

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Strasbourg, le 1<sup>er</sup> juin 2017

T- PD(2017)03

**COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES  
PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE  
DES DONNEES A CARACTERE PERSONNEL**

**PROJET DE RECOMMANDATION EN MATIERE DE  
PROTECTION DES DONNEES RELATIVES A LA SANTE**

Direction Générale Droits de l'Homme et Etat de droit

## TABLE DES MATIERES

|  |    |
|--|----|
| Recommandation .....   | 2  |
| Annexe à la Recommandation CM/Rec(2017).....   | 4  |
| Chapitre I. Dispositions générales .....   | 4  |
| Chapitre II. Les conditions juridiques du traitement des données relatives à la santé..... | 5  |
| Chapitre III. Les droits de la personne concernée.....                                     | 9  |
| Chapitre IV. Les référentiels d'interopérabilité et de sécurité .....                      | 11 |
| Chapitre V. La recherche scientifique .....  | 13 |
| Chapitre VI. Les dispositifs mobiles .....   | 15 |

## Recommandation

### **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 des données relatives à la santé, dont l'environnement a, depuis l'adoption de la Recommandation (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.

Les bénéfices de cette dématérialisation croissante des données peuvent se traduire à maints égards, comme notamment en matière d'amélioration des politiques de santé publique, des soins, de la prise en charge des patients. La promesse de ces bénéfices nécessite de s'assurer que l'avènement et la quantité sans cesse croissante de données potentiellement identifiantes, couplés aux capacités d'analyse technique liées à une médecine personnalisée, s'accompagnent de mesures juridiques et techniques de nature à préserver une protection effective des personnes concernées.

La volonté des personnes de contrôler davantage leurs données et de maîtriser les décisions issues de leur traitement, participe 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 la façon dont des décisions qui les concernent sont prises 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 (97) 5 relative à la protection des données médicales, terme auquel on préférera le terme plus général de « données relatives à la santé », en réaffirmant le droit à la santé, le caractère sensible des données relatives à la santé et l'importance d'encadrer leur utilisation afin de garantir un usage respectant les droits et libertés fondamentales de toute personne notamment le droit au respect de la vie privée et 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 bénéficie d'un niveau de protection plus élevé en raison notamment du risque de discrimination pouvant résulter de leur traitement.

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.

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 (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'en assurer la promotion vers les différents acteurs qui traitent les données relatives à la 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**

#### **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, 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 à cette fin l'importance du développement de systèmes d'information interopérables et sécurisés.

#### **Champ d'application**

La présente recommandation est applicable au traitement, dans les secteurs public et privé, de données à caractère personnel relatives à la santé.

A ce titre, elle s'applique également à l'échange et au partage des données relatives à la santé réalisés au moyen d'outils numériques qui contribuent au respect 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.

#### **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 des ressources déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes.

- L'expression "anonymisation" désigne le procédé appliqué aux données à caractère personnel pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement.

- L'expression "pseudonymisation" désigne un mode de traitement 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 passé, actuel et futur 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, adapté aux pratiques et applicable aux systèmes d'information de santé et qui recouvre les domaines 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 relatives à la 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 » désigne le recours à des fournisseurs de service externalisés, quel que soit le support, pour assurer de façon sécurisée la conservation numérique de données.

## **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 (voir principe 5), 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 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 (s'agissant par exemple des garanties à assurer dans le cadre de la recherche scientifique, voir le principe 17) permettent le respect des droits et libertés fondamentales 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 tel que défini au principe 13 de la présente recommandation ou en vertu d'autres fondements légitimes prévus par la loi, tels qu'énumérés au principe 5 de la présente recommandation.

- d. Les données devraient en principe et dans la mesure du possible être collectées auprès de la personne concernée. Si la personne concernée n'est pas en mesure de fournir les données et que celles-ci sont nécessaires à la finalité du traitement, elles peuvent être collectées auprès d'autres sources dans le respect des principes de la présente recommandation.
- 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. 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.
- g. Les droits de la personne dont les données sont traitées doivent être respectés, en particulier les droits d'accès aux données, d'information, de rectification et d'opposition, d'effacement et de portabilité tels que prévus au principe 11 de la présente recommandation.

