regulation of Internet of Things?

Not in the concerned member States.

7. Electronic Doctor (online Doctor) and on-line appointments

- Is your legal framework providing for a regulation of online Medical Treatment and in the on-line appointment system covered by such a framework?

Not in the concerned member States.

- Is it allowed to perform medical treatment via online services?

It is generally not allowed.

2. Récapitulatif des propositions

Proposition n° 1

- Définir de façon large la donnée de santé pour y inclure toutes les informations susceptibles de caractériser l'état de santé d'un individu, les prestations de services de santé servies ainsi que l'environnement médico-social de la personne.
- Définir les notions d'"anonymisation" et de "pseudonymisation".

Proposition n° 2

- Définir les notions d'échange et de partage des données de santé.
- Définir les termes d'urbanisation des systèmes d'information de santé.

Proposition n° 3

- Définir les termes d'hébergement/Cloud Computing.
- Définir les termes de "santé mobile" en distinguant les finalités de bien-être et de prise en charge sanitaire.

Proposition n° 4

- Rappeler les grands principes de protection des données de santé à caractère personnel tout en intégrant à travers le principe du "*privacy by design*" la notion de conformité à un cadre permettant d'adapter les finalités de collecte et de traitement des données et la détermination du ou des responsable(s) de traitement.
- Reconnaître un secret professionnel partagé entre professionnels de santé qui prennent en charge les mêmes patients.

Proposition n° 5

- Rendre opposable le principe de la conformité aux référentiels d'interopérabilité.
- Laisser aux Etats l'organisation de leur mise à jour.

Proposition n° 6

- Rappeler l'importance des mesures de sécurité dans le traitement de l'information de santé.
- Rendre opposables les référentiels d'identification des acteurs, professionnels et patients.
- Organiser l'activité d'hébergement des donnés de santé.

Proposition n° 7

- Renforcer les droits des patients sur leurs données de santé en intégrant la notion "d'empowerment".
- Limiter le recueil du consentement aux cas où le droit interne le prévoit expressément.

Proposition n° 8

- Adapter au nouveau contexte de démultiplication des données de santé l'encadrement permettant une utilisation secondaire de ces données à des fins d'amélioration de la santé publique.