Strasbourg, 26 March / mars 2018 T-PD(2018)11

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

(Convention 108)

PROJET D'EXPOSE DES MOTIFS

de la Recommandation CM/rec(2018) du Comité des Ministres aux Etats membres sur la protection des données relatives à la santé

Direction Générale droits de l'Homme et Etat de droit

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, conjuguant ainsi plusieurs aspects de l'autodétermination informationnelle.

3. Les phénomènes de mobilité géographique, le développement des objets connectés et des dispositifs médicaux connectés contribuent également à la croissance exponentielle du volume de données produit, le phénomène du *Big data*[1] 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 relatives à la 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 à caractère personnel.

5. Les Etats sont en effet aujourd'hui confrontés à des enjeux majeurs pour lesquels le traitement des données relatives à la santé peut jouer et joue 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. L'e-santé, c'est-à-dire l'utilisation des technologies de l'information et de la communication (TIC) 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 à laquelle le Comité des Ministres du Conseil de l'Europe avait adopté la Recommandation (97)5 du Conseil de l'Europe sur la protection des données médicales.

[1] *Big data* : le terme « mégadonnées » désigne ordinairement des ensembles de données extrêmement volumineux qui peuvent être analysés par ordinateur en vue d'en extraire des inférences statistiques sur les schémas, les tendances et les corrélations de données. Pour plus d'informations, voir les « Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées ».
https://rm.coe.int/t-pd-2017-1-lignes-directrices-big-data-fr/16806f06d1

8. En effet, le développement des TIC 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 relatives à la 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 fondées 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 la multiplication des flux de données, qu'il s'agisse de flux *d'échanges ou de partages* de données entre acteurs qui traduisent la dématérialisation des courriers et dossiers et qui consiste, sur le modèle des messageries électroniques, à permettre à un acteur de transmettre des données relatives à la santé à un ou plusieurs autres acteurs pour une finalité bien précise et selon une diffusion maîtrisée entre émetteur et destinataires des données, ou bien à mettre à disposition des données relatives à la santé, 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. Il apparait crucial de rappeler que les données relatives à la santé qui permettent d'identifier une personne sont toujours susceptibles de révéler l'intimité de la vie privée et, à ce titre, doivent continuer à bénéficier d'un statut particulier et être protégées par des règles ayant pour objectif de garantir leur confidentialité. Le respect du secret professionnel (médical) est au centre de cette garantie.

12. La Recommandation vise à permettre de faciliter la pleine application des principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE n° 108, ci-après la « Convention 108 ») à ce nouvel environnement d'échange et de partage des données relatives à la santé.

Commentaires détaillés sur la recommandation

Chapitre I - Dispositions générales

1. Objet

13. La Recommandation (2018)… est destinée à prendre en compte les évolutions récentes en matière de données relatives à la santé: 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 affaiblir les principes fondamentaux de la protection de la vie privée ?

14. La recommandation prescrit les mesures qui permettent le respect des droits des personnes et la confidentialité des données relatives à la santé faisant l'objet d'un traitement.

15. Cette nouvelle Recommandation tient évidemment également compte 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, tels que par exemple le principe de « *privacy by design »* qui impose de prendre en compte la protection des données dès la conception des systèmes assurant le traitement de la donnée, ainsi que les moyens de favoriser la portabilité des données au moyen de l'interopérabilité des systèmes.

16. 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 révision de la Recommandation de 1997.

2. Champ d'application

17. Il est rappelé que la Convention 108, dans son article 6, inclut les données à caractère personnel relatives à la santé au titre des catégories spéciales de données ne pouvant être traitées qu'avec la mise en place de garanties appropriées complémentaires. Il appartient donc aux Etats membres de s'assurer que des garanties appropriées pour la protection des personnes soient accordées dans les cas où des données relatives à la santé sont traitées.

18. A l'instar de la Convention qui ne fait pas de distinction entre les secteurs public et privé, la recommandation s'applique aux données relatives à la santé traitées dans le cadre des activités relevant des deux secteurs, y compris dans le domaine du bénévolat, étant donné qu'ils doivent répondre aux mêmes exigences et qu'il y a de fréquents échanges de données entre les deux secteurs.

19. Sont exclus du champ de la recommandation les traitements de données effectués à l'initiative de la personne dans un cadre exclusivement personnel et domestique. C'est de plus en plus fréquemment le cas 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.

20. Il convient à cet égard de préciser que l'application des principes de protection des données aux entités commerciales qui proposent des services dans le cadre d'activités exclusivement personnelles et domestiques, à partir d'applications mobiles impliquant le traitement de données relatives à la santé, pourrait faire l'objet d'un document d'orientation distinct qui viserait spécifiquement les implications liées aux traitements réalisés dans cet environnement mobile (problématiques des flux transfrontières de données notamment, qui ne sont pas traitées dans la Recommandation).

