PROTECTION DES DONNÉES RELATIVES À LA SANTÉ

Recommandation CM/Rec(2019)2

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PROTECTION DES DONNÉES RELATIVES À LA SANTÉ

Recommandation CM/Rec(2019)2
adoptée par le Comité des Ministres
du Conseil de l'Europe
le 27 mars 2019

Conseil de l'Europe

Édition anglaise :
Protection of health-related data

Couverture et mise en page :
Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

Recommandation CM/Rec(2019)2

(adoptée par le Comité des Ministres le 27 mars 2019, lors de la 1342e réunion des Délégués des Ministres)

Le Comité des Ministres, en vertu de l'article 15.*b* du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Conscient de l'utilisation croissante des nouvelles technologies dans le traitement de données relatives à la santé ;

Eu égard aux dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[1] 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), et convaincu de l'intérêt de faciliter l'application de ces principes aux traitements de données relatives à la santé ;

Observant que les États sont aujourd'hui confrontés à des enjeux majeurs liés au traitement des données relatives à la santé dont l'environnement, depuis l'adoption de la Recommandation n° R (97) 5 du Comité des Ministres aux États membres relative à la protection des données médicales, a considérablement évolué ;

Constatant que 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 ;

1. Le protocole portant amendement à la Convention 108 (STCE nº 223) a été ouvert à la signature le 10 octobre 2018, et la convention ainsi révisée doit encore entrer en vigueur.

Considérant que les bénéfices de cette dématérialisation croissante des données peuvent se traduire à maints égards, notamment en matière d'amélioration des politiques de santé publique, des soins ou de la prise en charge des patients, et que la perspective de tels bénéfices exige 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 mesures juridiques et techniques de nature à permettre une protection effective des personnes concernées ;

Notant que la volonté des personnes de contrôler davantage leurs données personnelles et de maîtriser les décisions fondées sur le traitement de ces données et l'implication croissante des patients dans la compréhension de la façon dont des décisions qui les concernent sont prises contribuent également à cette évolution ;

Notant par ailleurs que la mobilité géographique qui s'accompagne d'un développement d'applications mobiles liées à la santé, de dispositifs médicaux et d'objets connectés contribue 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 ;

Observant que ce constat partagé par les États membres conduit à remplacer la Recommandation n° R (97) 5 du Comité des Ministres aux États membres relative à la protection des données médicales, et à employer le terme plus général de « données relatives à la santé » dans la nouvelle recommandation, tout en réaffirmant 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 ;

Considérant que 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 ;

Convaincu que toute personne a droit à la protection de ses données relatives à la santé et que, dans le cadre de ses relations avec un professionnel du secteur de la santé ou du secteur médico-social, la personne prise en charge a droit au respect de sa vie privée et à la confidentialité des informations la concernant ;

Soulignant que le traitement des données relatives à la santé devrait toujours 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,

Recommande aux gouvernements des États membres :

- de prendre des mesures afin d'assurer que les principes contenus dans l'annexe à cette recommandation, qui remplace la Recommandation n° R (97) 5 susmentionnée, sont reflétés dans leur droit et leur pratique ;
- d'assurer, à cette fin, que cette recommandation et son annexe sont portées à l'attention des autorités responsables des systèmes de santé, à charge pour celles-ci d'en assurer la promotion vers les différents acteurs qui traitent les données relatives à la santé, en particulier les professionnels de santé ainsi que les délégués à la protection des données ou les personnes assurant des fonctions similaires ;
- de promouvoir l'acceptation et l'application des principes contenus dans l'annexe à 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 qu'ils sont 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(2019)2

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 de sauvegarde des droits de l'homme et des libertés fondamentales (STE n° 5, « 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

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

2.2. 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 :

- « donnée à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;
- « 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 ;
- « anonymisation » désigne le procédé appliqué aux données à caractère personnel pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement ;
- « 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 soient pas attribuées à une personne physique identifiée ou identifiable. Les données pseudonymisées sont des données à caractère personnel ;
- « 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 ;

– « données génétiques » désigne toutes les données relatives aux caractéristiques génétiques d'une personne, qu'elles aient été héritées ou acquises lors du développement prénatal, résultant de l'analyse d'un échantillon biologique de cette personne, notamment une analyse des chromosomes, de l'ADN ou de l'ARN, ou de tout autre élément permettant d'obtenir des informations équivalentes ;

– « 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 ;

– « 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 ;

– « 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. Ces référentiels peuvent être rendus opposables par le droit ;

– « interopérabilité » désigne la possibilité pour différents systèmes d'information de communiquer et d'échanger des données ;

– « dispositifs 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 ;

– « professionnels de santé » recouvre tout professionnel reconnu en tant que tel par la loi, exerçant dans le secteur sanitaire, médico-social ou social, astreint à une obligation de confidentialité et délivrant des soins de santé ;

– « 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 – 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 qui suivent :

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 fondamentales de la personne.

c. Le traitement des données doit être nécessaire et proportionné à la finalité légitime poursuivie, et ne devrait être effectué que sur la base du consentement de la personne concernée tel que défini au principe 5.*b* 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 des derniers développements technologiques, 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, ou la destruction, la perte, l'utilisation, l'indisponibilité, l'inaccessibilité, la modification ou la divulgation de celles-ci.

