COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 24 mai 2016 T-PD(2016)04rev

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)

PROJET DE RECOMMANDATION EN MATIERE DE PROTECTION DES DONNEES DE SANTE

Direction Générale Droits de l'Homme et Etat de droit

Recommandation CM/Rec(2016)…. du Comité des Ministres aux Etats membres en matière de protection des données de santé *(adoptée par le Comité des Ministres … 2016, lors de la … réunion des Délégués des Ministres).*

Les Etats sont aujourd'hui confrontés à des enjeux majeurs liés au traitement de la donnée de santé, dont l'environnement a, depuis l'adoption de la Recommandation n° R (97) 5 relative à la protection des données médicales, considérablement évolué.

Cette évolution est due au phénomène de dématérialisation de la donnée rendu possible par l'informatisation du secteur de la santé et à la multiplication des échanges du fait du développement d'internet.

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

En outre, les phénomènes de mobilité, le développement des objets et dispositifs médicaux connectés contribuent à de nouveaux usages et à la production d'un volume rapidement croissant de données.

Ce constat partagé par les Etats membres conduit à proposer une nouvelle rédaction de la Recommandation n° R (97) 5 relative à la protection des données médicales, terme auquel on préfèrera le terme plus général de « données de santé », en réaffirmant le caractère sensible des données de santé et l'importance d'encadrer leur utilisation afin de garantir un usage respectant les droits et libertés fondamentales de l'individu notamment le droit au respect de la vie privée.

Le Comité des Ministres, conformément à l'article 15.*b* du Statut du Conseil de l'Europe, recommande aux Etats membres :

– d'assurer que les principes contenus dans l'annexe de la présente recommandation, qui remplace la Recommandation N° R (97) 5 susmentionnée, sont reflétés dans la mise en œuvre des législations nationales relatives à la protection des données de santé, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données de santé ;
– d'assurer, à cette fin, que la présente recommandation et son annexe sont portées à l'attention des autorités établies conformément à la législation nationale en matière de protection de données et chargées de contrôler l'application de cette législation, ainsi que des autorités en charge des systèmes de santé ;
– de promouvoir l'acceptation et l'application des principes contenus dans l'annexe de la présente recommandation, au moyen d'instruments complémentaires, tels que des codes de conduite, en s'assurant que ces principes sont bien connus, compris et mis en application par tous les intervenants du secteur de la santé, et pris en compte dans la conception, le déploiement et l'utilisation des TIC dans ce secteur.

Annexe à la Recommandation CM/Rec(2016)…

Chapitre I
Dispositions générales

1. Objet

La présente Recommandation a pour objet de fournir aux Etats membres des orientations en vue d'encadrer l'utilisation et les différents usages des données de santé afin de garantir

le respect des droits et libertés fondamentales de toute personne physique notamment le droit à la vie privée. Elle fournit également les lignes directrices d'un développement de systèmes d'information interopérables et sécurisés permettant d'accroitre la qualité des soins et l'efficience des systèmes de santé.

2. Champ d'application

La présente recommandation est applicable au traitement de données à caractère personnel relatives à la santé (données de santé) dans les secteurs publics et privés.

Elle définit également les principes de l'échange et du partage des données de santé à l'aide des outils numériques respectueux des droits de la personne et de la confidentialité des données.

Les dispositions de la présente Recommandation ne s'appliquent pas au traitement de données de santé effectué par une personne dans le cadre d'activités exclusivement personnelles ou domestiques.

3. Définitions

Aux fins de la présente recommandation, les expressions suivantes sont définies ainsi :

- L'expression « donnée à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais ou des activités déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes.

- L'expression "données de santé" recouvre toutes données susceptibles de révéler l'état de santé de la personne en relation avec son état physique et/ou mental passé, présent ou futur quelle que soit leur source. Elle concerne également toute information relative à sa prise en charge sanitaire et sociale. Il peut s'agir par ailleurs d'informations de nature biologique et génétique. Sont en outre concernées les données relevant du bien-être et/ou des habitudes de vie dès lors qu'elles révèlent un état de santé.

- L'expression « données génétiques » se réfère à toute donnée relative aux caractéristiques génétiques d'un individu soit héritées soit 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.

