EXPOSE DES MOTIFS

de la Recommandation CM/rec(2016) du Comité des ministres aux Etats membres sur la protection des données de santé

Commentaires d'ordre général sur la Recommandation

1. Le développement du numérique au cours des dernières années a conduit à une véritable « datification » de nos sociétés. Les données sont partout et constituent une matière première précieuse pour la création de nouvelles connaissances et un enjeu mondial de croissance majeur pour de nombreux pays.

2. Le secteur de la santé n'échappe pas à ces évolutions du fait d'une part de l'informatisation croissante du secteur professionnel et notamment des activités de soins et de prévention, de recherche en sciences de la vie, de gestion des systèmes de santé, et d'autre part de l'implication croissante des patients.

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

4. Les données de santé représentent donc des enjeux singuliers et un potentiel de création de valeur dont la concrétisation dépendra de la capacité des pays 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.

5. 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, des enjeux de qualité des soins, des enjeux de transparence et de démocratie sanitaire, des enjeux d'efficience des systèmes de santé dans un contexte généralisé de croissance des dépenses de santé et des enjeux d'innovation et de croissance dans des domaines aussi variés et importants que la médecine personnelle ou médecine de précision et les technologies de l'information.

6. 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 désormais bien identifié par tous les acteurs.

7. 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.

8. En effet, le développement des nouvelles technologies de l'information et de la communication dans les domaines sanitaires et médico-social conjugué aux défis rappelés

précédemment auxquels sont confrontées nos sociétés a eu un effet systémique sur les organisations et le rôle des différents acteurs du soin.

9. 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.

10. La technicité croissante des soins impose des prises en charge pluridisciplinaires et l'intervention d'un nombre croissant d'acteurs au service d'un même patient. Ces processus amènent à distinguer deux grands types de flux de données qui répondent à des exigences différentes en matière de confidentialité :
- Des flux d'*échanges* de données entre acteurs qui traduisent la dématérialisation des courriers et qui consiste, sur le modèle des messageries électroniques, à permettre à un acteur de transmettre des données de santé personnelles à un ou plusieurs autres acteurs pour une finalité bien précise et selon une diffusion maîtrisée entre émetteur et destinataires des données
- Des flux de *partage* de données qui consiste à mettre à disposition des données en règle générale sur une plateforme, données qui restent accessibles selon des règles spécifiques pour des finalités et des acteurs non nécessairement identifiés au départ sur le modèle des dossiers médicaux partagés.

11. 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.

12. Le respect du secret professionnel (médical) est au centre de cette garantie.

Commentaires détaillés sur la recommandation

Chapitre I - Dispositions générales

1. Objet de la Recommandation

13. La nouvelle Recommandation du Conseil de l'Europe destinée à actualiser et à remplacer celle de 1997 prend 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 ?

14. Cette nouvelle Recommandation tient évidemment compte également des principes du Règlement (UE) 2016/6/679 du Parlement Européen et du Conseil du 27 avril 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, en particulier le principe du *Pivacy by design* qui impose de prendre en compte la protection des données dès la conception des systèmes assurant le traitement de la donnée.

15. Elle tient compte également des résultats de l'analyse faite des questionnaires adressés aux Etats membres du Conseil de l'Europe préalablement au lancement des travaux de refonte de la Recommandation de 1997.

16. Elle concerne toute donnée de santé à caractère personnel collectée et traitée dans les secteurs publics et privés et exclut les utilisations à des fins exclusivement personnelles ou domestiques.

2. Champ d'application

17. Il est rappelé que la convention, dans son article 6, dispose que les données à caractère personnel relatives à la santé ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Selon la convention, il appartient donc aux Etats contractants de s'assurer que des garanties appropriées pour la protection des individus soient accordées dans les cas où des données relatives à la santé sont traitées dans des fichiers automatisés non couverts par la recommandation.

18. A l'instar de la convention qui ne fait pas de distinction entre les secteurs public et privé, la recommandation s'applique aux fichiers de données de santé dans les deux secteurs étant donné qu'ils doivent répondre aux mêmes exigences et qu'il y a de fréquents échanges de données entre les deux secteurs.

19. La recommandation introduit les principes de l'échange et du partage des données de santé qui recouvrent l'essentiel des modalités de communication des données et les mesures qui permettent dans ces deux cas le respect des droits des personnes et la confidentialité des données.

20. Sont exclus du champ de la recommandation les traitements de données effectués à l'initiative de la personne dans un cadre strictement personnel et domestique. C'est le cas de plus en plus fréquent lors de l'usage d'applications ou d'objets connectés dans le cadre domestique et dès lors que ces données ne sont pas collectées par un tiers mais demeurent stockées dans les équipements de la sphère domestique.

3. Définitions

21. La définition de l'expression « donnée à caractère personnel » concorde avec celle de la Convention n° 108. Il s'agit d'une définition établie de longue date qui a été réaffirmée au fil du temps dans divers instruments juridiques du Conseil de l'Europe. L'expression « donnée à caractère personnel » est définie de manière large. Elle intègre dorénavant l'utilisation courante des nouvelles technologies et des moyens de communication électronique dans les secteurs de la santé, du médico-social et du social.