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, 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 du cycle 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. Les responsables du traitement ainsi que les sous-traitants agissant sous leur responsabilité devraient prendre toutes les mesures appropriées afin de se conformer à leurs 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 équivalant à celui qui incombe 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 qui suivent.

a. 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 :

– 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 prévues par la loi ;

- pour des motifs de santé publique, tels que 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, aux produits de santé et aux dispositifs médicaux, dans les conditions prévues par la loi ;
- aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne lorsque le consentement ne peut être recueilli ;
- 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 de la loi ou de tout accord collectif respectueux de cette dernière ;
- 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 prévues par la loi ;
- 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 (en ce qui concerne notamment les traitements de données relatives à la santé à des fins de recherche, voir les conditions prévues au chapitre V) ;
- pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- pour des motifs d'intérêt public important, sur la base de la loi, qui doivent être proportionnés 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.

b. 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. 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.

c. 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.

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

e. 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 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.*b*, sauf lorsque la loi exclut le consentement comme fondement légal du traitement des données génétiques. Les dispositions de la Recommandation CM/Rec(2015)5 du Comité des Ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi sont à prendre en compte dès lors que le traitement de données génétiques intervient dans le cadre de l'emploi.

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 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. Le traitement de données génétiques peut être réalisé aux fins d'identification des personnes dans le cadre de crises ou d'actions humanitaires sous réserve que des garanties appropriées soient prévues par la loi.

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 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 CM/Rec(2016)8 du Comité des Ministres aux États membres 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.

7.6. La personne concernée a le droit de connaître toute information relative à ses données génétiques sous réserve des dispositions des principes 11.8 et 12.7. Toutefois, 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 d'un test, 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 différents professionnels aux fins de prise en charge et d'administration de soins de santé d'une personne, la personne concernée sera informée préalablement, sauf impossibilité en cas d'urgence ou conformément au principe 11.6. Lorsque le partage repose sur le consentement de la personne concernée, conformément au principe 5.*b*, 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 aux mêmes règles de confidentialité que les professionnels de santé.

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. Chaque professionnel de santé ne peut, dans ce cas, transmettre ou recevoir que les données qui relèvent du périmètre de ses missions, en fonction de ses habilitations. Des mesures appropriées devraient 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 devrait 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 la confidentialité, l'intégrité et la disponibilité de ces données.

9. Communication des données relatives à la santé pour des finalités 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 la loi à obtenir un accès aux données.

9.2. Les compagnies d'assurances ne peuvent pas être considérées comme des destinataires autorisés à accéder aux données relatives à la santé des personnes, sauf si le droit le prévoit moyennant des garanties appropriées et conformément au principe 5.

9.3. Les employeurs ne peuvent pas être considérés comme des destinataires autorisés à accéder aux données relatives à la santé des personnes, sauf dans les conditions posées dans la Recommandation CM/Rec(2015)5 du Comité des Ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi.

9.4. À 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 relatives à la santé 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 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 – Droits de la personne concernée

11. Transparence du traitement

11.1. Le responsable du traitement doit informer la personne concernée du traitement de ses données relatives à la santé.

11.2. L'information doit porter sur :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, de celles 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 la disposition de la personne concernée pour exercer auprès du responsable du traitement ses droits d'accès, de rectification et d'effacement de ses données.

11.3. L'information doit, le cas échéant, afin de garantir la loyauté et la transparence du traitement, également porter sur :

- la possibilité de traiter ultérieurement les données de la personne concernée pour une finalité compatible, dans le respect de garanties appropriées prévues par le droit et dans les conditions prévues au principe 4.1.*b ;*
- 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.

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

11.5. 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 également informée avant que les données qui la concernent soient traitées.

11.6. Le responsable du traitement n'est pas tenu de fournir cette information si la personne la détient déjà. En outre, lorsque les données à caractère personnel ne sont pas obtenues directement auprès de la personne concernée, le responsable du traitement n'est pas tenu de l'informer dès lors que le traitement est expressément prévu par la loi ou que cela s'avère impossible, par exemple parce que les coordonnées de la personne ont changé et qu'elle n'a pu être retrouvée ou qu'elle est perdue de vue, 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.

11.7. Le souhait d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic devrait être respecté, sauf lorsque cela constitue un risque sérieux pour la santé de tiers.