- L'expression "référentiels" désigne un ensemble coordonné de règles et/ou de processus maintenu à l'état de l'art et applicable aux systèmes d'information de santé et qui recouvre les domaines de l'identification, de l'interopérabilité et de la sécurité.

- L'expression "dossier médical électronique" désigne un ensemble sécurisé, structuré ou non, de données de santé d'une même personne qui l'accompagne tout au long de son parcours de soins. Il permet au patient et aux professionnels de santé autorisés de partager les informations utiles à la coordination des soins.

- L'expression "messagerie sécurisée" désigne un service permettant d'échanger de façon sécurisée des données de santé à caractère personnel entre personnes identifiées.

- L'expression "droit à la portabilité " désigne le droit pour les personnes concernées de recevoir les données les concernant confiées à un responsable du traitement, dans un format structuré, et couramment utilisé et de les transmettre, le cas échéant, à un autre

responsable du traitement.

- L'expression "applications mobiles" désigne un ensemble de moyens accessibles en mobilité permettant de communiquer et de gérer des données de santé à distance. Elle recouvre des formes diverses comme les objets connectés et les dispositifs médicaux.

- L'expression"professionnels de santé" recouvre tout professionnel reconnu comme tel par le droit national et le droit de l'Union européenne, exerçant dans le secteur sanitaire, médico-social ou social, astreint au secret professionnel et participant à la coordination des soins d'une personne qu'il prend en charge.

- L'expression "hébergement de données de santé" désigne le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données de santé sur internet.

- L'expression "anonymisation" désigne le procédé appliqué aux données de santé pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement. L'anonymisation est irréversible.

- L'expression "pseudonymisation" désigne une technique qui permet de rendre une donnée non identifiante aussi longtemps qu'elle n'est pas associée à d'autres éléments conservés séparément et qui permettraient une identification.

- Les notions d'échange et de partage de données de santé qui peuvent caractériser le traitement des données de santé sont définies de la façon suivante. L'échange de données correspond à la communication d'informations à un (des) destinataire(s) clairement identifié(s) par un émetteur connu. Le partage de données permet de mettre des données à la disposition de plusieurs personnes fondées à en connaître selon des principes de droit d'accès sans que ces personnes ne soient nécessairement initialement connues.

- Le terme "communication" signifie toute opération de traitement et notamment l'échange ou le partage de données à caractère personnel permettant de rendre accessibles à des personnes autorisées des données à caractère personnel, quels que soient les moyens ou les supports utilisés.

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

4. Le respect des principes de protection des données à caractère personnel dès la conception (*privacy by design*)

4.1 La personne qui traite des données de santé doit respecter les principes suivants :

a. Le traitement des données doit être proportionné à la finalité légitime poursuivie et ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi.

b. Les données à caractère personnel doivent être traitées licitement, de façon loyale. Elles doivent être collectées pour des finalités explicites, déterminées et légitimes et ne doivent pas être traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques est compatible avec ces fins, à condition que des garanties complémentaires s'appliquent.

c. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ; elles doivent être exactes et si

nécessaire mises à jour.

d. Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

e. Des mesures de sécurité appropriées doivent être mises en place pour empêcher les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation à des tiers non autorisés.

f. 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.

4.2 Le traitement de données de santé n'est autorisé que dans la mesure où des garanties spécifiques et appropriées sont prévues par le droit interne afin de prévenir les risques que leur traitement peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.

4.3 Les finalités pour lesquelles les données de santé sont traitées doivent également être prises en compte pour permettre un usage pertinent de ces données et adapter en conséquence les garanties.

4.4 En principe, les données de santé doivent être collectées et traitées par des professionnels de santé, des organismes agissant sous la responsabilité de professionnels de santé ou par les personnes concernées elles-mêmes. Les responsables du traitement et leurs sous-traitants qui ne sont pas des professionnels de santé ne devraient collecter et traiter des données de santé que dans le respect de règles de confidentialité et de mesures de sécurité comparables à celles incombant à un professionnel de santé.

4.5 Ces 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. Le respect de ces principes doit être réexaminé régulièrement tout au long de la vie du traitement. Le responsable du traitement doit évaluer l'impact en termes de protection des données et de respect de la vie privée de ses applications.

4.6 Le responsable du traitement doit prendre toutes les mesures appropriées afin de se conformer à ses obligations en matière de protection des données personnelles et doit être en mesure de démontrer en particulier à l'autorité de contrôle compétente que le traitement dont il est responsable est en conformité avec de telles obligations.

5. Le traitement des données de santé

5.1 Le traitement des données de santé doit être effectué de manière loyale et licite et uniquement pour des finalités déterminées.

5.2 Les données de santé doivent en principe être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 5, 6, 7, 9 et 12 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données.

5.3 Les données de santé peuvent être traitées et communiquées :

a. si la loi le prévoit ou si le traitement repose sur un contrat avec un professionnel de la

santé prévoyant des garanties appropriées :

i. aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de gestion de services de santé par les professionnels de santé et du secteur social et médico-social ;
ii. pour des motifs d'intérêt public dans le domaine de la santé publique comme par exemple, la protection à l'égard de risques sanitaires internationaux ou pour assurer un haut niveau de qualité et de sécurité aux traitements médicaux, produits de santé et dispositifs médicaux ;
iii. pour des motifs d'intérêt général dans le domaine de la gestion des demandes de prestations et de services de protection sociale et d'assurance maladie ;
iv. pour des motifs de santé publique dès lors qu'ils sont licites, légitimes et sont compatibles avec la finalité initiale de collecte des données ;

b. si la personne concernée a donné son consentement conformément au principe 12 de la présente recommandation, sauf dans les cas où le droit interne prévoit qu'une interdiction de traiter les données de santé ne peut être levée par le seul consentement de la personne concernée ;

c. dans la mesure où la loi l'autorise :
   i. aux fins de sauvegarde des intérêts vitaux de la personne ou d'une personne incapable physiquement ou légalement d'exprimer son consentement ;
   ii. pour des motifs tenant aux obligations des responsables du traitement et à l'exercice de leurs droits ou de ceux de la personne concernée dans le domaine de l'emploi et de la protection sociale, dans le respect des règles du droit interne ou de tout accord collectif respectueux de ce dernier et prévoyant des garanties appropriées ;
   iii. pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice
   iv. pour des motifs tenant à la recherche dans le domaine de la santé et du secteur médico-social ;
   v. pour des traitements à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions définies par le droit interne pour garantir la protection des intérêts légitimes de la personne et dès lors que le résultat ne permet pas d'identifier la personne.

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

6. Données relatives à l'embryon et au fœtus

6.1 Les données médicales relatives à l'embryon et au fœtus, telles que notamment les données résultant d'un diagnostic préimplantatoire, devraient être considérées comme des données à caractère personnel et jouir d'une protection comparable à celle des données de santé d'un mineur.

6.2 A moins que le droit interne n'en dispose autrement, le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir en tant que personne concernée.

7. Données génétiques

7.1 Les données génétiques traitées à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou d'une tierce personne (tests

génétiques sur des incapables au bénéfice de membres de leur famille par exemple) ou pour la recherche scientifique ne devraient être utilisées qu'à ces seules fins ou pour permettre à la personne concernée de prendre une décision libre et éclairée à leur sujet.

7.2 Le traitement des données génétiques pour les besoins d'une procédure judiciaire ou d'une enquête pénale devrait faire l'objet d'une loi spécifique offrant des garanties appropriées. Ces données devraient servir exclusivement à la vérification de l'existence d'un lien génétique dans le cadre de l'administration de la preuve, à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. En aucun cas elles ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

7.3 Tout traitement des données génétiques à d'autres fins que celles prévues aux points 7.1 et 7.2 devrait être autorisé par la loi, en particulier dans les cas où il s'agit de prévenir un préjudice sérieux pour la santé de la personne concernée ou de tiers. En aucun cas, les données génétiques ne peuvent donner lieu à une exploitation commerciale. Le traitement des données génétiques en vue de dépister des maladies peut être autorisé dans l'intérêt vital et dès lors qu'il existe des garanties appropriées définies par la loi.

7.4 La publication de données génétiques permettant d'identifier la personne concernée, un parent consanguin ou utérin de la personne concernée, un membre de sa famille sociale, ou une personne ayant un lien direct avec la lignée génétique de la personne concernée devrait être interdite.

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

8.1 Toute personne a droit à la protection de ses données de santé. Dans le cadre de ses relations avec un professionnel de santé, médico-social et social, la personne prise en charge a droit au respect de sa vie privée et au secret des informations la concernant.

8.2 La nécessité d'une plus grande coordination entre professionnels intervenant dans le secteur sanitaire, médico-social et social doit conduire le droit interne de chacun des Etats membres à reconnaitre un secret professionnel partagé entre des professionnels eux-mêmes astreints au secret professionnel par la loi.

8.3. L'échange et le partage de données de santé entre professionnels de santé doivent être limités aux informations strictement nécessaires à la coordination ou la continuité des soins, à la prévention ou au suivi médico-social et social de la personne, chacun ne pouvant transmettre ou recevoir que les données qui relèvent strictement du périmètre de ses missions.

8.4 La personne concernée doit être informée préalablement de la nature des données collectées et traitées et des professionnels de santé participant à l'équipe de soins. Elle doit pouvoir à tout moment s'opposer à l'échange et au partage de ses données de santé.

9. Communication à des tiers autorisés

9.1 Les données de santé ne doivent pas être communiquées, sauf dans les conditions énumérées dans le cadre de la présente Recommandation.

9.2 Elles peuvent être communiquées à des tiers autorisés par le droit interne à obtenir un accès ponctuel et limité aux données. Il peut s'agir des autorités judiciaires, des experts désignés par une autorité juridictionnelle ou des agents d'une administration désignés par

un texte.

9.3 Les médecins de compagnies d'assurance et les employeurs ne peuvent être considérés comme des tiers autorisés à accéder aux données de santé des patients.

10. La conservation des données de santé

10.1 Les données de santé ne doivent être conservées que pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Le droit interne peut prévoir des durées de conservation précises tenant compte de la nature du support de conservation des données de santé.

10.2 La conservation de données de santé pour des finalités différentes de celles pour lesquelles elles ont été initialement collectées, doit être réalisée dans le respect des principes de la présente Recommandation.

10.3 La personne concernée peut elle-même demander la suppression de ses données à moins qu'elles ne soient rendues anonymes de façon irréversible ou que des intérêts légitimes s'y opposent.

Chapitre III
Les droits de la personne

11. Le droit à l'information

11.1 Toute personne doit être informée de la collecte et du traitement de ses données de santé.

Elle devrait être informée :

- de l'identité et des coordonnées du responsable du traitement et, le cas échéant, de celle de ses sous-traitants,
- de la finalité du traitement des données et de l'existence, le cas échéant, de son fondement légal,
- de la durée de conservation de ses données,
- des destinataires des données et des transferts de données prévus vers un pays tiers,
- de la possibilité de refuser le traitement de ses données ou de revenir sur son accord initial et des conséquences qui s'y attachent,
- de la possibilité de traiter ultérieurement ses données pour une finalité compatible dans le respect de garanties appropriées prévues par le droit interne,
- des techniques particulières utilisées pour traiter ses données de santé,
- des conditions et des moyens mis à sa disposition pour exercer auprès du responsable du traitement ses droits d'accès, de rectification et de suppression de ses données de santé et de la possibilité de s'opposer à leur traitement.

11.2 Cette information doit être réalisée au moment de la collecte des données ou lors de la première communication à moins que cette information se révèle impossible ou exige des efforts disproportionnés. Elle doit être appropriée et adaptée aux circonstances. En particulier, lorsque la personne est dans l'incapacité physique ou juridique de recevoir cette information, celle-ci pourra être donnée à la personne qui la représente légalement. Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient traitées.

11.3 L'information de la personne concernée peut être limitée, si la dérogation est prévue

par la loi et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique :

- à la prévention d'un danger concret ou à la répression d'une infraction pénale,
- pour des raisons de santé publique,
- pour protéger la personne et les droits et libertés des tiers.

11.4 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. En cas d'urgence médicale, lorsque la vie de la personne est en jeu, les soins priment sur l'information.