3. Définitions

21. La définition de l'expression « donnée à caractère personnel » correspond à celle de la Convention 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 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. Le « traitement de données » commence par la collecte de données relatives à la santé et englobe toutes les opérations effectuées sur les données, qu'elles le soient de façon totalement automatisée ou en partie seulement. Lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données désigne une opération ou des opérations effectuée(s) sur des données relatives à la santé au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques ou qui permettent au responsable du traitement ou à toute autre personne de rechercher, combiner ou mettre en corrélation des données relatives à une personne.

23. Les notions d'échange et de partage de données de santé peuvent caractériser aujourd'hui le traitement des données de santé.

24. L'échange correspond à 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.

25. 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 - sans que ces personnes ne soient nécessairement initialement connues - 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.

26. La définition de la « donnée personnelle » englobe 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'une même personne sans en connaître nécessairement l'identité.

27. Les expressions « anonymisation » et « pseudonymisation » désignent des procédés désormais courants appliqués aux données relatives à la 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. Le procédé d'anonymisation des données permet quant à lui de supprimer toute possibilité d'identification directe ou indirecte de la personne concernée, le risque de ré-indentification de cette dernière étant néanmoins à souligner au vu des corrélations et inférences réalisables à partir de plusieurs bases distinctes.

28. Les définitions retenues sont conformes à celles de l'avis du Groupe de l'Article 29 du 10 avril 2014[2] sur le sujet.

29. 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 ré-identification, 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).

30. 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.

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

32. La multiplication des données de sources différentes relatives à une même personne et les nouvelles capacités de traitement de ces données et notamment le « *data mining* » 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

[2] « Opinion 05/2014 on anonymisation technique ».

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.

33. 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 pseudonymisées (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.

34. 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.

35. L'expression « *données relatives à la santé* » est dorénavant préférée à celle de « *données médicales »* afin de permettre d'appliquer le dispositif protecteur à tout traitement de données à caractère personnel relatives à la santé d'une personne et de dépasser le seul cadre du monde des professions médicales, les données sensibles dont il est question étant utilisées de façon croissante en dehors de cet environnement.

36. Elle traduit un concept plus large de la donnée relative à la 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. Elle englobe le traitement d'informations relatives à la santé physique ou mentale passée, actuelle et future d'une personne, laquelle peut être malade ou bien portante.

37. La donnée relative à la santé couvre donc en particulier toute information relative à l'identification du patient dans le système de soin ou le dispositif utilisé pour collecter et traiter des données de santé, toute information obtenue lors d'un contrôle ou d'un examen médical y compris des échantillons biologiques et des données génomiques, toute information médicale : 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.

38. 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 relative à la santé couvre donc également celui des données médico-sociales.

39. Les données relatives à la 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 toute information relative aux habitudes de vie de la personne et à son bien-être dès lors qu'elles sont en rapport avec sa santé.

40. 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.

41. La notion de « responsable du traitement » désigne la personne ou l'organe qui dispose du pouvoir de décision à l'égard des finalités et moyens du traitement de données, que ce soit en vertu d'une désignation officielle ou de circonstances factuelles à apprécier au cas par cas. Par exemple, au sein d'un établissement de santé, le directeur est considéré comme responsable du traitement. Afin de déterminer si un organe ou une personne peuvent être qualifiés de responsable du traitement, une attention particulière doit être portée au fait de savoir si il ou elle détermine les motifs justifiant le traitement, à savoir ses finalités, ainsi que les moyens utilisés. La décision de recourir à tel ou tel prestataire pour participer à la mise en place des moyens nécessaires au traitement est du ressort du responsable du traitement. D'autres facteurs pertinents dans cet exercice de qualification comprennent le fait de contrôler ou non les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder. Les personnes qui ne sont pas directement subordonnées au responsable du traitement et qui effectuent le traitement pour son compte, conformément à ses instructions, sont des sous-traitants. Le responsable du traitement conserve la responsabilité du traitement lorsque ce dernier est effectué pour son compte par un sous-traitant.

42. Cette notion doit aujourd'hui prendre 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.

43. Le « sous-traitant » est toute personne physique ou morale (autre que les employés du responsable du traitement) qui accomplit les opérations de traitement pour le compte du responsable du traitement conformément à ses instructions, lesquelles définissent les limites de l'utilisation autorisée des données à caractère personnel par le sous-traitant. L'activité d'hébergement de bases de données pour le compte d'un responsable du traitement est

caractéristique d'une activité de sous-traitance, de même que l'activité de maintenance pour le compte d'un responsable du traitement.