11.8. Le responsable du traitement n'est pas tenu d'informer la personne concernée si des dispositions sont prévues par la loi, et si celles-ci constituent des mesures nécessaires et proportionnées dans une société démocratique pour les motifs énumérés à l'article 9 de la Convention 108.

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 ou 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 ces 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 des dispositions de la Convention 108. Elle a le droit d'obtenir la 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 que ces données 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[2], de ses données relatives à la santé. Il devrait être uniquement possible de déroger à cette interdiction lorsque la loi prévoit qu'un tel traitement puisse être fondé sur le

2. Se référer notamment à la Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.

consentement de la personne concernée ou que le traitement est nécessaire pour des motifs d'intérêt public important. Les dispositions d'une telle loi devraient être proportionnées 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 des 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 concernée pourrait 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 tous les moyens nécessaires pour s'assurer du respect de l'exercice effectif de ces droits dans le cadre de leur déontologie professionnelle.

12.7. Les droits des personnes concernées peuvent faire l'objet de restrictions dès lors qu'elles sont prévues par la loi et qu'elles constituent des mesures nécessaires et proportionnées dans une société démocratique pour les motifs énumérés à l'article 9 de la Convention 108.

12.8. La loi devrait prévoir les garanties appropriées de nature à assurer le respect des droits de la personne.

Chapitre IV – Sécurité et interopérabilité

13. Sécurité

13.1. Le traitement des données relatives à la santé doit être sécurisé. À cet égard, des mesures de sécurité adaptées aux risques pour les droits de l'homme et les libertés fondamentales doivent être définies et appliquées 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. Les règles de sécurité prévues par la loi ou autres réglementations et, le cas échéant, inscrites dans des référentiels devraient se traduire par l'adoption de mesures techniques et organisationnelles maintenues à l'état de l'art et 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 procéder à une vérification des actions effectuées 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 peuvent y accéder.

13.5. La possibilité de l'audit 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 peut permettre de répondre à des impératifs relevant du domaine de la santé et peut apporter des moyens techniques qui facilitent la mise à jour, qui évitent la duplication de données identiques dans de multiples bases de données et 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 fondés sur des normes internationales et offrant un cadre technique qui facilite l'interopérabilité devraient assurer qu'un haut niveau de sécurité est garanti tout en offrant une telle interopérabilité. Leur mise en œuvre peut être suivie au moyen de schémas de certification.

Chapitre V – Recherche scientifique

15. 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 dispositions 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 de données relatives à la santé pour une recherche scientifique devrait être appréciée au regard de la finalité poursuivie par le projet de recherche 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, en principe, être traitées dans un projet de recherche scientifique que si la personne concernée y a consenti dans le respect des conditions prévues au principe 5.*b*. Cependant, la loi peut prévoir le traitement de données relatives à la santé à des fins de recherche sans que la personne concernée y ait consenti. Les dispositions d'une telle loi devraient être proportionnées 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 organisationnelles 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 préalable si les conditions décrites au principe 11.6 sont remplies. En outre, et sans préjudice des dispositions de la Recommandation CM/Rec(2016)6 du Comité des Ministres aux États membres sur la recherche utilisant du matériel biologique d'origine humaine, 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 indépendant compétent (par exemple un 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 indépendant compétent désigné par la loi.

15.9. L'anonymisation doit être pratiquée dès lors que les objectifs poursuivis par les recherches scientifiques le permettent ; 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. Ces mesures doivent être mises 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 devraient 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 ; ou

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 – 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 que ces données 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. À 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 cette recommandation.

16.2. Les personnes qui utilisent ces dispositifs mobiles, dès lors que ces derniers génèrent le traitement de leurs données à caractère personnel,

devraient 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. À 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 dispositifs 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 dispositifs 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

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 explicite, spécifique et libre 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 ; ou

d. ce transfert constitue une mesure nécessaire et proportionnée pour la liberté d'expression dans une société démocratique.

Le développement du numérique a conduit à une véritable « datification » de nos sociétés. Les données personnelles sont partout et constituent une matière première précieuse pour la création de nouvelles connaissances et un enjeu mondial de croissance majeur pour de nombreux pays.

Le secteur de la santé n'échappe pas à ces évolutions du fait d'une part de sa numérisation générale et de l'usage désormais fréquent des outils numériques par les professionnels dans le cadre notamment des activités de soins et de prévention, de recherche en sciences de la vie, de gestion des systèmes de santé, et d'autre part de l'implication croissante des personnes concernées par les soins.

Les données relatives à la santé, touchant aux informations les plus intimes de la personne et de sa vie privée, doivent bénéficier d'un statut particulier qui prenne en compte le risque potentiel de discrimination résultant de leur traitement.

Cette recommandation vise à faciliter la pleine application des principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la « Convention 108 ») ainsi que de prendre en compte les principes développés dans la Convention modernisée et de les appliquer à ce nouvel environnement d'échange et de partage des données relatives à la santé.

PREMS 052419

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE