COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 3 mars 2017 T- PD(2016)04rev4

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 RELATIVES A LA 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 relatives à la 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 des 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 relatives à la santé », en réaffirmant le caractère sensible de ces données et l'importance d'encadrer leur utilisation afin de garantir un usage respectant les droits et libertés fondamentales de l'individu notamment le droit à la protection des données à caractère personnel

Les données relatives à la 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 pouvant résulter de leur traitement.

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 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 ainsi que des délégués à la protection des données ou des personnes assurant les mêmes fonctions ;

– 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 relatives à la 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 relatives à la 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 souligne également l'importance du 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 relatives à la santé à caractère personnel dans les secteurs publics et privés.

A ce titre, elle s'applique également à l'échange et au partage des données relatives à la 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 relatives à la 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, des efforts ou le recours à des ressources déraisonnables. Par ailleurs, les avancées technologiques et autres développements peuvent influer sur ce que revêt la notion de « délais, efforts ou ressources 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 organisée et qui permettraient une identification directe ou indirecte de la personne. 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 « 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, quel que soit le support, pour assurer de façon sécurisée la conservation de données de santé sur internet.

Chapitre II

Les conditions juridiques du traitement des données relatives à la santé

4. Principes relatifs au traitement des données

4.1 La personne qui traite des données relatives à la santé devrait respecter les principes suivants :

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

b. Les données 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 explicite de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi.

d. Les données devraient en principe être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que dans le respect des principes 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 relatives à la santé et de l'évaluation des risques potentiels devraient être mises en place pour empêcher les risques tels que l'accès accidentel ou non autorisé aux données, leur destruction, perte, utilisation, indisponibilité, inaccessibilité, 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 relatives à la 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 traiter des données relatives à la santé que dans le respect de règles de confidentialité et de mesures de sécurité similaires à celles incombant à un professionnel de santé.

5. Finalités et bases légitimes du traitement des données relatives à la santé

5.1 Les données relatives à la santé peuvent être traitées pour les finalités suivantes dès lors que la loi l'autorise et que des garanties appropriées sont prévues :

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, l'action humanitaire ou pour assurer un haut niveau de qualité et de sécurité aux traitements médicaux, produits de santé et dispositifs médicaux ;

iii. aux fins de sauvegarde des intérêts vitaux de la personne concernée ou

d’une autre personne ;

iv. 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 ;

v. pour des motifs de santé publique dès lors qu’ils sont licites, légitimes et sont compatibles avec la finalité initiale de collecte des données ;

vi. pour des traitements à des fins de recherche scientifique ou historique ou à des fins archivistiques dans l’intérêt public ou à des fins statistiques dans les conditions définies par le droit interne pour garantir la protection des intérêts légitimes de la personne ;

vii. 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 ;

viii. pour des motifs nécessaires à la constatation, à l’exercice ou à la défense d’un droit en justice.

5.2 Les données relatives à la santé peuvent également être traitées dès lors que la personne concernée a donné son consentement conformément au principe 13 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 et dès lors que des garanties appropriées sont prévues.

5.3 Les données relatives à la santé peuvent également être traitées dès lors que le traitement repose sur un contrat avec un professionnel de santé et dès lors que des garanties appropriées sont prévues.

5.4 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.

5.5. 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 relatives à la 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.

5.6 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

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 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 afin de permettre la poursuite 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 pour des raisons liées à une action humanitaire ou pour des raisons de santé et notamment pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers et si la loi le prévoit ou que la personne concernée y a consenti. 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 dès lors qu'elle ne l'interdit pas.

7.4. Les données génétiques ne peuvent pas faire objet d'un traitement pour déterminer, par exemple, l'aptitude professionnelle d'employés ou de candidats à l'emploi, même avec le consentement de l'intéressé.

7.5. Les données génétiques ne devraient être collectées que si la , loi le prévoit et que des garanties appropriées sont prévues.

7.6 La personne concernée a le droit de connaître toute information recueillie sur sa santé. Cependant, la volonté de la personne soumise à une analyse génétique de ne pas savoir devrait être respectée et cette personne devrait être informée, préalablement à la réalisation des tests, de la possibilité dont elle dispose de ne pas être informée de résultats y compris 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, notamment au regard de l'obligation de soigner qui incombe aux médecins.

7.7 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, 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, pour des finalités précises, notamment dans le cadre de publications de résultats de recherche et 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 relatives à la 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 personne concernée devrait être informée préalablement, sauf impossibilité en cas d'urgence, de la nature des données relatives à la santé traitées ainsi que des professionnels de santé qui la prennent en charge. Elle doit pouvoir à tout moment s'opposer à l'échange et au partage de ses données relatives à la santé.

8.3 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.

8.4. L'échange et le partage de données relatives à la 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, dans ce cas, transmettre ou recevoir que les données qui relèvent strictement du périmètre de ses missions.

9. Communication à des destinataires autorisés

9.1 Les données relatives à la santé peuvent être communiquées à des destinataires 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, des agents d'une administration désignés par un texte ou des organisations humanitaires.

9.2 Les médecins de compagnies d'assurance et les employeurs ne peuvent pas, en principe, être considérés comme des destinataires autorisés à accéder aux données relatives à la santé des patients sauf si le droit interne le prévoit et moyennant des garanties appropriées.

9.3 La communication des données relatives à la santé, à moins que le droit interne ne prévoie d'autres garanties appropriées, ne peut intervenir que si le destinataire est soumis aux règles de confidentialité propres aux professionnels des soins de santé ou à des règles de confidentialité similaires.

10. La conservation des données de santé

10.1 Les données relatives à la santé ne doivent être conservées que pour la durée nécessaire à la réalisation des finalités légitimes pour lesquelles elles sont traitées.

10.2 La conservation de données relatives à la 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

11. Les droits de la personne concernée

Les droits des personnes à l'égard de leurs données doivent pouvoir s'exercer aisément et chaque Etat doit s'assurer que chaque personne dispose des moyens nécessaires, adéquats, légaux effectifs et pratiques pour les exercer.

Les professionnels de santé doivent mettre en œuvre les moyens nécessaires pour s'assurer du respect de l'exercice effectif de ces droits comme un élément de leur déontologie professionnelle.

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.

12. La transparence du traitement

12.1 Toute personne doit être informée de la collecte et du traitement de ses données relatives à la santé.

L'information doit porter sur :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, de celle de ses sous-traitants,
- la finalité du traitement des données et de l'existence, le cas échéant, de son fondement légal,
- la durée de conservation de ses données,
- les destinataires ou catégories de destinataires des données et des transferts de données prévus vers un pays tiers, ou vers une organisation internationale,
- la possibilité, le cas échéant, de s'opposer au traitement de ses données sauf si le responsable du traitement justifie d'un motif légitime prévalant sur les intérêts, ou droits et libertés fondamentales de la personne, ou de revenir sur son consentement initial,
- les conditions et les moyens mis à sa disposition pour exercer auprès du responsable du traitement ses droits d'accès, de rectification et d'effacement de ses données lorsque dans ce dernier cas, elles ont été traitées en violation des dispositions de la présente Recommandation.

Elle peut porter sur :

- la possibilité de traiter ultérieurement ses données pour une finalité compatible dans le respect de garanties appropriées prévues par le droit interne,
- les techniques particulières utilisées pour traiter ses données de santé,
- la possibilité de déposer une plainte auprès d'une autorité de contrôle,
- l'existence de décisions automatisées comprenant le profilage.

12.2 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.

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

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

13. Le consentement

13.1 Lorsque la personne concernée est appelée, conformément au droit interne, à donner son consentement au traitement de ses données relatives à la santé, celui-ci devrait être libre, spécifique, éclairé et explicite. Dès lors que l'expression du consentement est dématérialisée, celle-ci doit pouvoir être prouvée par tout dispositif technique.

13.2 Le consentement n'exonère pas celui qui le recueille de ses obligations d'information préalable.

14. Les droit d'accès, d'opposition, de rectification, d'effacement et de portabilité

14.1 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 sans délais et frais excessifs et sous une forme intelligible :

- 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,
- connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués.

14.2 Le droit à la portabilité permet à la personne concernée d'exiger du responsable de traitement qu'il transmette dans un format structuré, lisible et interopérable à un autre responsable de traitement, ses données traitées de façon automatisée.

14.3 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 relatives à la 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.

14.4 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 relatives à la santé

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

15. Les référentiels d'interopérabilité

15.1 Le développement de systèmes d'information efficients, respectueux des droits des personnes concernées doivent avoir pour objectif l'amélioration du suivi sanitaire de la personne tout au long de son parcours de soins.

A cet effet, les professionnels de santé ainsi que tout organisme public ou privé autorisé à traiter des données relatives à la santé, notamment les personnes responsables des applications permettant l'échange et le partage des données relatives à la 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.

La prise en compte de ces référentiels doit intervenir dès la conception des systèmes d'information (« *privacy by design* »).

Leur respect doit en particulier être assuré, dès lors que les données relatives à la santé sont collectées et traitées dans le cadre des relations de prise en charge et de soins.

15.2 Ces référentiels ont pour objet de définir des standards permettant l'échange et le partage des données relatives à la santé par les systèmes d'information et d'assurer le suivi de leur mise en œuvre dans des conditions de sécurité requises, par exemple en recourant à la certification.

16. Les référentiels de sécurité

16.1 Le traitement des données relatives à la santé devrait être sécurisé et à cet égard, des politiques de sécurité adaptées aux risques pour les droits et libertés fondamentales doivent être définies.

16.2 Ces règles de sécurité, maintenues à l'état de l'art et révisées de façon régulière, doivent se traduire par l'adoption de mesures techniques et organisationnelles de nature à protéger les données relatives à la santé contre toute destruction illégale ou accidentelle, toute perte, toute altération et de prévenir tout accès non autorisé et toute indisponibilité ou inaccessibilité. En particulier, le droit interne devrait prévoir d'organiser et d'encadrer les modalités de collecte, de conservation et de restitution des données relatives à la 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 bases 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 des données relatives à la 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 relatives à la 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 Le traitement des données relatives à la santé à des fins de recherche scientifique devrait être effectué dans un but légitime et dans le respect des principes de protection des droits de l'Homme appliqués en la matière.