44. 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 relatives à la 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 il participe également au renforcement de la sécurité des données. Certains référentiels servent de fondement aux démarches de certification et leur respect peut constituer dans des domaines spécifiques un tel enjeu qu'ils peuvent être rendus opposables par la législation nationale.

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

46. L'expression « applications mobiles » 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 aux applications de "msanté" ou de "*quantified self*", il apparaît nécessaire de poser certains principes d'utilisation et de traitement des données relatives à la santé par ces objets connectés dont une des caractéristiques majeures est de démultiplier la quantité de données produites.

47. 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.

48. 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 relatives à la santé.

49. Le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données relatives à la santé sur internet, de façon externalisée, conduit à introduire la notion d' « hébergement externe de données » relatives à la santé.

50. L'hébergement externalisé 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 des 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*).

51. La sensibilité des données relatives à la 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.

Chapitre II. Les conditions juridiques du traitement des données relatives à la santé

4. Principes relatifs au traitement des données

52. Il doit être rappelé que les données à caractère personnel relatives à la santé 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, du droit à la vie privée des personnes et de la confidentialité de ces informations.

53. Les principes qui commandent la protection des données personnelles tels que garantis par la Convention 108 doivent être respectés. Ils doivent être rappelés comme un cadre général et obligatoire : notamment 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 des droits des personnes concernées et de leur information.

54. Les Etats membres peuvent prévoir dans leur droit interne d'autres conditions plus strictes et protectrices des personnes concernées s'agissant par exemple du traitement des données génétiques.

55. Le principe de collecte loyale implique que les données relatives à la 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 relatives à la santé par une tierce personne (un professionnel de santé).

56. 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 relatives à la santé doit être conforme aux autres dispositions du principe 5.

57. 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, d'effacement, ainsi que la portabilité des données.

58. En tout état de cause, il appartient toujours aux autorités nationales de protection des données de s'assurer du respect de ces principes et de diffuser toutes

recommandations de nature à faire respecter le principe de « *privacy by design* ».

59. Les principes de protection des données personnelles doivent être pris en compte et intégrés dès la conception des systèmes d'information traitant 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 du traitement doit évaluer l'impact de ses applications en termes de protection des données et de respect du droit à la vie privée.

60. L'obligation faite au responsable du traitement d'assurer une protection adéquate des données relatives à la santé est liée à la responsabilité de vérifier et d'être en mesure de démontrer que le traitement de données est conforme au droit en vigueur. Parmi les mesures appropriées que le responsable du traitement et le sous-traitant peuvent avoir à prendre afin d'être en conformité figurent : la formation des employés, la mise en place de procédures appropriées de notification (indiquant par exemple quand des données doivent être effacées du système), l'établissement de clauses contractuelles particulières en cas de délégation du traitement, la nomination de délégués à la protection des données, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité.

61. En principe seuls les professionnels de santé, soumis aux règles de confidentialité, devraient collecter et traiter des données relatives à la 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. Bases légitimes du traitement des données relatives à la santé

62. Conformément au principe de licéité du traitement, les conditions de la légitimité du traitement doivent être établies clairement et les circonstances dans lesquelles les données relatives à la santé peuvent être traitées sont à ce titre énumérées.

63. Les données relatives à la santé peuvent être traitées si la loi le prévoit, s'il existe une obligation contractuelle qui l'impose, si la personne concernée a donné son consentement et en tout état de cause, que les garanties définies au principe 4 sont respectées.

64. Les données relatives à la santé peuvent être traitées, dans la mesure où la loi le prévoit, à des fins de médecine préventive, diagnostique ou thérapeutique, ou de gestion de services de santé par les professionnels de santé incluant ceux travaillant dans le secteur social et médico-social.

65. Les données relatives à la santé traitées 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 motivée pour délivrer un soin. Par conséquent, le traitement des données relatives à la santé par ces services de santé est admis, à condition que ce traitement soit réalisé dans l'intérêt du patient.

66. De tels services de santé peuvent être gérés par le professionnel de santé qui a collecté les données relatives à la santé, ou par quelqu'un d'autre. Dans le dernier cas les données relatives à la santé nécessaires peuvent être communiquées par le professionnel de santé conformément au principe 9.

67. Les données relatives à la santé peuvent également être traitées, lorsque cela est prévu par la loi, pour des motifs de santé publique, comme la protection à l'égard de risques sanitaires et en matière de sécurité sanitaire.