11.5 Le droit interne doit prévoir les garanties appropriées de nature à assurer le respect de ces droits.

12. Le consentement

12.1 Lorsque la personne concernée est appelée à donner son consentement au traitement de données de santé, celui-ci devrait être libre, spécifique, éclairé et explicite. Son recueil dès lors qu'il est dématérialisé doit être tracé. Il n'exonère pas celui qui le recueille de ses obligations d'information préalable.

12.2 Les résultats des analyses génétiques devraient être formulés dans les limites des objectifs de la consultation médicale, du diagnostic ou du traitement pour lesquels le consentement a été obtenu.

12.3 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.

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

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

13.1 Toute personne doit pouvoir accéder à ses données de santé directement auprès de la personne qui les détient.

13.2 Le droit d'accès qui emporte le droit de communication des informations, également sur support papier, permet à la personne d'exercer son droit de rectification et d'effacement. Il emporte avec lui le droit de recevoir les données dans un format structuré qui permette de transmettre les données à un autre responsable de traitement désigné par la personne dont les données sont concernées.

13.3 Le droit à l'effacement s'exerce sous réserve des cas prévus par le droit interne invoquant des motifs légitimes. La personne a le droit de s'opposer pour des motifs légitimes à la collecte de ses données de santé à caractère personnel sauf lorsque le détenteur des données invoque une raison impérieuse et légitime qui concerne l'intérêt général de la santé publique.

13.4 En cas de refus de rectifier ou d'effacer les données ou en cas de rejet de l'opposition de la personne concernée, celle-ci doit pouvoir faire recours.

13.5 L'accès aux données de santé peut être refusé, limité ou différé uniquement si la loi le prévoit, et :

a. si cela constitue une mesure nécessaire et appropriée dans une société démocratique à la protection la sécurité nationale, à la sûreté publique, à la prévention, à l'investigation ou à la répression des infractions pénales ; ou
b. si la connaissance de ces informations est susceptible de causer une atteinte grave à la santé de la personne concernée ; ou
c. si l'information sur la personne révèle également des informations sur des tiers, ou, en ce qui concerne les données génétiques, si ces informations sont susceptibles de porter une atteinte grave à des parents consanguins ou utérins, ou à une personne ayant un lien direct avec cette lignée génétique ; ou
d. si les données sont utilisées à des fins de recherche scientifique ou à des fins statistiques et qu'il n'existe aucun risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées, notamment du fait que les données ne sont pas utilisées pour des décisions ou des mesures relatives à une personne déterminée.

13.6 La personne soumise à une analyse génétique devrait être informée des découvertes inattendues si les conditions suivantes ont été remplies :

a. le droit interne n'interdit pas une telle information ;
b. la personne a fait la demande explicite de cette information ;
c. l'information n'est pas susceptible de porter une atteinte grave :
    i. à la santé de la personne ; ou
    ii. à un parent consanguin ou utérin de la personne, à un membre de sa famille sociale, ou à une personne ayant un lien direct avec la lignée génétique de la personne, à moins que le droit interne ne prévoie d'autres garanties appropriées.

Sous réserve du droit interne, la personne devrait également être informée si ces découvertes revêtent pour elle une importance thérapeutique ou préventive directe.

Chapitre IV
Référentiels pour le traitement des données de santé

Le traitement des données de santé doit conduire chaque acteur à un niveau d'exigence élevé pour assurer la confidentialité des données de santé particulièrement sensibles.
Les usages qui peuvent en être faits et leur divulgation volontaire ou non exposent les personnes à des préjudices particulièrement importants. Les questions de disponibilité des données (au moment d'un acte médical critique pas exemple), d'intégrité et d'auditabilité (dont l'imputabilité) sont par ailleurs tout aussi essentielles.

Dès lors que le recours au numérique conduit à être mieux soigné, ces considérations techniques deviennent éthiques, la disponibilité des données et l'interopérabilité rejoignant la notion de continuité des soins et d'égalité, une absence de réversibilité technique pouvant se traduire en perte de chance pour le malade par exemple.

14. Référentiels

14.1 Conformément au principe de *privacy by design* tel que défini au point 4.5, les applications qui gèrent des données de santé doivent intégrer dès leur conception les principes de protection des données personnelles et les référentiels de sécurité et d'interopérabilité et s'assurer de la conformité de leur traitement à ces principes et référentiels.

