COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

T-PD(2016)04rev2

3 octobre 2016

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

CM/Rec(2017)…. du Comité des Ministres aux Etats membres en matière de protection des données de santé

(adoptée par le Comité des Ministres … 2017, 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 d'informations du fait du développement d'internet.

La volonté des personnes de contrôler davantage leurs données et de maîtriser le traitement qui en est fait, participent également à cette évolution. 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 dans la compréhension de leur traitement caractérisent notamment ce nouvel environnement.

En outre, les phénomènes de mobilité géographique qui s'accompagnent d'un développement dispositifs médicaux et des objets 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.

Les données de santé font en effet partie des données appartenant à une catégorie particulière qui en vertu de l'article 6 de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel bénéficient d'un niveau de protection plus élevé en raison du risque de discrimination découlant d'un traitement irrégulier.

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

– de prendre des mesures afin 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 leur droit et leur pratique ;

– d'assurer, à cette fin, que la présente recommandation et son annexe sont portées à l'attention des délégués à la protection des données, des autorités en charge des systèmes de santé à charge pour ceux-ci d'assurer le relais vers les différents acteurs qui traitent les données de santé et, en particulier les professionnels 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 qui traitent les données de santé, et pris en compte dans la conception, le déploiement et l'utilisation des technologies de l'information et de la communication (TIC) dans ce secteur.

Annexe à la Recommandation CM/Rec(2017)…

Chapitre I

Dispositions générales

1. Objet

La présente Recommandation a pour objet de fournir aux Etats membres des orientations en vue d'encadrer le traitement 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 et à la protection des données personnelles comme prévu à l'article 8 de la Convention Européenne des Droits de l'Homme. 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 propose également des principes pour organiser l'échange et le partage des données de santé à l'aide d''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 vivante 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 "anonymisation" désigne le procédé appliqué aux données de santé pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement.

- 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 de façon sécurisée et qui permettraient une identification. Les données pseudonymisées sont des données à caractère personnel.

- L'expression « donnée relative à la santé » désigne toute donnée à caractère personnel relative à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne.

- l'expression « données génétiques » désigne 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.

- L'expression « traitement de données » s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données.

- L'expression « responsable du traitement » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données.

- L'expression « sous-traitant » signifie la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données pour le compte du responsable du traitement.

- L'expression « référentiels » désigne un ensemble coordonné de règles et/ou de processus maintenu à l'état de l'art, adaptés aux pratiques 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 structuré ou non de données, sous forme électronique, relatif à une même personne et qui l'accompagne tout au long de son parcours de soins. Il permet notamment 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 et autorisées.

- L'expression « droit à la portabilité » désigne le droit pour les personnes concernées de recevoir les données les concernant fournies à un responsable du traitement, lorsque le traitement est fondé sur le consentement de la personne concernée ou sur un contrat, dans un format structuré, et couramment utilisé et de les transmettre, le cas échéant, à un autre responsable du traitement. Ce droit est rendu possible par l'interopérabilité des formats utilisés par les systèmes d'information.

- 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 qui peuvent notamment être utilisés à des fins diagnostiques, thérapeutiques ou de bien-être.

- L'expression « professionnels de santé » recouvre tout professionnel reconnu comme tel par le droit interne, exerçant dans le secteur sanitaire, médico-social ou social, astreint à une obligation de confidentialité 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 fournisseurs de service d'hébergement de données externalisés pour assurer de façon sécurisée la conservation de données de santé.

Chapitre II

Les conditions juridiques du traitement des données de santé

4. Principes relatifs au traitement des données

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

a. Les données à caractère personnel doivent être traitées de façon transparente, licite et loyale.

b. Les données à caractère personnel 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 archivistiques dans l'intérêt public, à des fins de de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales, dès lors que des garanties appropriées permettent le respect des droits et libertés de la personne.

c. 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.

d. 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.

e. 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.

f. Les données ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire aux finalités pour lesquelles elles sont traitées sauf si elles sont utilisées à des fins archivistiques dans l'intérêt public, à des fins de de recherche scientifique ou historique ou à des fins statistiques et dès lors que des garanties appropriées permettent le respect des droits et libertés de la personne.

g. Des mesures de sécurité appropriées, tenant compte de l'état de l'art technique, de la nature sensible des données de santé et de l'évaluation des risques potentiels fondées sur des référentiels devraient 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 personnes non autorisées.

h. Les droits de la personne dont les données sont collectées et traitées doivent être respectés, en particulier le droit d'accès aux données, d'information, de rectification et d'opposition, d'effacement et de portabilité.

4.2 Le traitement de données de santé n'est autorisé que dans la mesure où des garanties appropriées sont prévues par le droit interne, complétant celles prévues dans la Convention 108 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 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.

5. Finalité du traitement des données de santé

5.1 Les données de santé peuvent être traitées :

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 ;

   ou

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 ;

   ou

c. dans la mesure où la loi l'autorise, en particulier :

   i. aux fins de sauvegarde des intérêts vitaux de la personne ou d'une personne concernée ou d'une autre personne ;

   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 scientifique dans le domaine biomédical et 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 publié ne permet pas d'identifier la personne.

Dans tous les cas, des garanties appropriées devraient 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.

5.2 Obligations complémentaires

a. Ces principes de protection des données personnelles doivent être pris en compte et intégrés dès la conception des systèmes d'information effectuant le traitement des données de santé. Le respect de ces principes devrait être réexaminé régulièrement tout au long de la vie du traitement. Le responsable du traitement devrait évaluer l'impact en termes de protection des données et de respect de la vie privée de ses applications.

b. Le responsable du traitement devrait prendre toutes les mesures appropriées afin de se conformer à ses obligations en matière de protection des données personnelles et devrait 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.

6. Données relatives à l'enfant à naître

6. Les données médicales relatives aux enfants à naître, telles que notamment les données résultant d'un diagnostic préimplantatoire, devraient jouir d'une protection comparable à celle des données relatives à la santé d'un mineur.

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 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 ne devrait être entrepris que si la loi le prévoit. Le traitement de données génétiques à des fins prédictives, afin d'identifier le sujet comme porteur d'un gène responsable d'une maladie ou de détecter une prédisposition ou une susceptibilité génétique à une maladie ne peut être effectué qu'à des fins médicales ou de recherche médicale, et sous réserve des garanties appropriées prévues par la loi.

7.4 La personne concernée a le droit de connaître toute information recueillie sur sa santé. Cependant, la personne soumise à une analyse génétique devrait être informée, préalablement à la réalisation des tests, de la possibilité dont elle dispose de ne pas être informée de découvertes inattendues. Sa volonté de ne pas savoir peut, dans son intérêt ou celui d'une tierce personne concernée, faire l'objet de restrictions.

7.5 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 à moins qu'elle soit expressément autorisée par le droit interne, avec les garanties appropriées.

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 devraient 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 devrait être informée préalablement si les circonstances le permettent de la nature des données de santé 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 devraient 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 aux données. Il peut s'agir notamment 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 pas, en principe, être considérés comme des tiers autorisés à accéder aux données de santé des patients sauf si le droit interne le prévoit et moyennant des garanties appropriées.

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 légitimes pour lesquelles elles sont traitées. 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, devrait être réalisée dans le respect des principes de la présente Recommandation.

Chapitre III

Les droits de la personne concernée

Les droits des personnes concernées doivent être conciliés avec d'autres droits et intérêts légitimes. Ils peuvent faire l'objet de restrictions dès lors qu'elles sont prévues par une loi, qu'elles constituent des mesures nécessaires et proportionnées dans une société démocratique pour les motifs énumérés à l'article 9 de la Convention 108.

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 doit 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, ou, si possible, des critères utilisés pour déterminer cette durée,
- des destinataires ou catégories de destinataires des données et des transferts de données prévus vers un pays tiers, ou vers une organisation internationale,
- de la possibilité, le cas échéant, de s'opposer au traitement de ses données ou de revenir sur son accord initial et,
- 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.

Elle devrait également être informée :

- 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,
- de la possibilité de déposer une plainte auprès d'une autorité de contrôle,
- de l'existence de décisions automatisées comprenant le profilage.

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 en particulier pour des traitements à des fins de recherche scientifique ou historique ou à des fins statistiques. 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. Seules l'urgence ou l'impossibilité d'informer peuvent dispenser du respect de l'information ; les soins priment sur l'information.

11.3 La volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic ou d'une prédisposition génétique doit être respectée, sauf lorsque cela constitue un risque sérieux pour la santé de tiers.

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

12. Le consentement

12. Lorsque la personne concernée est appelée, conformément au droit interne, 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.

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

13.1 Toute personne a le droit de savoir si des données à caractère personnel la concernant font l'objet d'un traitement et si c'est le cas, d'avoir accès aux informations suivantes :

- la ou les finalités du traitement,
- les catégories de données à caractère personnel concernées,
- les destinataires ou catégories de destinataires des données et les transferts de données prévus vers un pays tiers, ou vers une organisation internationale,
- la durée de conservation de ses données, ou, si possible, les critères utilisés pour déterminer cette durée
- la possibilité, le cas échéant, de s'opposer au traitement de ses données ou de revenir sur son accord initial
- de la possibilité de déposer une plainte auprès d'une autorité de contrôle,
-l'existence de décisions automatisées comprenant le profilage.

13.2 Le droit d'accès aux informations, également sur support papier, permet à la personne d'exercer son droit de rectification et d'effacement, le droit d'obtenir les données dans un format structuré, quand le traitement automatisé est fondé sur le consentement ou sur un contrat, permet de transmettre les données à un autre responsable e traitement désigné par la personne concernée.

13.3 Le droit à l'effacement s'exerce sous réserve des cas prévus par la loi invoquant des motifs légitimes. La personne a le droit de s'opposer pour des motifs tenant à sa situation personnelle à la collecte de ses données de santé à caractère personnel à moins qu'elles ne soient rendues anonymes ou que 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 devrait pouvoir disposer d'un recours.

Chapitre IV

Référentiels pour le traitement des données de santé

Le traitement des données de santé devrait conduire chaque acteur à un niveau d'exigence élevé pour assurer la confidentialité des données de santé.

14. Référentiels

14. Conformément au principe de *privacy by design* tel que défini au point 4.5, les applications qui gèrent des données de santé devraient 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.

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 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.

e. assurer l'authentification des personnes et des systèmes qui interviennent dans le traitement 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 devrait être sécurisé.

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 devrait 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 - devrait 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. Il impose également 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.

16.5 L'auditabilité devrait 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.

16.6 L'activité qui consiste à conserver dans des systèmes analogiques et numériques des données de santé et les rendre disponibles pour le compte des utilisateurs devrait être réalisée dans le respect des référentiels de sécurité et des principes de protection des données personnelles.

16.7 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.

Chapitre V

La recherche scientifique

17. La recherche scientifique

17.1 L'utilisation des données de santé à des fins de recherche scientifique devrait être effectuée dans un but légitime et dans le respect des principes de protection des droits de l'Homme dans les domaines concernés.

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

17.3 Avant de se voir demander son consentement à l'utilisation de ses données de santé à des fins de recherche scientifique, la personne concernée devrait bénéficier d'une information compréhensible aussi précise que possible, concernant :

– la nature de la recherche envisagée et les choix éventuels qu'elle peut exercer ;
– les conditions applicables à la conservation des données, y compris les politiques en matière d'accès et d'éventuels transferts ; et
– les droits et garanties prévus par la loi, et, notamment, son droit de refuser de donner son consentement ainsi que de le retirer à tout moment. Des restrictions peuvent être apportées en cas d'urgence sanitaire. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet.

17.4 Les conditions de traitement des données de santé à des fins de recherche scientifique doivent être appréciées par un ou plusieurs organismes désignés par le droit interne.

17.5Les professionnels de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données relatives à la santé qu'ils détiennent pour autant que la personne concernée ait été informée préalablement de cette faculté et y ait consenti conformément aux principes de consentement libre et éclairé.

17.6 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 la loi autorise cette publication.

17.7 Dans tous les cas, des garanties appropriées devraient 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 de l'homme et des libertés fondamentales.

Chapitre VI
Les dispositifs mobiles

18. Les dispositifs mobiles

18.1 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.

18.2 Dès lors que les données collectées par ces applications sont susceptibles de révéler l'état de santé d'une personne, concernent toute 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 devraient 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.

18.3 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, une collecte ou un transfert, 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.