4.2 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 :

- a. 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 ;
- b. pour des motifs d'intérêt public dans le domaine de la santé publique comme par exemple, la protection à l'égard de risques sanitaires l'action humanitaire ou pour assurer un haut niveau de qualité et de sécurité aux traitements médicaux, produits de santé et dispositifs médicaux ;
- c. aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;
- d. 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 ;
- e. pour des motifs de santé publique compatibles avec la finalité initiale de collecte des données, dès lors qu'ils sont licites et légitimes ;
- f. pour des traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions définies par le droit interne (telle que notamment l'obligation d'une information préalable détaillée de la personne concernée lui permettant d'exercer son droit de refuser de participer à une recherche scientifique) pour garantir la protection des intérêts légitimes de la personne ;
- g. 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 ;

- h. 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.

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.

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. Les 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 relatives à la santé d'enfants à naître, telles que notamment les données résultant d'un diagnostic prénatal ou d'une identification des caractéristiques génétiques du fœtus 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 ne devraient être collectées que si la loi le prévoit et que des garanties appropriées sont prévues.

7.2 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'un membre de sa famille biologique ou pour la recherche scientifique ne devraient être utilisées qu'à ces seules fins ou pour permettre aux personnes concernées par les résultats de ces examens de prendre une décision éclairée à leur sujet.

7.3 Le traitement de données génétiques pour les besoins d'une enquête ou d'une procédure judiciaire devrait 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 risque réel et immédiat ou afin de permettre la poursuite d'une infraction pénale déterminée. En aucun cas ces données ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

7.4 Tout traitement de données génétiques à d'autres fins que celles prévues aux points 7.2 et 7.3 ne devrait être entrepris que pour éviter tout préjudice grave à la santé de la personne concernée ou d'un membre de sa famille biologique ainsi que pour des raisons humanitaires.

7.5 Les données prédictives existantes résultant de tests génétiques ne devraient pas être traitées à des fins d'assurance, sauf si cela est spécifiquement autorisé par la loi. Dans ce cas, leur traitement ne devrait être autorisé qu'après une évaluation indépendante du respect des critères applicables définis par la loi, au regard du type de test utilisé et du risque particulier à couvrir.

7.6 La personne concernée a le droit de connaître toute information recueillie sur sa santé. Cependant, le souhait de la personne dont les données génétiques sont traitées de ne pas savoir devrait être respecté 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. Son souhait de ne pas savoir peut, dans son intérêt ou celui d'un membre de sa famille biologique faire l'objet de restrictions prévues par la loi, 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 ou une personne ayant un lien direct avec sa lignée génétique devrait être interdite à moins que la ou les personnes concernées y aient expressément consenti de façon préalable et qu'une telle publication soit expressément autorisée par le droit interne, pour des finalités précises et avec les garanties appropriées.

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

8.1 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.

8.2 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 reconnaître 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 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 et en fonction de leurs habilitations.

8.4 L'utilisation d'un dossier médical électronique et d'une messagerie électronique de nature à permettre le partage et l'échange de données relatives à la santé doivent respecter ces principes.

## **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 ou si la personne concernée y a consenti.

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

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, notamment au regard de la compatibilité des finalités de ce traitement ultérieur avec les finalités du traitement initial.

## **Chapitre III. Les droits de la personne concernée**

### **11. Les droits d'accès, d'opposition, de rectification, d'effacement et de portabilité**

11.1 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,
- la connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués.

11.2 Le droit à l'effacement s'exerce sous réserve des cas prévus par la loi invoquant des motifs légitimes. La personne concernée a le droit d'obtenir rectification des données qui la concernent. Elle a par ailleurs le droit de s'opposer pour des motifs tenant à sa situation personnelle au traitement de ses données relatives à la santé à moins qu'elles ne soient rendues anonymes, que le détenteur des données invoque une raison impérieuse et légitime qui concerne l'intérêt de la santé publique ou qu'il s'agisse de données traitées conformément aux conditions établies au principe 17 de la présente recommandation.

