COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 8 juin 2018 T- PD(2018)06

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

CM/Rec(2018)…. du Comité des Ministres aux États membres en matière de protection des données relatives à la santé

(adoptée par le Comité des Ministres … 2018, lors de la … réunion des Délégués des Ministres).

Eu égard aux dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE n° 108, ci-après la « Convention 108 »), ainsi que celles de son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001 (STE n° 181), le Comité des Ministres est convaincu de l'intérêt de faciliter l'application de ces principes aux traitements de données relatives à la santé.

Les États 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 (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 croissante du secteur professionnel et notamment des activités de soins de santé et de prévention, de recherche en sciences de la vie, de gestion du système de 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. Ils nécessitent de s'assurer que l'avènement et la quantité sans cesse croissante de données, couplés aux capacités d'analyse technique qui conduisent à une médecine personnalisée, s'accompagnent de protections juridiques et techniques de nature à préserver une protection effective des personnes concernées.

La volonté des personnes de contrôler davantage leurs données personnelles et de maîtriser les décisions issues de leur traitement, l'implication croissante des patients dans la compréhension de la façon dont des décisions qui les concernent sont prises, participent également à cette évolution.

Par ailleurs, les phénomènes de mobilité géographique qui s'accompagnent d'un développement d'applications mobiles, des dispositifs médicaux et des objets connectés contribuent également à de nouveaux usages et à la production d'un volume rapidement croissant de données relatives à la santé traitées par des parties prenantes plus diverses.

Ce constat partagé par les États membres conduit à proposer une nouvelle rédaction de la Recommandation (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 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 108, bénéficient 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 à la confidentialité des informations la concernant.

Le traitement des données relatives à la santé doit en tout état de cause servir la personne concernée ou conduire à améliorer la qualité et l'efficacité des soins de santé, ainsi que les systèmes de santé lorsque cela est possible, tout en respectant les droits fondamentaux de la personne.

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

– de prendre des mesures afin d'assurer que les principes contenus dans l'annexe à cette recommandation, qui remplace la Recommandation (97) 5 susmentionnée, sont reflétés dans leur droit et leur pratique ;

– d'assurer, à cette fin, que cette recommandation et son annexe soient 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 cette 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(2018)…

Chapitre I. Dispositions générales

1. Objet

La présente recommandation a pour objet de fournir aux États 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 à cette fin l'importance du développement de systèmes d'information sécurisés interopérables.

2. Champ d'application

Cette recommandation est applicable au traitement de données à caractère personnel relatives à la santé, dans les secteurs public et privé. 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. Elle ne saurait être interprétée comme limitant ou portant atteinte à la faculté d'accorder aux personnes concernées, par la loi, une protection plus étendue.

Les dispositions de cette 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 cette recommandation, les expressions suivantes sont définies ainsi :

- L'expression « donnée à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »).

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

- L'expression « pseudonymisation » désigne le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. 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 lors du développement prénatal, résultant de l’analyse d’un échantillon biologique de cet individu, notamment une analyse des chromosomes, de l’ADN ou de l’ARN ou de tout autre élément permettant d’obtenir des informations équivalentes.

- 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, l’agence ou tout 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. Ils peuvent être rendus opposables par le droit.

- 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 et les dispositifs médicaux connectés 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 délivrant des soins de santé.

- L'expression « hébergement externe de données » 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 Toute 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 énoncées au principe 5 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 permettent le respect des droits et libertés de la personne.

c. Le traitement des données doit être nécessaire et proportionné à la finalité légitime poursuivie et ne doit être effectué que sur la base du consentement de la personne concernée tel que défini au principe 5.2 ou en vertu d’autres fondements légitimes prévus par la loi, tels qu’énumérés dans les autres paragraphes du principe 5.

d. Les données à caractère personnel 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 cette recommandation.

e. Les données doivent être adéquates, pertinentes et non excessives pour ce qui est nécessaire 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 qu'un accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, indisponibilité, inaccessibilité, modification ou divulgation.

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, et d'effacement tels que prévus aux principes 11 et 12 de cette recommandation.

4.2. Les principes de protection des données personnelles devraient être pris en compte et intégrés par défaut (« *privacy by default* ») dès la conception des systèmes d'information effectuant le traitement des données relatives à la santé (« *privacy by design* »). Le respect de ces principes devrait être réexaminé régulièrement tout au long de la vie du traitement. Avant de commencer le traitement et à intervalles réguliers, le responsable du traitement devrait procéder à un examen de l'impact potentiel des traitements de données envisagés sur la protection des données et le respect du droit à la vie privée, ainsi que des mesures destinées à réduire les risques.

