Nations Unies A/74/277*

Assemblée générale

Distr. générale
5 août 2019
Français
Original : anglais

Soixante-quatorzième session
Point 72 b) de l'ordre du jour provisoire**
Promotion et protection des droits de l'homme : questions relatives aux droits de l'homme, y compris les divers moyens de mieux assurer l'exercice effectif des droits de l'homme et des libertés fondamentales

Droit à la vie privée

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale le rapport établi par le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, en application de la résolution 28/16 du Conseil des droits de l'homme.

* Nouveau tirage pour raisons techniques (3 septembre 2019)
** A/74/150.

19-13343X* (F)

Rapport du Rapporteur spécial sur le droit à la vie privée

Résumé

Le présent rapport a été établi par le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, et transmis en application de la résolution 28/16 du Conseil des droits de l'homme.

Le rapport contient un résumé des activités et une recommandation sur la protection et l'utilisation des données de santé.

I. Résumé des activités

1. Depuis octobre 2018, le Rapporteur spécial sur le droit à la vie privée s'est rendu en Allemagne, en Argentine et en République de Corée. Il rendra compte de ces visites au Conseil des droits de l'homme en 2020. Les travaux sur la question de la surveillance se sont poursuivis, notamment avec le Forum international de contrôle des services de renseignement, qui s'est tenu à Malte en 2018 et se tiendra à Londres en 2019. Le Rapporteur spécial remercie les gouvernements des pays hôtes d'avoir soutenu ces événements, qui ont abouti à l'élaboration d'un principe applicable à l'échange international de données de renseignement : « *Tout transfert est contrôlable* ». Le Rapporteur spécial a élaboré un projet de rapport sur la question du genre, qui sera présenté lors d'une consultation prévue à New York les 30 et 31 octobre 2019, ainsi que des directives sur la protection de la vie privée et des directives concernant les méthodes de mesure de la protection des données personnelles des enfants. Il a aussi élaboré la recommandation qui figure dans l'annexe du présent rapport. Le Rapporteur spécial remercie le Conseil de l'Europe d'avoir participé à l'accueil de la réunion de consultation sur les données de santé en juin 2019.

II. Données de santé

2. Le droit qu'a toute personne de jouir du meilleur état de santé physique et mentale possible a été reconnu par la Déclaration universelle des droits de l'homme (art. 25) et les instruments internationaux des droits de l'homme tels que le Pacte international relatif aux droits économiques, sociaux et culturels (art. 12), la Convention relative aux droits de l'enfant (art. 24), la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (art. 12) ou la Convention relative aux droits des personnes handicapées (art. 25).

3. On a de plus en plus conscience du caractère sensible des données de santé. À l'ère du numérique, elles sont recueillies et utilisées d'une multitude de façons, souvent sans le consentement de la personne concernée ou sans que celle-ci en soit informée. L'industrie de la collecte et de l'exploitation des données de santé et le nombre croissant de violations de données sont extrêmement préoccupants.

4. C'est dans ce contexte que le Rapporteur spécial a créé en 2017 l'Équipe spéciale chargée de la question de la vie privée et de la protection des données de santé afin qu'elle formule à l'intention des États Membres une recommandation sur la protection et l'utilisation des données de santé, qui puisse être utilisée comme référence internationale en matière de normes minimales de protection de ce type de données. La recommandation est le fruit de consultations mondiales et tient compte des observations de plusieurs centaines de parties prenantes.

5. L'élaboration de la recommandation a été coordonnée par le secrétaire de l'Équipe spéciale, Sean McLaughlan, dirigée par son président, Nikolaus Forgó, et menée avec le concours des membres de l'Équipe : Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Trix Mulder, Katerina Polychronopoulos, Chris Puplick, Mariana A. Rissetto, William Smart, Sam Smith, Jane Kaye, Steve Steffensen, Thomas Trezise, Melania Tudorica, Marie-Catherine Wagner et Helen Wallace.

6. La recommandation repose sur le principe que toute personne a le droit de jouir du meilleur état de santé physique et mentale possible et a le droit au niveau le plus élevé possible de protection de ses données de santé, indépendamment de tout critère relatif au handicap, au genre, à l'identité de genre, à l'expression du genre ou autres

facteurs. Elle met l'accent sur l'importance du consentement pour protéger la dignité humaine et l'intégrité, tout en ménageant un espace pour les utilisations des données sanitaires qui servent l'intérêt public (comme la recherche scientifique), sous réserve des garanties appropriées.

7. La texte figurant en annexe est une version abrégée de la recommandation, qui met les principaux éléments en relief. Aux fins de sa transposition dans le droit interne, les États sont invités à utiliser la version intégrale, disponible à l'adresse www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf.

Annexe

Recommandation sur la protection et l'utilisation de données de santé

Chapitre I

Dispositions générales

1. Objet

1.1. La présente recommandation a pour objet de fournir des principes directeurs concernant le traitement des données de santé.

1.2 Les orientations figurant dans la présente recommandation doivent servir de référence internationale pour les normes minimales de protection des données de santé.

2. Champ d'application

2.1 La présente recommandation s'applique au traitement des données de santé dans tous les secteurs de la société, public et privé compris.