11.3 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.

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

11.5 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.

11.6 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.

11.7 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, dont notamment les objectifs d'intérêt public général de l'Etat ayant trait à la santé publique.

## **12. La transparence du traitement**

12.1 Toute personne doit être informée 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, 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 conformément aux dispositions du point 11.2, 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.

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 et dans les conditions prévues au point 4.1.b,
- 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 de la part du responsable du traitement, en particulier pour des traitements à des fins archivistiques dans l'intérêt public, 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'obligation de transparence. Dans ce cas, l'information sera fournie dès que possible.

12.3 Le souhait d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respecté, 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**

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

## **Chapitre IV. Les référentiels d'interopérabilité et de sécurité**

### **14. Les référentiels**

14.1 Le développement de systèmes d'information efficaces et respectueux des droits des personnes concernées doit 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 les référentiels auxquels le droit interne de chaque pays peut donner une force juridique.

14.2 L'interopérabilité des systèmes permet de contribuer à la portabilité des données et doit à ce titre être encouragée. Le traitement des données relatives à la santé requiert par ailleurs de chaque acteur un niveau d'exigence élevé pour assurer la confidentialité de ces données.

### **15. Les référentiels d'interopérabilité**

15.1 Ces référentiels ont pour objet de définir des standards permettant la portabilité, 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.

15.2 La prise en compte de ces référentiels doit intervenir dès la conception des systèmes d'information (« *privacy by design* ») et une attention particulière doit être portée au traitement de données relatives à la santé dans le cadre des relations de prise en charge et de soins.



## **16. Les référentiels de sécurité**

16.1 Le traitement des données relatives à la santé doit 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 en matière de recherche génétique, de sa famille biologique.

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

- la nature de la recherche scientifique envisagée, les choix éventuels qu'elle peut exercer ainsi que toutes conditions pertinentes régissant l'utilisation des données, 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 Dans la mesure où il n'est pas toujours possible de définir de façon préalable les finalités des différents projets de recherche au moment de la collecte des données, les personnes concernées devraient pouvoir exercer un choix 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 données relatives à la santé ne devraient être utilisées dans un projet de recherche que si celui-ci relève du champ de l'acceptation de la personne concernée. Lorsque l'utilisation proposée des données ne relève pas de ce champ, son acceptation de l'utilisation proposée devrait être recherchée 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 données relatives à la santé ne devraient être utilisées dans le projet de recherche que sous réserve d'une évaluation indépendante portant sur le respect des conditions suivantes :

- a. des éléments sont apportés témoignant que des efforts raisonnables ont été déployés pour contacter la personne concernée ;
- b. la recherche présente un intérêt important sur le plan scientifique et le traitement de ces informations est proportionné au but recherché ;
- c. les buts de la recherche ne peuvent être raisonnablement atteints qu'en utilisant des données pour lesquelles un consentement n'a pu être obtenu ; et
- d. 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 en ait été informée préalablement conformément aux dispositions du point 17.3.

17.8 La pseudonymisation des données, avec intervention d'un tiers de confiance lors de la séparation de l'identification, est au nombre des mesures qui peuvent être mises en œuvre afin de garantir le respect des droits et libertés fondamentales de la personne concernée. Ceci est à privilégier dès lors que les finalités de la recherche scientifique concernée peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées.

17.9 Lorsqu'une personne décide de se retirer d'une recherche scientifique, ses données relatives à la santé traitées dans le cadre de cette recherche doivent être détruites ou anonymisées et la personne concernée doit en être informée.

17.10 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.

17.11 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 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 sur la personne et sont susceptibles de révéler une information sur l'état physique ou mental de la personne en lien avec sa santé 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 concernées 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 de façon préalable toute l'information nécessaire sur la nature du dispositif et son fonctionnement afin de pouvoir en maîtriser l'usage. 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.

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 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.