22. Elle concerne toute information susceptible d'identifier directement ou indirectement une personne physique prenant ainsi en compte les techniques de pseudonymisation qui permettent aujourd'hui de "chaîner" les informations d'un même individu sans en connaître nécessairement l'identité.

23. - L'expression "*données de santé*" doit dorénavant être préférée à celle de "*données*

médicales".

24. 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 personnels sociaux.

25. La donnée de santé à caractère personnel couvre donc en particulier 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.

26. Sont également concernées les données dites médico-sociales ou sociales qui désignent toute donnée produite par des professionnels exerçant dans le secteur social et médico-social dès lors qu'elles contribuent à caractériser l'état de santé de la personne concernée. Par souci de simplification, le terme de donnée de santé à caractère personnel couvre donc également celui des données médico-sociales.

27. Les données de santé doivent donc être définies de façon plus large de telle sorte qu'une protection appropriée soit également offerte aux informations qui caractérisent la situation sanitaire de la personne dans son ensemble. La prise en charge sanitaire des patients est désormais plus globale et doit prendre en compte une dimension médico-sociale et sociale tout au long de son parcours de soins. Elle doit également intégrer toutes informations relatives aux habitudes de vie de la personne et à son bien-être dès lors qu'elles sont en rapport avec sa santé.

28. - Les données génétiques sont toutes les données relatives aux caractéristiques héréditaires d'un individu ou acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN ou de tout autre élément permettant d'obtenir des informations équivalentes.

29. - La définition de l'expression "référentiels" est justifiée par l'importance croissante que prennent ces référentiels dans le développement des systèmes d'informations de santé et des données de santé. Leur respect crée les conditions d'une interopérabilité des systèmes sans laquelle les fonctions d'échange et de partage des données sont impossibles et qui conditionnent également la sécurité des données. Certains référentiels servent de fondement aux démarches de certification et leur respect peut constituer dans certains domaines un tel enjeu qu'ils sont rendus opposables dans les droits locaux.

30. Le respect des référentiels permet de constituer un ensemble structuré d'information qui tend à constituer un cadre commun à l'ensemble des applications qui traitent des données de santé.

31. L’expression « dossier médical électronique » désigne toute forme dématérialisée de dossier médical. Les nécessités de coordination des soins d’une part et la promotion des droits des patients ainsi que leur implication croissante dans leur prise en charge dans le contexte de l’informatisation des systèmes de santé tend à substituer à une conservation éparse d’informations sous un format papier un assemblage cohérent des informations sous la forme d’un dossier en format numérique.

32. Les dossiers médicaux numériques ou électroniques peuvent être constitués et conservés par un seul professionnel de santé ou être plus ou moins partagés au sein d’équipes plus ou moins large de soignants et ainsi retracer les épisodes de santé de la personne de façon plus ou moins exhaustive.

33. L’expression « messagerie sécurisée » désigne des services de messagerie électronique compatibles avec les niveaux et référentiels de sécurité prescrits pour transporter des données de santé personnelles.

34. La définition de l'expression "droit à la portabilité " se rapporte à la portabilité des données de santé c’est-à-dire à la capacité de traiter ces données au sein de différents systèmes. Cette portabilité est une des résultantes de l’interopérabilité et du respect de référentiels. La portabilité des données apparaît comme un droit car, s’agissant de données de santé elle conditionne des notions essentielles comme la disponibilité des données ou la continuité des soins. Les soins, pour être assurés par différents acteurs utilisant des applications et des environnements informatiques différents, sont de plus en plus souvent conditionnés par la capacité à traiter des données provenant de systèmes différents. Ce droit est désormais également visé par le Règlement européen sur la protection des données personnelles dans son article 20.

35. L’expression « application mobile » renvoie à la notion de santé mobile qui se développe depuis plusieurs années dans tous les pays (les réponses apportées au questionnaire le démontrent). Elle 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.

36. Traditionnellement c’est le soin qui produit de la donnée - la visite chez le professionnel de santé alimente un dossier médical. Désormais ces dispositifs médicaux dont beaucoup mais non exclusivement sont mis en œuvre en situation de mobilité vont produire via des capteurs et des algorithmes des données qui vont-elles-mêmes impacter les soins.

37. La définition de l’expression « professionnels de santé » doit faire référence dans chaque pays à une liste de professions mais également à des listes de personnes et des dispositifs qui permettent de les identifier de façon certaine. La gestion des identités de ces professionnels du secteur sanitaire et médico-social doit être assurée de telle sorte que les citoyens puissent être certains d'être pris en charge par une communauté astreinte au secret professionnel. Ce dispositif permettra en outre de fonder l'attribution de moyens d'authentification dans les différents systèmes d'information et d’assurer une traçabilité des

accès aux données de santé personnelles.

38. Le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données de santé sur internet conduit à introduire la notion d'"hébergement de données de santé".
39. L'hébergement est devenu aujourd'hui un moyen efficace de gérer les bases de données et un passage obligé pour assurer les fonctions d'échange et de partage de ces données. Le terme de *Cloud Computing* est utilisé pour définir les différents modes de mise à disposition sur internet de ces bases : Saas (*Software as a service*), Iaas (Infrastructure as a service) et Paas (*Plate-forme as a service*).

40. La sensibilité des données de santé que ces plateformes sont appelées à héberger justifient que des conditions soient définies pour assurer aux personnes dont les données sont concernées un niveau de sécurité élevé.

41. Les expressions "anonymisation" et "pseudonymisation" désignent des procédés désormais courants appliqués aux données de santé permettant soit de couper le lien entre l'identité de la personne et les données qui la concernent, soit d'être en mesure de "chaîner" les informations de cet individu sans en connaître l'identité.

42. Les définitions retenues sont conformes à celles de l'avis du G 29 du 10 avril 2014[1] sur le sujet.

43. L'anonymisation (ou désidentification) des données à caractère personnel désigne la méthode et le résultat du traitement de données à caractère personnel dans le but d'empêcher irréversiblement l'identification de la personne concernée. D'une manière générale, il ne suffit donc pas de supprimer directement des éléments qui sont, en eux-mêmes, identifiants pour garantir que toute identification de la personne n'est plus possible. Une solution d'anonymisation efficace doit empêcher la réidentification, ce qui ne se limite pas simplement à empêcher l'individualisation (isoler un individu dans un ensemble de données, retrouver le nom et/ou l'adresse d'une personne) mais également la corrélation (relier entre eux des ensembles de données distincts concernant un même individu) et l'inférence (déduire de cet ensemble de données des informations sur un individu).

44. La pseudonymisation est une technique consistant à remplacer un attribut (généralement un attribut unique) par un autre dans un enregistrement. Le résultat de la pseudonymisation peut être indépendant de la valeur initiale (comme dans le cas d'un numéro aléatoire généré par le responsable du traitement ou d'un nom choisi par la personne concernée) ou il peut être dérivé des valeurs originales d'un attribut ou d'un ensemble d'attributs, par exemple au moyen d'une fonction de hachage ou d'un système de chiffrement. La personne physique est donc toujours susceptible d'être identifiée indirectement. Par conséquent, la pseudonymisation ne permet pas, à elle seule, de produire un ensemble de données anonymes, elle réduit le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée; à ce titre, c'est une mesure de sécurité utile, mais non une méthode d'anonymisation.

45. Au regard de la protection des données à caractère personnel, les données pseudonymisées

[1] Opinion 05/2014 on Anonymisation Technique.

restent des données à caractère personnel.

46. La multiplication des données de sources différentes relatives à un même individu et les nouvelles capacités de traitement de ces données et notamment le « data matching » modifient considérablement la notion de réversibilité de l'anonymisation des données personnelles (ré-identification). Des données considérées comme anonymes à un moment donné peuvent présenter plus tard un risque élevé de ré-identification du fait de l'apparition de nouvelles techniques ou de nouvelles sources de données, particulièrement dans un contexte marqué par le « Big Data ». Les techniques les plus sûres d'anonymisation restent l'agrégation de données qui transforment des données individuelles en données collectives. Mais ces techniques interdisent nombre de traitements ultérieurs. Il est donc souvent légitime de préserver le caractère individuel des données tout en maîtrisant le risque de ré-identification des personnes.

47. L'anonymisation (action irréversible) reste souhaitable chaque fois qu'elle est possible et aboutit à des données impersonnelles. Dans tous les autres cas les données individuelles doivent être considérées comme peudonymisées (ou indirectement nominatives) et présentent un risque plus ou moins élevé de ré-identification d'une part et de divulgation d'autre part. C'est l'évaluation de ces deux risques (ré-identification et divulgation) au regard de la sensibilité des données traitées qui doit conduire à des mesures de sécurité appropriées.

48. 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.

49. 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.

50. L'échange doit être distingué du partage de données, qui rend accessibles les informations selon un principe d'habilitations. Le partage 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. L'existence d'un dossier médical électronique en constitue un exemple.

Chapitre II
Les conditions juridiques d'utilisation des données de santé

4. Le respect des principes de protection des données à caractère personnel

51. 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.

52. 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 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.

53. La prise en compte de ces principes dès la conception des applications est aujourd'hui traduite sous le principe du *Privacy by design* et la responsabilité de sa prise en compte repose sur le responsable de l'application qui est redevable de leur respect (*notion d'accountability*).

54. 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.

55. 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 données produites et pour des finalités qu'il n'est pas toujours facile de déterminer à l'avance.

56. 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. [2] Il apparaît donc nécessaire de prévoir, 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.

57. A titre d'illustration, peut-être citée 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 produites dans une finalité de soins individuels.

58. De la même façon la notion de responsable de traitement doit prendre aujourd'hui en compte l'absence de frontières aux transferts de données et la nouvelle responsabilité indéniable des plates-formes internet dans la réalisation d'un traitement et notamment la définition des moyens mis en œuvre.

[2] "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).

59. 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*".

60. Les principes de protection des données personnelles doivent être pris en compte et intégrés dès la conception des systèmes d'information collectant, utilisant et exploitant des données de santé à caractère personnel. Le respect de ces principes doit être révisé régulièrement tout au long de la vie du traitement. Le responsable de traitement doit évaluer l'impact en termes de protection des données et de respect de la vie privée de ses applications.

61. Les droits de la personne dont les données sont collectées et traitées doivent être respectés, en particulier son droit d'accès aux données, de communication, de rectification et d'opposition

62. Le principe 4.2 relève comme l'une de ces garanties le fait qu'en principe seuls les professionnels de santé, soumis aux règles de confidentialité, devraient collecter et traiter des données de santé, ou, lorsque cela est nécessaire, des personnes agissant au nom de professionnels de santé, dans la mesure où ces personnes sont sujettes aux mêmes règles.

5. Le traitement des données de santé

63. Une fois de plus, prenant en compte la nature sensible des données médicales, le principe 4.1 rappelle les dispositions de l'article 5 de la convention: la collecte et le traitement doivent être loyaux et licites et effectués uniquement pour des finalités déterminées. Ces exigences se retrouvent dans la suite du chapitre 4.

64. Le principe de collecte loyale est rendu plus explicite au principe 5.2: les données de santé doivent, dans des conditions normales, être obtenues auprès de la personne concernée elle-même. Ce principe concerne donc la "divulgation" de ses données par la personne concernée elle-même, et non pas la "communication" des données de santé par une tierce personne (un professionnel de santé).

65. Il est évident que cette règle ne peut pas toujours s'appliquer : dans ces cas, d'autres sources d'information ne peuvent être consultées que si cela est nécessaire pour atteindre la finalité pour laquelle les données ont été traitées (un traitement médical, par exemple) ou si la personne concernée ne peut pas fournir elle-même les données. Mais dans tous les cas, la collecte de données de santé doit être conforme aux dispositions du chapitre 5, du chapitre 8 (secret médical partagé), du chapitre 9 (communication à des tiers).

66. Après les dispositions indiquant comment les données de santé devraient être collectées (principe 5.1) et auprès de qui (principe 5.2), le principe 5.3 prévoit dans quelles circonstances les données de santé peuvent être collectées et traitées. Elles peuvent être collectées si la loi le prévoit, s'il existe une obligation contractuelle qui l'impose, si la personne concernée a donné son consentement conformément au principe 12. Le principe 5.3 ne constitue pas une dérogation au principe 4.2, mais pose des conditions pour la légitimité de la collecte et du traitement.

67. Le principe 5.3 a permet également de collecter et traiter les données médicales si celles-ci sont nécessaires au respect d'engagements en raison d'un contrat, à condition toutefois que le droit interne l'autorise. Les rédacteurs de la recommandation ont considéré qu‘une obligation contractuelle ou un droit contractuel devrait pouvoir donner lieu à une collecte ou un traitement de données de santé, étant donné que le consentement de la personne concernée a déjà été acquis au moment de la conclusion du contrat.

68. Les données de santé peuvent également être collectées auprès de la personne concernée ou auprès d'autres sources si cela est prévu par la loi pour l'une des finalités énoncées dans le chapitre 5. Lors de la collecte et du traitement des données de santé, les garanties appropriées telles que décrites au chapitre 4 doivent être prévues par le droit interne. Par ailleurs, les données de santé peuvent être collectées et traitées dans la mesure où la loi l'autorise pour les finalités énoncées dans le principe 5.3.a et c, à des fins médicales préventives, diagnostiques ou thérapeutiques, ou de gestion de services de santé par les professionnels de santé incluant ceux travaillant dans le secteur social et médico-social, pour des motifs d’intérêt public comme la protection à l’égard de risques sanitaires et en matière de sécurité sanitaire et tout motif de santé publique légitime. Dès lors que la loi l’autorise, la collecte et la communication des données de santé est possible aux fins de sauvegarde des intérêts vitaux de la personne concernée, en vue de la constatation, l'exercice ou la défense d'un droit en justice, pour des motifs de recherche, pour permettre aux responsables de traitement de satisfaire à leurs obligations et exercer leurs droits ou ceux de la personne concernée dans le domaine de l’emploi et de la protection sociale dès lors que le droit interne l’autorise et prévoit les garanties appropriées.

69. Les données de santé collectées par un professionnel de santé à des fins médicales préventives ou à des fins diagnostiques ou thérapeutiques peuvent, après les soins proprement dits, également être nécessaires pour accomplir d'autres services dans l'intérêt du patient; par exemple lui fournir les médicaments indiqués, faire établir par le service administratif de l'hôpital les éléments de facturation, ou encore organiser le remboursement des frais encourus par les services de sécurité sociale. Les rédacteurs de la recommandation ont estimé que la finalité du traitement par de tels "services de santé" (qui ne couvrent pas des compagnies d'assurances agissant sur une base contractuelle) est compatible avec la finalité de la collecte de ces données de santé initialement motivées pour délivrer un soin. Par conséquent, le principe 5.3 a permet le traitement des données médicales par ces services de santé, à condition que ce traitement soit réalisé dans l'intérêt du patient.

70. De tels service de santé peuvent être gérés par le professionnel de santé qui a collecté les données de santé, ou par quelqu'un d'autre. Dans le dernier cas les données de santé nécessaires peuvent être communiquées par le professionnel de santé conformément aux principes 9.1, 9.2 et 9.3.

71. La collecte et le traitement de données de santé à des fins de constatation, d'exercice ou de défense d'un droit en justice ne peuvent intervenir qu'en présence d'un cas concret, par exemple un conflit entre un médecin et son patient au sujet d'un traitement légitimant le médecin à communiquer des données à son avocat pour le défendre lors de l'action en justice. Une collecte "en prévision de" n'est pas licite.