2.2 La présente recommandation ne limite ni n'affecte en rien les lois accordant aux sujets dont les données sont traitées plus de droits, de protection et/ou de voies de recours que le minimum qu'elle propose.

2.3 La présente recommandation ne s'applique pas au traitement des données de santé réalisé par des personnes physiques dans le cadre d'activités purement personnelles ou domestiques.

3. Définitions

- « Action humanitaire » : activité entreprise en toute impartialité pour porter assistance ou secours et assurer la protection des personnes touchées en cas d'urgence humanitaire. L'action humanitaire peut comprendre l'assistance humanitaire, l'aide humanitaire et la protection[1].
- « Agent sanitaire » : toute personne participant à des activités dont le principal objectif est d'améliorer la santé.
- « Algorithmes médicaux » : logiciels ou algorithmes informatisés qui aident à prendre des décisions concernant la santé ou à analyser des informations relatives à la santé. Il s'agit notamment d'algorithmes avec et sans interférence humaine.
- « Anonymisation » : processus irréversible appliqué aux données personnelles pour que la personne concernée ne puisse être identifiée en aucune circonstance ni par quelque moyen que ce soit, directement ou indirectement, notamment par l'utilisation d'autres données ou par association avec d'autres données.
- « Applications mobiles » : moyens accessibles dans un environnement mobile permettant de communiquer et gérer des données de santé. Cela comprend différentes formes, comme les logiciels, les instruments et appareils médicaux

[1] Christopher Kuner et Massimo Marelli (dir.), *Handbook on Data Protection in Humanitarian Action* (Comité *international* de la Croix-Rouge, 2017).

et sanitaires portables connectés, pouvant être utilisés pour la prévention, le diagnostic, la surveillance et le traitement, la récréation ou le bien-être.

- « Assuré » : personne qui a conclu un contrat d'assurance ou prévoit de le faire. Cette définition s'applique également aux personnes couvertes par une assurance publique ou une assurance ayant un mandat légal.
- « Assureur » : société privée, organisme de sécurité sociale ou réassureur.
- « Atteinte à la protection des données de santé » : destruction, perte ou altération accidentelle ou illégale de données de santé ; divulgation non autorisée de telles données ; accès accidentel ou illégal à telles données ; blocage de l'accès licite à ces données (y compris les pratiques illégales d'enfermement propriétaire) ; vente de données de santé transmises, stockées ou autrement traitées. La présente définition exclut la destruction intentionnelle licite.
- « Autorité de surveillance compétente » : autorité publique indépendante dont le rôle est, exclusivement ou notamment, de surveiller l'application et le respect des dispositions de la présente recommandation.
- « Cadre de référence » : ensemble coordonné de règles et/ou de processus mis à jour, adaptés à la pratique et applicables aux systèmes d'information sanitaire, couvrant les domaines de l'interopérabilité et de la sécurité.
- « Consentement » : acte affirmatif clair (déclaration écrite, y compris électronique, ou orale) par lequel l'intéressé(e) indique de façon libre, précise, éclairée et sans ambiguïté, qu'elle ou il consent au traitement de données personnelles la ou le concernant. Cela peut inclure le fait de cocher une case lors de la visite d'un site Internet, le choix de paramètres techniques pour des services de la société de l'information ou tout autre déclaration ou comportement indiquant clairement dans ce contexte que la personne concernée accepte la proposition de traitement de ses données personnelles. Par conséquent, le silence, les cases pré-cochées ou l'inactivité ne sauraient être interprétés comme l'expression d'un consentement. Le consentement doit porter sur toutes les activités de traitement menées dans le(s) même(s) but(s). Si le traitement a plusieurs objectifs, le consentement doit être donné pour chacun d'entre eux. Si le consentement de la personne concernée est demandé par voie électronique, la demande doit être claire, concise et ne doit pas perturber inutilement l'utilisation du service pour lequel elle est requise.
- « Contrôleur » : personne(s) physique(s) ou morale(s), autorité publique, prestataire de services, agence ou tout autre organisme (individuellement ou collectivement) qui a/ont le pouvoir de décider du traitement de données de santé.
- « Données autochtones » : données, informations ou connaissances (sous toutes leurs formes et sur tout support) concernant ou pouvant toucher des peuples autochtones ou des populations des Premières Nations, collectivement ou individuellement, ou émanant de ces peuples et populations, pouvant inclure la langue, la culture, des données génétiques, des éléments environnementaux ou des ressources de peuples autochtones.
- « Données de santé » : toutes données personnelles concernant la santé physique et mentale d'une personne, y compris la prestation de services de soins de santé qui révèlent des informations sur l'état de santé passé, actuel et futur de cette personne. Les données génétiques entrent dans la catégorie des données de santé au sens de la présente recommandation. Les données de santé concernant, mais pas exclusivement, des données résultant d'essais, tels que le diagnostic prénatal, le diagnostic avant l'implantation ou découlant de l'identification des

caractéristiques génétiques, qu'elles soient ou non considérées comme des données de santé de la mère, doivent être protégées au même niveau que les autres données de santé.