17.2 La nécessité du traitement à des fins de recherche scientifique de données relatives à la santé devrait être appréciée au regard de la finalité poursuivie et du risque encouru par la personne concernée et sa famille biologique.

17.3 La personne concernée doit bénéficier d'une information transparente, compréhensible et aussi précise que possible, concernant :

– la nature de la recherche envisagée, les choix éventuels qu'elle peut exercer ainsi que toutes conditions pertinentes régissant l'utilisation des matériels, y compris concernant la reprise de contact et le retour d'informations ;
– les conditions applicables à la conservation des données, y compris les politiques en matière d'accès et d'éventuels transferts ;
– les droits et garanties prévus par la loi, et, notamment, son droit de refuser de participer à la recherche ainsi que de se retirer à tout moment.

Des restrictions peuvent être apportées en cas d'urgence sanitaire.

17.4 Lorsque le consentement est requis par le droit interne, il doit être libre et éclairé par l'information préalable. Cette information doit également porter sur le droit de refuser son consentement ainsi que de le retirer à tout moment.

Dans la mesure où il n'est pas toujours possible de délimiter la finalité complète d'une recherche au moment de la collecte des données, 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.

17.5 Des matériels biologiques ne devraient être utilisés dans un projet de recherche que si celui-ci relève du champ du consentement donné par la personne concernée. Lorsque l'utilisation proposée de matériels biologiques identifiables dans un projet de recherche ne relève pas du champ du consentement donné auparavant par la personne concernée, son consentement à l'utilisation proposée devrait être recherché et, à cette fin, des efforts raisonnables devraient être faits pour contacter la personne concernée. Le souhait de la personne concernée de ne pas être contactée devrait être respecté. Lorsque les tentatives pour contacter la personne concernée s'avèrent infructueuses, les matériels biologiques ne devraient être utilisés dans le projet de recherche que sous réserve d'une évaluation indépendante portant sur le respect des conditions suivantes :

i. des éléments sont apportés témoignant que des efforts raisonnables ont été déployés pour contacter la personne concernée ;

ii. la recherche présente un intérêt important sur le plan scientifique et le traitement de ces informations est proportionné au but recherché;

iii. les buts de la recherche ne peuvent être raisonnablement atteints qu'en utilisant des matériels biologiques pour lesquels un consentement n'a pu être obtenu ; et

iv. aucune opposition expressément formulée par la personne concernée à une telle utilisation à des fins de recherche n'est connue.

17.6 Les conditions de traitement des données relatives à la santé à des fins de recherche scientifique doivent être appréciées, le cas échéant, par un ou plusieurs organismes désignés par le droit interne.

17.7 Les 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 le cas échéant.

17.8 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.

17.9 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

Les dispositifs mobiles permettent le développement de nouvelles pratiques médicales et de santé publique. Ils recouvrent tout à la fois des applications concernant le mode de vie et le bien-être qui peuvent se connecter à des dispositifs médicaux ou des capteurs ainsi que des systèmes de conseil personnalisés et d'observance.

18. Les dispositifs mobiles

18.1 Dès lors que des données sont collectées par des applications mobiles, qu'elles soient ou non implantées chez l'homme, susceptibles de révéler l'état de santé d'une personne ou concernent toute information relative à sa prise en charge sanitaire et sociale et/ou sont traitées dans un contexte médical, elles constituent des données relatives à la santé. A ce titre elles devraient bénéficier des mêmes protections juridiques et de confidentialité que celles applicables aux autres modes de traitements de données relatives à la santé telles que définies par la présente Recommandation et, le cas échéant, complétées par le droit des Etats.

18.2 Les personnes qui utilisent ces applications mobiles dès lors qu'elles génèrent des traitements de données à caractère personnel, doivent bénéficier des mêmes droits que ceux visés au Chapitre III de la présente recommandation. Elles doivent notamment avoir reçu toute l'information nécessaire sur la nature du dispositif et son fonctionnement. A cet effet des conditions générales d'utilisation claires et transparentes doivent être rédigées par le responsable du traitement et avec le concours du fabricant et du distributeur du dispositif dont les rôles doivent être précisés.

Le patient utilisateur doit être en mesure de maîtriser l'usage du dispositif.

18.3 Le recours à des applications mobiles doit s’accompagner de garanties de sécurité spécifiques et adaptées à l’état de l’art de nature à s’assurer en particulier de l’authentification de la personne concernée et du chiffrement des transmissions de données.

18.4 L’hébergement par un tiers technologique des données relatives à la santé produites à l’aide des applications mobiles doit être soumis au respect de règles de sécurité de nature à assurer leur confidentialité, leur intégrité et leur restitution à la demande de la personne concernée.

18.5 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 un partage des données relatives à la santé peuvent être soumises à de moindres exigences de sécurité à l’exception des obligations d’information sur le dispositif qui restent identiques.

Par ailleurs, des orientations sur l’application des principes de protection des données relatives à la santé aux entités commerciales qui proposent des services à partir d'applications mobiles, sont à prévoir dans un document distinct de la présente Recommandation.