4.3 Le responsable du traitement ainsi que les sous-traitants agissant sous sa responsabilité devraient prendre toutes les mesures appropriées afin de se conformer à ses obligations en matière de protection des données personnelles et devraient être en mesure de démontrer en particulier à l'autorité de contrôle compétente que le traitement est en conformité avec ces obligations.

4.4 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 des mesures de sécurité garantissant un niveau de protection équivalent à celle incombant aux professionnels de santé.

5. Bases légitimes du traitement des données relatives à la santé

Le traitement n'est licite que dans la mesure où le responsable du traitement peut justifier d'une au moins des bases légitimes décrites dans les paragraphes suivants :

5.1 Sans préjudice des situations prévues aux paragraphes suivants, les données relatives à la santé peuvent uniquement être traitées lorsque des garanties appropriées sont inscrites dans la loi et que le traitement est nécessaire :

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, dans les conditions définies par la loi ;

b. pour des motifs de 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, dans les conditions définies par la loi ;

c. aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne lorsque le consentement ne peut être recueilli ;

d. 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 ;

e. pour des motifs d'intérêt public dans le domaine de la gestion des demandes de prestations et de services de protection sociale et d'assurance maladie, dans les conditions définies par la loi ;

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 la loi pour garantir la protection des droits fondamentaux et intérêts légitimes de la personne (s'agissant notamment des traitements de données relatives à la santé à des fins de recherche, voir les conditions prévues au Chapitre V);

g. pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

h. pour des motifs d'intérêt public important, sur la base de la loi, et qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

5.2 Les données relatives à la santé peuvent être traitées dès lors que la personne concernée a donné son consentement, sauf dans les cas où le droit prévoit qu'une interdiction de traiter les données de santé ne peut être levée par le seul consentement de la personne concernée. Lorsque le consentement de la personne concernée au traitement de ses données relatives à la santé est requis, conformément au droit, celui-ci devrait être libre, spécifique, éclairé et explicite. Il peut être exprimé par voie électronique. La personne concernée doit être informée de son droit de retirer son consentement à tout moment et du fait qu'un tel retrait ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. Il doit être aussi simple de retirer son consentement que de le donner.

5.3 Les données relatives à la santé peuvent être traitées dès lors que le traitement est nécessaire à l'exécution d'un contrat conclu par ou au nom de la personne concernée avec un professionnel de santé soumis aux conditions définies par la loi, y compris une obligation de secret.

5.4 Les données relatives à la santé qui ont été manifestement rendues publiques par la personne concernée peuvent être traitées.

5.5 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 afin de garantir le respect des droits et libertés fondamentales.

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 de leurs caractéristiques génétiques devraient bénéficier d'une protection appropriée.

7. Données génétiques relatives à la santé

7.1. Les données génétiques ne devraient être collectées que sous réserve des garanties appropriées et que si la loi le prévoit, ou que le consentement de la personne concernée a été recueilli conformément aux dispositions du principe 5.2, sauf lorsque la loi exclut le consentement comme fondement légal du traitement.

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 dans le respect des garanties procédurales appropriées, lorsqu'il n'existe aucune autre alternative ou moyen moins intrusif de vérifier l'existence d'un tel lien génétique. Ces données ne devraient pas être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement, sauf si des garanties appropriées sont prévues par la loi.

7.4 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 que dans le respect absolu des critères applicables définis par la loi, au regard du type de test utilisé et du risque particulier à couvrir. Les dispositions de la Recommandation (2016)8 sur le traitement des données à caractère personnel relatives à la santé à des fins d'assurance, y compris les données résultant de tests génétiques sont également à prendre en compte en la matière.

7.5 La personne concernée a le droit de connaître toute information relative à sa santé. Par ailleurs, pour des raisons qui lui appartiennent, la personne concernée peut souhaiter ne pas connaître certains éléments relatifs à sa santé et toute personne devrait être informée, préalablement à la réalisation de tests, de la possibilité dont elle dispose de ne pas être informée de résultats, y compris de découvertes inattendues. Le souhait de ne pas savoir peut, dans des circonstances exceptionnelles, faire l'objet de restrictions prévues par la loi, notamment dans l'intérêt de la personne concernée ou au regard de l'obligation de soigner qui incombe aux médecins.

8. Partage de données relatives à la santé à des fins de prise en charge et d'administration de soins de santé

8.1 En cas de partage de données relatives à la santé entre professionnels aux fins de prise en charge et d'administration de soins de santé d'un individu, la personne concernée sera informée préalablement, sauf impossibilité en cas d'urgence ou conformément au principe 11.4. Lorsque le partage repose sur le consentement de la personne concernée, conformément au principe 5.2, un tel consentement peut à tout moment être retiré. Lorsque le partage est rendu possible par la loi, la personne concernée doit pouvoir s'opposer au partage de ses données relatives à la santé.

8.2 Les professionnels intervenant dans un cas individuel spécifique dans le secteur sanitaire et médico-social et partageant des données dans un but d'amélioration de la coordination visant à assurer la qualité des soins de santé devraient être soumis au secret professionnel imposé aux professionnels de santé ou aux mêmes règles de confidentialité.

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. Les mesures appropriées doivent être prises afin de garantir la sécurité des données.

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 devraient respecter ces principes.

8.5 Dans le cadre de l'échange ou du partage de données relatives à la santé, des mesures physiques, techniques et administratives de sécurité devraient être adoptées, de même que des mesures nécessaires pour garantir leur confidentialité, leur intégrité et leur disponibilité.

9. Communication des données relatives à la santé pour des motifs autres que la prise en charge et l'administration de soins de santé

9.1 Les données relatives à la santé peuvent être communiquées à des destinataires autorisés par le droit à obtenir un accès aux données.

9.2 Les 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 le prévoit moyennant des garanties appropriées et si la personne concernée y a consenti conformément aux conditions prévues au principe 5.2.

9.3 A moins que la loi ne prévoie d'autres garanties appropriées, la communication des données relatives à la santé 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 équivalentes.

10. Conservation des données de santé

Les données ne devraient 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 fondamentales de la personne. Dans ce cas, les données devraient, en principe, être anonymisées dès que la recherche, l'activité archivistique ou l'étude statistique le permet.

Chapitre III. Les droits de la personne concernée

11. Transparence du traitement

11.1 La personne concernée doit être informée du traitement de ses données relatives à la santé par celui qui en est responsable.

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 l'existence, le cas échéant, de son fondement légal,
- la durée de conservation des 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 principe 12.2,
- 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 doit, le cas échéant afin de garantir la loyauté et la transparence du traitement, également porter sur :

- la possibilité de traiter ultérieurement ses données pour une finalité compatible dans le respect de garanties appropriées prévues par le droit et dans les conditions prévues au principe 4.1b,
- 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, y compris le profilage qui n'est acceptable que si la loi le permet et sous réserve de garanties appropriées.

11.2 Cette information doit être fournie préalablement à la collecte des données ou lors de la première communication.

11.3 L'information doit être compréhensible et facilement accessible, formulée dans un langage clair et adapté aux circonstances, afin de permettre à la personne concernée de bien comprendre le traitement de données envisagé. En particulier, lorsque la personne est dans l'incapacité physique ou juridique de recevoir cette information, celle-ci pourra être donnée à la personne qui la représente légalement. Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient traitées.

11.4 Une dérogation au droit d'information est permise si la personne concernée détient déjà les informations nécessaires. En outre, lorsque les données à caractère personnel ne sont pas obtenues de la part de la personne concernée, il ne devrait pas être demandé au responsable du traitement d'apporter une telle information dans le cas où le traitement est expressément prévu par la loi, que cela s'avère impossible ou encore quand cela exige des efforts disproportionnés de la part du responsable du traitement, notamment dans le cadre d'un traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

11.5 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.

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

12. Accès aux données, rectification, effacement, opposition au traitement et portabilité des données

12.1 La personne concernée 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'obtenir la communication et d'avoir accès au moins aux informations suivantes, sans délais et frais excessifs, sous une forme intelligible et dans les mêmes conditions :

- 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,
- le raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués, notamment en cas de profilage.

12.2 La personne concernée a le droit à la suppression des données traitées en violation de cette recommandation. Elle 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 ou à moins que le responsable du traitement ne démontre des raisons impérieuses et légitimes justifiant la poursuite du traitement des données.

12.3 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.