14.2 Ces référentiels ont pour objet, en fonction des usages, de définir de façon coordonnée avec les acteurs les conditions d'usages des données de santé dans les systèmes d'information afin d'assurer leur confidentialité et leur interopérabilité. Ils recouvrent les domaines de l'identification, de l'interopérabilité et de la sécurité.

15. Les référentiels d'interopérabilité

15.1 Ces référentiels spécifient les standards à utiliser dans les échanges et lors du partage des données de santé entre systèmes d'information de telle façon qu'un produit ou un système informatique puisse fonctionner avec d'autres produits ou systèmes existants ou futurs. Ils impliquent l'utilisation d'un langage commun (interopérabilité sémantique) et des référentiels techniques (interopérabilité technique) communs.

15.2 Pour garantir aux personnes concernées le respect de leurs droits et permettre le développement de systèmes d'information efficients, les professionnels de santé et les patients ainsi que tout organisme autorisé à traiter des données de santé, notamment les personnes responsables des plateformes permettant l'échange et le partage des données de santé, doivent respecter des règles de sécurité et des référentiels auxquels le droit interne de chaque pays peut donner une force juridique par exemple en recourant à un procédé de certification et qui doit conduire à leur acceptabilité par l'ensemble des acteurs. Leur respect doit en particulier être assuré, dès lors que les données de santé sont collectées et traitées dans le cadre des relations de prise en charge et de soins.

15.3 Ces référentiels ont pour objet de définir des standards permettant l'échange et le partage des données de santé par les systèmes d'information et d'assurer le suivi de leur mise en œuvre dans des conditions de sécurité requises.

15.4 Ils sont fondés sur les principes suivants :

a. utiliser un langage et des formats communs de contenus partagés ou échangés fondés sur des standards communs (interopérabilité sémantique) ;

b. recourir à des services interopérables et à des règles d'utilisation communes ;

c. utiliser pour le transport des données, des protocoles d'interconnexion et d'acheminement de l'information sécurisés ;

d. garantir aux personnes concernées une identification fiable afin d'assurer l'unicité de leur identité au sein des différents systèmes d'information. L'identifiant retenu doit être unique, univoque, pérenne et reconnu par l'ensemble des acteurs et fondé sur un dispositif de certification fiable ;

e. assurer l'authentification des personnes et des systèmes qui interviennent dans le traitement des données à l'aide de dispositifs reconnus par l'ensemble des acteurs et de nature à garantir la sécurité de l'échange et du partage des données ;

f. utiliser des solutions sécurisées telles que définies au Principe 16.

16. Les référentiels de sécurité

16.1 Le traitement des données de santé doit être sécurisé et recourir à des solutions qui garantissent la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données.

16.2 Ces règles de sécurité, maintenues à l'état de l'art, doivent se traduire par l'adoption de

mesures techniques et organisationnelles de nature à protéger les données de santé contre toute destruction illégale ou accidentelle, toute perte, toute altération et de prévenir tout accès non autorisé. En particulier, le droit interne doit prévoir d'organiser et d'encadrer les modalités de collecte, de conservation et de restitution des données de santé.

16.3 La disponibilité - c'est-à-dire le bon fonctionnement du système - doit être assurée par des mesures de nature à rendre accessibles les données de façon sécurisée et dans le respect des habilitations de chacun.

16.4 Le respect de l'intégrité impose de vérifier toute action effectuée sur la nature des données, leur modification éventuelle et leur effacement, y compris lors de la communication des données.

16.5 La confidentialité des données se traduit par la mise en place de mesures destinées à contrôler les accès aux serveurs de données et aux données elles-mêmes en s'assurant que seules les personnes autorisées puissent accéder aux données.

16.6 L'auditabilité doit conduire à disposer d'un système permettant de tracer tous les accès au système d'information et de pouvoir imputer à une personne les actions qu'elle a effectuées.

16.7 L'activité qui consiste à conserver sur internet des données de santé et les rendre disponibles pour le compte des utilisateurs doit être réalisée dans le respect des référentiels de sécurité et des principes de protection des données personnelles.