68. S'il apparaît encore nécessaire de lister les différentes finalités pour lesquelles les données relatives à la santé peuvent être collectées et traitées, il convient aussi de prendre en compte le fait que les avancées technologiques démultiplient le volume des données produites et pour des finalités qu'il n'est pas toujours facile de déterminer à l'avance.

69. Les principes traditionnels de protection des données ne sont pas toujours aisément applicables à ce phénomène de « *datification* », le Big Data en constituant un exemple concret. Il apparaît donc nécessaire de prévoir, à côté des finalités classiques de traitement des données relatives à la santé, la capacité des Etats à prévoir un usage de ces données.

70. 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. Il doit être possible de traiter des données relatives à la santé pour des finalités non prévues initialement mais qui restent compatibles avec celles-ci et dans le respect de garanties appropriées.

71. Dès lors que la loi le prévoit, le traitement des données relatives à la santé est possible aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne. Il existe en effet des cas dans lesquels le consentement ne de la personne ne pourra être recueilli, en raison d'une urgence ou de l'impossibilité de le faire compte tenu de l'état de la personne.

72. Les données relatives à la santé peuvent également être traitées, lorsque cela est prévu par la loi, pour des motifs d'intérêt public en matière de gestion des demandes de prestations et de services de protection sociale et d'assurance maladie. La prise en charge financière de dépenses de maladie implique le traitement de données relatives à la santé par les organismes d'assurance maladie.

73. Les données relatives à la santé peuvent également être traitées, lorsque cela est prévu par la loi et dans les conditions établies par celle-ci, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Les traitements mis en œuvre par des instituts de recherche médicale ou à des fins statistiques pour évaluer le niveau de santé d'une population ou la prévalence de pathologies à des fins épidémiologiques relèvent de ces finalités. Il en est de même de la conduite d'essais cliniques visant à mettre sur le marché de nouvelles molécules.

74. Dès lors que la loi le prévoit et dans le respect des garanties appropriées pertinentes, le traitement des données relatives à la santé est possible pour permettre aux responsables du 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. Les services de médecine du travail peuvent en effet collecter et traiter les données relatives à la santé nécessaires pour apprécier l'aptitude ou l'inaptitude à l'emploi de personnels. Des garanties appropriées doivent être toutefois prises pour éviter de transmettre aux employeurs les données relatives à la santé.

75. Le traitement de données relatives à la santé à des fins de constatation, d'exercice ou de défense d'un droit en justice ne peut 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.

76. Les données relatives à la santé peuvent également être traitées, lorsque cela est prévu par la loi, pour des motifs d'intérêt public important. La surveillance de certaines maladies infectieuses transmissibles peut justifier la collecte de données de santé de façon obligatoire au nom de l'intérêt de la santé publique.

77. En dehors de toute disposition ou obligation juridique, les données relatives à la santé peuvent également être 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 relatives à la santé, le consentement de la personne concernée offre moins de garanties 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. Aussi, les conditions d'un tel consentement et les dérogations possibles sont d'une grande importance.

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

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

80. Son exigence ne doit pas masquer ou dédouaner la personne tenue de le

recueillir du respect de mesures de sécurité ou de la nécessité d'information, qui sont la vraie protection de la personne aujourd'hui.

81. 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.

82. 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 libre, spécifique, éclairé et explicite. Il doit préalable et/ou concomitant à la collecte et à l'enregistrement de l'information.

83. Il doit rester réversible et maîtrisé par la personne concernée 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. Il convient en effet de souligner que si le consentement peut être exprimé par voie électronique, il convient alors que des mesures de sécurité et d'authentification robustes soient en place.

84. Lorsque l'on envisage de traiter des données de santé concernant une personne légalement incapable qui n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne permet pas à la personne concernée d'agir en son propre nom, le consentement de la personne pouvant agir légalement au nom de la personne concernée, ou d'une autorité, ou de toute personne ou instance désignée par la loi, est requis.

85. Si la personne légalement incapable a été informée de l'intention de traiter ses données relatives à la santé, son souhait devrait être pris en considération, à moins que le droit interne ne s'y oppose.

86. Enfin, le principe 5 permet de traiter les données relatives à la santé si celles-ci sont nécessaires au respect d'engagements en raison d'un contrat (par exemple le contrat entre un hôpital et un groupe industriel chargé de l'hébergement des données dès lors que des garanties appropriées sont prises pour ne pas modifier les données), à condition toutefois que des garanties appropriées soient prévues. Les rédacteurs de la recommandation ont considéré qu'une obligation contractuelle ou un droit contractuel devrait pouvoir donner lieu à un traitement des données relatives à la santé, étant donné que le consentement de la personne concernée a déjà été acquis au moment de la conclusion du contrat.