12.4 La personne concernée a le droit de ne pas faire l'objet d'une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé, y compris le profilage (voir notamment la Recommandation (2010)13 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage), de ses données relatives à la santé. Il est uniquement possible de déroger à cette interdiction lorsque la loi prévoit qu'un tel traitement puisse être basé sur le consentement de la personne concernée ou que le traitement est nécessaire pour des motifs d'intérêt public important, une telle loi devant être proportionnée à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts de la personne concernée.

12.5 Dès lors que le traitement est effectué à l'aide de procédés automatisés, la personne concernée devrait pouvoir obtenir du responsable du traitement, sous réserve des conditions prévues par la loi, qu'il lui transmette ses données dans un format structuré, lisible mécaniquement et interopérable, afin de les transmettre à un autre responsable du traitement (portabilité des données). La personne peut également exiger que le responsable du traitement transmette lui-même ses données à un autre responsable du traitement.

12.6 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.

12.7 Le droit d'être informé et les autres droits des personnes concernées peuvent faire l'objet de restrictions dès lors qu'elles sont prévues par la 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'État ayant trait à la santé publique.

Chapitre IV. Sécurité et interopérabilité

13. Sécurité

13.1 Le traitement des données relatives à la santé doit être sécurisé. A cet égard, des mesures de sécurité adaptées aux risques pour les droits de l'homme et libertés fondamentales doivent être définies afin de garantir que chaque partie prenante observe un niveau d'exigence élevé pour assurer la licéité du traitement ainsi que la sécurité et la confidentialité de ces données.

13.2 Ces règles de sécurité définies par le droit, et éventuellement inscrites dans des référentiels, maintenues à l'état de l'art et révisées de façon régulière, devraient 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 ou altération et de prévenir tout accès non autorisé et toute indisponibilité ou inaccessibilité. En particulier, la loi devrait prévoir d'organiser et d'encadrer les modalités de collecte, de conservation et de restitution des données relatives à la santé.

13.3 La disponibilité d'un système - c'est-à-dire son bon fonctionnement - devrait être assurée par des mesures de nature à rendre accessibles les données de façon sécurisée et dans le respect du niveau d'habilitation des personnes autorisées.

13.4 Le respect de l'intégrité impose de vérifier toute action effectuée sur les 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 y accéder.

13.5 L'auditabilité devrait conduire à disposer d'un système permettant de tracer tous les accès au système d'information et les modifications et actions effectuées sur les données et de pouvoir en identifier l'auteur.

13.6 L'activité qui consiste à faire héberger de façon externalisée 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.

13.7 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'information, peuvent accéder aux données relatives à la santé dans la mesure indispensable à l'accomplissement de leurs tâches et de façon ponctuelle. Ils doivent respecter le secret professionnel et se conformer à toute mesure appropriée prévue par la loi pour garantir la confidentialité et la sécurité de ces données.

14. Interopérabilité

14.1 L'interopérabilité, qui est la possibilité pour différents systèmes d'information de communiquer et d'échanger des données, peut permettre de répondre à des impératifs relevant du domaine de la santé. Elle peut apporter des moyens techniques qui facilitent la mise à jour, qui évitent la duplication de données identiques dans de multiples bases de données ou qui contribuent à la portabilité.

14.2 Il est cependant nécessaire que l'interopérabilité soit mise en œuvre conformément aux principes contenus dans cette recommandation, notamment les principes de licéité, de nécessité et de proportionnalité et que des mesures de sauvegarde de la protection des données à caractère personnel soient prises lorsque des systèmes interopérables sont utilisés.

14.3 Des référentiels basés sur des normes internationales et offrant un cadre technique qui facilitent l'interopérabilité devraient veiller à ce qu'un haut niveau de sécurité soit garanti tout en offrant une telle interopérabilité. Leur mise en œuvre peut être suivie, par exemple en recourant à des schémas de certification.

Chapitre V. La recherche scientifique

15. La recherche scientifique

15.1 Le traitement des données relatives à la santé à des fins de recherche scientifique devrait être encadré de garanties appropriées prévues par la loi, complétant les autres prescriptions de cette recommandation, être effectué dans un but légitime et être conforme aux droits et libertés fondamentales de la personne concernée.

15.2 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 données génétiques, par sa famille biologique.

15.3 Les données relatives à la santé ne devraient être traitées dans un projet de recherche que si la personne concernée y a consenti (dans le respect des conditions prévues au principe 5.2). A titre d'exception, la loi peut prévoir le traitement de données relatives à la santé à des fins de recherche. Une telle loi devrait être proportionnée à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. Ces sauvegardes devraient expressément prévoir l'obligation de mettre en place des mesures techniques et d'organisation pour garantir le respect du principe de minimisation des données.

15.4 En plus des prescriptions du Chapitre III, 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'éventuelles communications ;

– 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.

15.5 Le responsable du traitement ne devrait pas avoir à fournir cette information si les conditions décrites au principe 11.4 sont remplies. En outre, la loi peut prévoir des dérogations à ses obligations d'informer la personne concernée si les données relatives à la santé n'ont pas été obtenues auprès d'elle et si l'obligation de l'informer risque de rendre impossible ou de sérieusement empêcher d'atteindre les objectifs de recherches spécifiquement visés. Dans un tel cas, le responsable du traitement devrait prendre des mesures appropriées pour protéger les droits et les libertés fondamentales de la personne concernée ainsi que ses intérêts légitimes, y compris en rendant l'information disponible publiquement.

15.6 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 donner un consentement uniquement pour certains domaines de recherche ou certaines parties de projets de recherche, dans la mesure où la finalité visée le permet et en tenant compte des normes éthiques reconnues.

15.7 Les conditions de traitement des données relatives à la santé à des fins de recherche scientifique doivent être appréciées, le cas échéant, par l'organisme compétent désigné par la loi (comité d'éthique).

15.8 Les professionnels de santé habilités à mener leurs propres recherches médicales et les scientifiques d'autres disciplines 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 principe 15.4 et dans le respect des garanties complémentaires prévues par le droit, telles que la demande d'un consentement explicite ou une évaluation par l'organisme compétent désigné par la loi.

15.9 L'anonymisation doit être pratiquée dès lors que les objectifs poursuivis par les recherches scientifiques le permettent, et dans le cas contraire, la pseudonymisation des données, avec intervention d'un tiers de confiance lors de la séparation de l'identification, est au nombre des mesures qui devraient être mises en œuvre afin de garantir le respect des droits et libertés fondamentales de la personne concernée. Ceci doit être mis en œuvre 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.

15.10 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 de manière à ne pas compromettre la validité scientifique de la recherche et la personne concernée devrait en être informée.

15.11 Les données à caractère personnel utilisées à des fins de recherche scientifique ne devraient pas être publiées sous une forme permettant d'identifier les personnes concernées sauf :

a. si la personne concernée a donné son consentement pour cela ;

b. si la loi permet une telle publication à la condition qu'elle soit indispensable à la présentation des résultats de recherche au cours de manifestations contemporaines et seulement dans la mesure où l'intérêt de publier les données prime sur les intérêts comme sur les droits et libertés fondamentales de la personne concernée.

Chapitre VI. Les dispositifs mobiles

16. Dispositifs mobiles

16.1 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 son état physique ou mental en lien avec sa santé et son bien-être ou concernent toute information relative à sa prise en charge sanitaire et médico-sociale, elles constituent des données relatives à la santé. A ce titre elles bénéficient 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 cette recommandation et, le cas échéant, complétées par le droit.

16.2 Les personnes qui utilisent ces applications mobiles, dès lors qu'elles génèrent le traitement de leurs données à caractère personnel, doivent bénéficier des mêmes droits que ceux visés au Chapitre III de cette 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, une information claire et transparente sur le traitement envisagé doit être rédigée par le responsable du traitement, avec le concours du fabricant et du distributeur du dispositif dont les rôles doivent être précisés à l'avance.

16.3 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.

16.4 L'hébergement externe 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.

Chapitre VII. Flux transfrontières de données relatives à la santé

17. Protéger les flux de données relatives à la santé

17.1 Les formes diverses et variées de traitement de données relatives à la santé (applications mobiles, partage, environnement cloud mondial, etc.) conduisent à une augmentation de la nature transfrontière de ces traitements.

17.2 Les flux transfrontières de données ne peuvent avoir lieu que lorsqu'un niveau approprié de protection des données est garanti, conformément aux dispositions de la Convention 108, ou sur la base du régime dérogatoire suivant, qui vise à permettre le transfert de données à un destinataire qui n'assure pas un tel niveau approprié de protection dès lors que :

a. la personne concernée a donné son consentement au transfert, après avoir été informée des risques introduits par l'absence de garanties appropriées ; ou
b. des intérêts spécifiques de la personne concernée le nécessitent dans un cas particulier ; ou
c. des intérêts légitimes prépondérants, notamment des intérêts publics importants, sont prévus par la loi et que le transfert constitue une mesure nécessaire et proportionnée dans une société démocratique.