16.8 Des professionnels non impliqués directement dans la prise en charge sanitaire de la personne mais assurant au titre de leurs missions le bon fonctionnement des systèmes d'informations, peuvent accéder dans la mesure indispensable à l'accomplissement de leurs tâches et de façon ponctuelle aux données de santé. Ils doivent respecter le secret professionnel et toutes mesures appropriées prévues par le droit interne pour garantir la confidentialité et la sécurité de ces données.

17. Les services de gestion des données de santé

17.1 Chaque Etat membre devrait mettre en place les services d'échange et de partage des données de santé, supports utiles en particulier à la coordination des soins et respectueux des référentiels définis aux principes 14 à 16. Dès lors que ces capacités d'échange et de partage contribuent à la qualité des prises en charge comme à la bonne gestion des systèmes de santé et autres finalités, au service tant des individus que de l'intérêt général et de la santé publique, chaque professionnel de santé et du secteur médico-social et social doit disposer d'un dispositif de gestion dématérialisée de son activité le mettant en capacité d'échanger ou de partager les données de santé des personnes.

17.2 Les patients doivent pouvoir bénéficier d'un dossier médical électronique sécurisé qui leur permet de disposer des informations utiles à leur suivi médical, médico-social et social tout au long de leur parcours de soin. Les informations de ce dossier médical peuvent avec l'accord du patient être partagées par les professionnels intervenant dans la prise en charge de la personne dans les conditions définies au principe 8.

17.3 Tout système de messagerie électronique permettant l'échange de données de santé doit respecter les référentiels définis dans le présent Chapitre.

Chapitre V

18. La recherche dans le domaine de la santé

18.1 L'utilisation des données de santé à des fins de recherche scientifique dans le domaine de la santé devrait être effectuée dans un but légitime et dans le respect des principes posés dans la présente Recommandation.

18.2 La nécessité du recours à des données de santé doit être appréciée au regard de la finalité poursuivie.

18.3 Les personnes concernées par la recherche doivent être informées de l'usage de leurs données et, quand le droit national le prévoit, consentir à cet usage sauf en cas d'urgence sanitaire. Lorsque la personne concernée est légalement incapable et que le droit interne ne lui permet pas d'agir en son propre nom, son représentant légal ou une autorité, ou toute personne ou instance désignée par la loi, recevra l'information et/ou donnera son consentement dans le cadre du projet de recherche.

18.4 Les conditions de traitement des données de santé à des fins de recherche dans le domaine de la santé et en particulier leur intérêt pour la santé publique doivent être appréciées par un ou plusieurs organismes désignés par le droit interne.

18.5 Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données de santé qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée.

18.6 Les données à caractère personnel utilisées à des fins de recherche scientifique ne peuvent être publiées sous une forme permettant d'identifier les personnes concernées à moins que ces dernières n'aient donné leur consentement en vue de la publication et que le droit interne autorise cette publication.

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

Chapitre VI
Les dispositifs mobiles

19. Les dispositifs mobiles

19.1 Le développement d'applications mobiles permet aux personnes concernées comme aux professionnels du secteur de la santé et du secteur médico-social et social de collecter et traiter à distance des 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 "mesure de soi" (*quantified self*), ces objets connectés permettent de quantifier et/ou d'évaluer des paramètres susceptibles de révéler l'état de santé d'une personne et sont dans certains cas utilisés directement pour poser des diagnostics et délivrer des soins.

19.2 Dès lors que les données collectées par ces applications sont susceptibles de révéler l'état de santé d'une personne, concernent tout information relative à sa prise en charge sanitaire et sociale et/ou sont traitées dans un contexte médical, elles constituent des données de santé. A ce titre elles doivent bénéficier des mêmes protections juridiques et de

confidentialité que celles applicables aux autres modes de traitements de données de santé telles que définies par la présente Recommandation et, le cas échéant, complétées par le droit des Etats.

19.3 Les applications de bien-être ou de "mesure de soi" utilisées pour le seul bénéfice de la personne qui l'utilise, mises en œuvre à des fins exclusivement personnelles et qui ne donnent pas lieu à une communication extérieure ne devraient pas être considérées comme soumises aux exigences de la présente Recommandation. Des orientations sur l'application des principes de protection des données au traitement de données de santé, au moyen de ces applications mobiles, par des entités du secteur privé sont à prévoir dans un document distinct de la présente Recommandation.