72. En dehors de toute disposition ou obligation juridique, les données de santé peuvent également être collectées et traitées si la personne concernée - ou son représentant légal - y

a consenti, à moins que le droit interne ne s'y oppose. Les rédacteurs de la recommandation ont été conscients du fait que, du point de vue de la protection des données de santé, le consentement de la personne concernée offre moins de garanties pour la sécurité des données que les obligations légales ou les dispositions de la loi qui, en vertu de l'article 6 de la convention, doivent être accompagnées de garanties appropriées. Au chapitre 12 de la recommandation, les conditions d'un tel consentement et les dérogations possibles sont élaborées plus amplement.

Il doit également être possible de traiter des données de santé pour des finalités non prévues initialement mais qui restent compatibles avec celles-ci et dans le respect de garanties appropriées. Cette notion de finalité compatible est également visée dans le Règlement européen sur la protection des données et constitue aujourd'hui le fondement à l'utilisation des données dans le cadre du Big Data.

6. Données relatives à l'embryon et au fœtus

(à compléter)

7. Données génétiques

(à compléter)

8. Le secret médical partagé aux fins de prise en charge et d'administration des soins

73. 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).

74. Dans ce contexte, le principe 8.1 rappel que le respect de la vie privée et le secret des informations qui les concernent reste un droit des personnes.

75. 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 notion d'équipe de soins doit être définie de telle façon qu'elle permette 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.

76. 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 technologiques de gestion des processus (mode Saas par exemple) ou de conservation (Cloud). Ce nouvel environnement informatique doit permettre la communication dans le respect des principes définis juridiquement et le respect du secret médical auquel sont astreints les professionnels de santé.

77. Le principe 8.2 introduit la notion de « secret partagé » qui permet d'échanger plus aisément des informations entre professionnels tenus au secret.

78. Reste que les données échangées et partagées entre professionnels doivent être pertinentes au regard des missions de chaque professionnel et de la situation de la personne et son intérêt.

79. Cette nécessité de communication entre professionnels tenus au secret dans l'intérêt du patient conduit à privilégier une obligation d'information de la personne sur la nature des données traitées et sur les professionnels participant à l'équipe de soins et une possibilité d'opposition de la personne concernée plutôt que l'exigence d'un consentement préalable et exprès ce que traduit le principe 8.4.

9. Communication à des tiers autorisés

80. Il est évident que les données de santé, une des catégories de données sensibles pour lesquelles la convention exige une protection spéciale, ne doivent pas être communiquées en dehors des conditions énumérées dans la présente recommandation. Cette mesure ne concerne pas les données rendues anonymes (auquel cas les données ne tombent plus dans le champ de la définition de données à caractère personnel).

81. Il existe toutefois certaines circonstances dans lesquelles des données de santé pertinentes doivent être révélées à des personnes ou organismes qui, tout en n'étant pas professionnel de santé répondant aux conditions du chapitre 8, agissent d'une autre manière dans l'intérêt immédiat de la personne (les services de sécurité sociale par exemple) ou effectuent un travail de recherche. Dans ce dernier cas, les dispositions du chapitre V s'appliquent en plus de celles du présent.

82. Le principe 9.2 rappelle que les accès aux données de santé par des tiers autorisés doit rester ponctuel et limités en fonction des raisons qui motivent cet accès. Ces accès sont limités aux autorités judiciaires, aux experts désignés par une autorité juridictionnelle ou aux agents d'une administration désignée par un texte.

83. Le principe 9.3 précise que les médecins de compagnies d'assurance et les employeurs ne peuvent être considérés comme des tiers autorisés à accéder aux données de santé des personnes. Cet éventuel accès relève le cas échéant d'un cadre contractuel consenti par la personne concernée (principe 5.3).

10. La conservation des données de santé

84. La recommandation tient compte d'une situation où les données de santé exigent une réglementation différente de celle des autres types de données. Il est indiqué au principe 10.1, que les données de santé ne doivent pas être conservées plus longtemps qu'il n'est nécessaire, l'accumulation de données de santé personnelles pendant des durées très longues rendant complexe pour les personnes l'exercice de leurs droits et serait une menace à leur vie privée.

85. Toutefois, l'intérêt de la santé publique, de la recherche médicale, ou des raisons

historiques ou statistiques, peut exiger la conservation de longue durée de données de santé, même après le décès des personnes concernées. Dans certains Etats membres, des réglementations précises visent la conservation des archives médicales. Le principe 10.2 permet la conservation prolongée des données de santé à condition que des garanties adéquates de sécurité et de protection de la vie privée soient données et que les principes de la présente recommandation soient respectées.

Chapitre III

Les droits de la personne

86. 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 aux données de santé et le droit de rectification doivent être garantis par tous les Etats à leurs citoyens.

11. Le droit à l'information

87. L'un des moyens de veiller à ce que les données médicales soient obtenues et traitées loyalement et licitement, comme le paragraphe a de l'article 5 de la convention l'exige, est d'informer la personne concernée d'un certain nombre d'éléments. Ces éléments sont énumérés au principe 5.1.

88. 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.

89. 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.

90. 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.

91. 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 …).

92. 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.

93. Les cas dans lesquels le professionnel de santé peut déroger à cette obligation d'information préalable 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. Le principe 11.4 rappelle que le soin prime sur l'information.

94. 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.

95. Alors que le Règlement européen sur la protection des données du 27 avril 2016 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.

96. 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, la collecte des données pouvant plus aisément se faire à l'insu de la personne.

97. 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.

12. Le consentement

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

104. 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.

13. Le droit d'accès, d'opposition et de portabilité

105. L'un des principes les plus importants en matière de protection des données, *confirmé dans l'article 8 de la convention*, est le droit de toute personne de connaître les informations sur elle-même enregistrées par d'autres personnes.

106. Le principe 13.1 résume, en ce qui concerne les données de santé, *les dispositions de l'article 8, paragraphes a et b, de la convention*: en règle générale, toute personne doit pouvoir avoir accès à ses données de santé et, de façon implicite, en connaître l'existence. Les exceptions à cette règle devraient être limitées au minimum. Pour cette raison, le principe 13.1 prévoit l'option de l'exercice du droit d'accès de façon indirecte (voir paragraphe suivant) ; dans ce cas, et sauf si ceci est contraire au droit interne, la personne concernée devrait le préciser et être en mesure de désigner à cette fin une personne de son choix qui devrait se voir octroyer un droit d'accès complet.

107. Comme dans le cas de l'information "individualisée", la personne concernée doit, dans la mesure du possible, pouvoir comprendre l'information à laquelle elle a accès. Cela n'implique pas que les données médicales doivent être enregistrées sous forme intelligible; souvent l'information est codifiée, par exemple pour les diagnostics. Ce qui importe, c'est que les informations soient accessibles à la personne concernée - ou à la personne de son choix - sous une forme qu'elle peut comprendre.

108. En vertu de l'article 8 de la convention, le droit d'accès à ses propres données va de pair avec le droit de la personne concernée d'obtenir, sous certaines conditions, la rectification ou l'effacement de ses données. Un des principes généraux de la protection des données est que les informations doivent être rectifiées ou effacées si elles sont erronées. Dans le secteur médical, toutefois, l'exercice de ce droit de rectification ou d'effacement peut parfois soulever des problèmes de nature spécifique et justifie le cas échéant des mesures particulières dans le droit interne.

109. Le principe 8.3 autorise donc la personne concernée à demander l'effacement de es données sous réserve des cas prévus par le droit interne de même que la personne peut s'opposer à leur collecte pour des motifs légitimes à l'exception des cas où existent des raisons légitimes et impérieuses concernant l'intérêt général.

110. Il est important de noter ici la jurisprudence de la Cour de Justice de l'Union Européenne sur le droit au déréférencement corollaire du droit à l'oubli. Un arrêt rendu par la Cour le 13 mai 2014 est venue préciser comment le droit à l'oubli, et plus particulièrement le

droit au déréférencement devait être mis en œuvre. Dans un arrêt du 13 mai 2014 *Google Spain c/ Costeja* (affaire C131/12) la Cour a, dans un premier temps, réaffirmé le droit à l'oubli de certaines informations litigieuses.

Elle précise dans un second temps que certaines informations doivent faire l'objet d'une désindexation si celle-ci est demandé par la personne physique concernée par les données. Pour faire l'objet d'un déréférencement elles doivent cependant remplir certains critères fixés par la Cour dans cet arrêt.

La Cour a tenté de concilier deux principes démocratiques essentiels qui caractérisent les libertés individuelles et publiques : le libre accès à l'information et la protection de la vie privée.

110. Comme l'article 9 de la convention, le principe 13.5 autorise des dérogations au droit d'accès aux données de santé si la loi prévoit un tel refus, une telle restriction ou un tel report. Le principe 13.5 est également inspiré par le principe général de la proportionnalité ; l'accès aux données de santé ne peut être refusé, limité ou différé que dans la mesure où cela est nécessaire.

111. Le droit d'accès peut premièrement être refusé, limité ou différé s'il s'agit d'une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'Etat, à la sûreté publique ou à la répression des infractions pénales. Les rédacteurs de la recommandation ont estimé que l'accès aux données de santé ne devrait pas être limité pour protéger les intérêts monétaires de l'Etat.

112. Deuxièmement, l'accès aux données médicales peut être refusé, limité ou différé s'il est susceptible de causer une atteinte grave à la santé physique ou mentale de la personne concernée : le paragraphe 13.5.b reconnaît "le droit de ne pas savoir". Dans ces cas, il serait néanmoins souhaitable que l'accès soit accordé dès que le risque d'atteinte a cessé d'exister.

113. Troisièmement, l'accès peut être refusé, limité ou différé s'il devait révéler des informations sur des tiers et que la protection des données à caractère personnel de ce tiers devait prévaloir sur l'intérêt de la personne concernée d'avoir accès à ses propres données médicales. Par ailleurs, les rédacteurs de la recommandation ont prévu au paragraphe c la possibilité de refuser, de limiter ou de différer l'accès aux données génétiques quand il peut porter une atteinte grave à tout membre de la lignée génétique ou à une personne qui a un lien direct avec cette lignée, par exemple un membre présumé de la famille qui se révèle ne pas être un membre de la lignée génétique, ou une personne n'étant pas présumée apparentée qui s'avère appartenir à la famille.

114. Enfin, le paragraphe d du principe 13.5 reprend la possibilité, *prévue à l'article 9, paragraphe 3, de la convention*, de restreindre le droit d'accès aux données utilisées à des fins statistiques ou de recherches scientifiques, lorsque cette restriction ne crée pas de risques d'atteinte à la vie privée des personnes concernées, par exemple lorsqu'il existe des garanties que les données ne seront pas utilisées pour prendre des décisions relatives à une personne déterminée.

Chapitre IV
Référentiels pour le traitement des données de santé

115. Les données de santé étant considérées comme sensibles, leur traitement conduit à définir certains niveau d'exigence en matière de sécurité et notamment de confidentialité. Ces exigences doivent s'inscrire autant que faire se peut dans un cadre commun qui en facilite le respect par les acteurs. Ce point motive la prise en compte de la question des référentiels dans la présente recommandation.

116. Si la divulgation des données de santé peut être préjudiciables aux personnes, la confidentialité n'est pas la seule mesure de sécurité et les questions de disponibilité des données (au moment d'un acte médical critique pas exemple), d'intégrité et d'auditabilité (dont l'imputabilité) sont tout aussi essentielles.

117. Assurer la continuité des soins délivrés par des professionnels de santé à une personne exige que l'information et donc ses données de santé soient disponibles au moment opportun et pour la bonne personne. La qualité des soins délivrés peut en dépendre et l'indisponibilité d'une donnée peut potentiellement conduire à une décision médicale inappropriée. Dès lors que le recours au numérique conduit à être mieux soigné, ces considérations techniques deviennent éthiques, la disponibilité des données et l'interopérabilité devenant des facteurs contribuant à la qualité et la sécurité des soins. Une absence de réversibilité technique qui conduirait à une perte de données peut se traduire en perte de chance pour le malade par exemple.

118. Les référentiels, qui visent à établir des cadres communs à différents systèmes, sont donc des éléments critiques s'agissant du traitement des données de santé. C'est le sens de l'introduction des chapitres 14, 15 et 16.

14. Référentiels

119. 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 notamment leur confidentialité et leur vie privée.

120. 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.

121. 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).

122. Ces référentiels sont en général organisés selon leur type et leur cible d'application.
Il peut s'agir :
- de référentiels organisationnels définissant les processus et organisations à mettre respecter et exposant les bonnes pratiques à destination des professionnels de santé et des acteurs;
- de référentiels techniques décrivant par exemple des modalités d'authentification des patients et des acteurs de santé, des niveaux de chiffrement, etc davantage destinés aux acteurs technologiques ;
- des référentiels sémantiques et d'identités des acteurs qui visent à définir des langages communs et des jeux de valeurs permettant une interprétation univoque de ces données au sein de différents

systèmes ;
- 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.

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

124. 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.

125. 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 donnés 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.

126. 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. 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.

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

15. Les référentiels d'interopérabilité

128. L'interopérabilité des systèmes d'information constitue le fondement de l'échange d'informations entre acteurs : elle favorise en effet la mise en œuvre entre différents systèmes d'information de service standardisés, en particulier des services de partage et d'échange dématérialisés des données.

129. L'interopérabilité des systèmes d'information dont dépendent le partage et l'échange des données de santé est devenue un enjeu majeur alors même qu'elle peut conditionner l'accès aux soins et leur qualité et représenter, en cas de défaillance, une perte de chance pour les personnes malades.

130. Les conditions de l'interopérabilité définies par le droit national doivent respecter les exigences de sécurité et de confidentialité des données personnelles de santé et des droits des personnes.

131. On distingue l'interopérabilité technique qui spécifie les protocoles d'interconnexion et d'acheminement de l'information et les services de partage et d'échange des données et l'interopérabilité sémantique qui concerne la syntaxe et la sémantique des données de

santé échangées ou mises en partage. Elle doit permettre notamment le traitement automatique des données au sein des applicatifs. Le principe 15.4 en énumère les principales composantes.

16. Les référentiels de sécurité

132. 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.

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

134. 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.

135. Les mesures de sécurité abordées au chapitre 16 doivent porter comme précisé aux principes 16.1 à 16.6 sur

- la disponibilité des données ce qui impose des mesures de maintenance adaptées des systèmes de façon à en garantir le bon fonctionnement dans le temps,
- l'intégrité des données qui conditionne leur fiabilité, leur cohérence et leur pertinence,
- la confidentialité qui prévient toute divulgation involontaire et réserve l'accès aux données aux seules personnes qui y sont autorisées,
- et enfin l'auditabilité c'est-à-dire la capacité d'un système à pouvoir être contrôlé et vérifié, la traçabilité des événements concernant les données en étant un des moyens essentiels.

136. La dimension technologique des systèmes d'information au sein desquels les traitements des données sont assurés peut imposer que des personnels non impliqués dans la prise en charge des personnes et non professionnels de santé accèdent à des données de santé. Ces accès doivent être ponctuels et motivés et se faire dans le respect du secret professionnel et des mesures appropriées prévues par le droit interne.

17. 17. Les services de gestion des données de santé

137. 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 terminologies communes entre professionnels.

138. 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.

139. La mise à disposition des citoyens d'un dossier médical électronique et de la garantie

d'échanges sécurisés entre acteurs du système de soins et médico-social sont aujourd'hui les deux services qui constituent le socle du partage et de l'échange des données de santé. Leurs conditions de mise en œuvre doivent respecter les conditions définies dans le présente Recommandation sur le traitement des données de santé.

ChapitreV - La recherche dans le domaine de la santé

18. La recherche dans le domaine de la santé

Recherche scientifique sur la base de données médicales

140. Le recours à des données de santé à des fins de recherche scientifique doit être effectué dans un but légitime. Les principes 18.1 et 18.2 rappellent notamment que la première mesure de protection des données de santé utilisées à des fins de recherche est l'anonymisation de ces données. La nécessité de traiter des données personnelles doit donc être appréciée au regard de la finalité de la recherche.

141. Le respect des principes posés par la présente recommandation doit conduire à veiller à ce que les données traitées soient adéquates, pertinentes et non excessives et que seules les données nécessaires aux fins de la recherche ne soient utilisées.

142. Le principe 18.3 rappelle le devoir d'information des personnes concernées par le traitement de leurs données. L'exigence d'un consentement à ce traitement relève du droit interne en excluant les cas d'urgence sanitaire.

143. Dès lors qu'il est fait usage de données de santé à caractère personnel, le droit interne doit désigner un ou plusieurs organismes en capacité d'apprécier les conditions dans lesquelles ces données sont traitées et l'intérêt de ces traitements pour la santé publique. Les questions de nature éthique ou méthodologiques relèvent de ces organismes et du droit interne et il n'a pas été jugé opportun de les aborder dans le cadre de cette recommandation.

144. S'il semble évident que la possibilité d'utiliser des données à caractère personnel pour la recherche scientifique ne signifie pas que les résultats de la recherche peuvent être publiés sous une forme permettant l'identification des personnes concernées, les rédacteurs de la recommandation ont estimé qu'il était nécessaire, en raison de la nature sensible des données de santé, de souligner cette exigence au principe 18.6.

Chapitre VI- Les dispositifs mobiles

19. Les dispositifs mobiles

145. La collecte de données personnelles en situation de mobilité se développe très rapidement sous des formes diverses et avec des finalités très différentes.

146. Qu'il s'agisse de l'utilisation de smartphones, de dispositifs médicaux connectés, de capteurs électroniques installés sur des objets et permettant de les connecter, ces outils

viennent bouleverser la frontière entre donnée de santé à caractère personnel et simple donnée de bien- être.

147. Habituellement présentées sous le vocable "Quantified Self", ces données traduisent une pratique qui consiste à se mesurer soi-même et à partager les données ainsi recueillies en utilisant les technologies de l'information. Si l'objectif poursuivi par ces systèmes n'est pas nouveau, la variété des outils utilisés pour y parvenir est quant à elle nouvelle.

148. Quels sont les critères aujourd'hui qui permettent de distinguer une donnée de santé collectée par le biais de ces outils de celle qui est collectée dans un cadre de soins et, doit-on les traiter sur le plan juridique et fonctionnel de la même façon ? S'agit-il des mêmes données ?

149. Ces questions, présentes dans tous les pays nécessitent d'être abordées dans la présente recommandation qui concerne les données de santé telles que définies précédemment c'est-à-dire très largement désormais.

150. Il semble qu'un critère assez simple qui permet de les distinguer est celui de leur usage. En effet, dès lors que les données collectées par l'intermédiaire de ces outils seraient utilisées pour administrer des soins, par exemple, pour affiner un diagnostic ou enrichir l'information nécessaire à la définition d'un traitement, alors les conditions de leur traitement doivent respecter le cadre juridique et fonctionnel applicable aux données de santé collectées et traitées dans le cadre des soins. Le principe 19.2 vient rappeler que dès lors que ces données sont susceptibles de révéler l'état de santé d'une personne, concernent sa prise en charge sanitaire ou social et/ou seraient traitées dans un contexte médical, elles répondent bien à la définition des données de santé et doivent bénéficier des principes énoncés dans la présente recommandation.

151. En revanche, dès lors qu'une donnée de santé à caractère personnel n'est pas collectée ni traitée dans le cadre d'une activité de délivrance de soins par des professionnels de santé, et qu'elle reste seulement utilisée par la personne qui la collecte, alors le cadre juridique et fonctionnel du traitement des données de santé tel que défini dans le présente recommandation ne lui serait pas applicable. Certes, des conseils peuvent être donnés à la personne concernant en particulier les précautions à prendre dès lors qu'elle partage ses informations avec d'autres, en particulier si ce partage s'effectue sur internet, par exemple il pourrait être recommandé, comme l'ont déjà fait certaines autorités de protection des données, d'utiliser un "pseudo" plutôt que sa réelle identité, mais nulle autre responsabilité que celle de la personne concernée n'est dans ce cas concernée.

152. Le principe 19.3 vise à prendre en compte ces conditions d'usage de ces données. La collecte de données au seul bénéfice de la personne qui utilise le dispositif mobile et mise en œuvre à son initiative à des fins exclusivement personnelles ne devraient donc pas être considérées comme soumises aux exigences de la présente recommandation. La collecte et la réutilisation de ces données par des acteurs tiers notamment au sein de plateformes doit faire l'objet de recommandations distinctes.

153. Au-delà du respect des règles de protection des données de santé, il conviendra également de prendre en compte certaines autres législations susceptibles de s'appliquer, comme par exemple celle sur les dispositifs médicaux.