- « Données génétiques » : toutes données personnelles concernant les caractéristiques génétiques d'un individu, qui ont été héritées ou acquises au cours du développement prénatal, ayant été obtenues par l'analyse d'un échantillon biologique de la personne concernée, en particulier, l'analyse de l'ADN ou de l'ARN chromosomique ou l'analyse de tout autre élément permettant d'obtenir des renseignements équivalents. Le caractère héréditaire de l'ADN signifie que l'analyse de l'ADN d'un individu peut également avoir des répercussions sur d'autres membres de la famille, groupes et populations. Il donne également des renseignements sur le phénotype d'un individu.

- « Données personnelles » : toute information concernant une personne physique identifiée ou identifiable (« personne concernée »).

- « Données publiques » : données disponibles pour l'utilisation et le partage sans restriction de lieu ou d'usage, et qui ne concernent pas des individus identifiables. Les données publiques peuvent être librement utilisées, partagées et élaborées par n'importe qui, partout et à toute fin. Elles peuvent être d'accès libre, présentées de façon pratique et sous un format modifiable et fournies dans des conditions permettant à tous la réutilisation et la redistribution, notamment les interactions et l'interopérabilité avec d'autres ensembles de données sans restriction.

- « Examen » : tout essai non génétique ou génétique ayant une valeur non clinique, diagnostique ou prédictive. Les résultats d'un examen ont une valeur de diagnostic s'ils confirment ou infirment un diagnostic médical. Les résultats d'un examen ont une valeur prédictive s'ils indiquent un risque d'apparition d'une maladie à l'avenir. La fiabilité des résultats des examens ayant une valeur prédictive est extrêmement variable d'une personne à l'autre. La notion d'examen couvre également les utilisations faites par les forces de l'ordre (par exemple analyses d'ADN aux fins d'investigations en cours ou prévisionnelles).

- « Gouvernance des données autochtones » : droit des peuples autochtones de décider de manière autonome, comment et pourquoi les données sont recueillies, accessibles au public et utilisées. Pareille gouvernance a pour objet de veiller à ce que les données concernant les peuples autochtones tiennent compte des priorités, valeurs, cultures, conceptions du monde ainsi que de la diversité des peuples autochtones. Il s'agit notamment des principes, structures, mécanismes de responsabilité, instruments juridiques et politiques dans le cadre desquels les peuples autochtones exercent un contrôle sur les données autochtones.

- « Handicap » (notion en cours d'évolution) : la situation de handicap résulte de l'interaction entre des personnes présentant des incapacités et les barrières comportementales et environnementales qui font obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres. Par personnes en situation de handicap, on entend des personnes qui présentent des incapacités physiques, mentales, intellectuelles ou sensorielles durables dont l'interaction avec diverses barrières peut faire obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres.

- « Interopérabilité » : capacité des différents systèmes d'information de communiquer et d'échanger des données.

- « Intersectionnalité » : nature interdépendante des catégorisations sociales telles que la race, la classe sociale et le genre, telles qu'elles s'appliquent à une

personne ou à un groupe donné, considérées comme créant un chevauchement et des systèmes interdépendants de discrimination ou de désavantages.

- « Organisation internationale » : organisation et ses organes subsidiaires régie par le droit international public ou tout autre organisme mis en place par, ou sur la base d'un accord, conclu entre deux ou plusieurs pays.
- « Personne concernée » : personne physique identifiée ou identifiable. Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant comme un nom, un numéro d'identification, des coordonnées géographiques, des éléments d'identification en ligne ou à un ou plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.
- « Profil » : ensemble de données de santé caractérisant une catégorie de personnes et destiné à être appliqué à un individu.
- « Profilage » : toute forme de traitement automatisé de données de santé consistant en l'utilisation de données sanitaires pour évaluer certains aspects personnels concernant une personne physique, en particulier pour étudier ou prévoir des aspects concernant les performances de cette personne physique au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa situation géographique ou ses mouvements.
- « Pseudonymisation » : tout traitement de données personnelles visant à ce qu'il ne soit plus possible d'identifier la personne concernée par les données sans utilisation d'informations supplémentaires conservées séparément et faisant l'objet de mesures techniques et institutionnelles (les données personnelles ne pouvant ainsi plus être attribuées à une personne physique identifiée ou identifiable). Les données pseudonymisées restent des données personnelles.
- « Recherche scientifique » : travaux créatifs et systématiques entrepris pour accroître la somme des connaissances et/ou pour concevoir de nouvelles applications des connaissances existantes. L'activité, dont les résultats ne sauraient être prévisibles, doit être novatrice, créative, systématique, transférable et/ou reproductible. Les facteurs permettant de déterminer si une activité relève de la recherche scientifique comprennent : le rôle de l'entité juridique où l'activité est exercée ; le rôle de la/des personne(s) physique(s) exerçant l'activité ; les normes de qualité appliquées, notamment l'utilisation d'une méthodologie scientifique et de publications scientifiques ; le respect des normes éthiques régissant la recherche. Toute activité de recherche menée dans toute discipline habilitée à traiter des données de santé (notamment les sciences médicales et les sciences de la santé, les sciences naturelles, le génie et la technologie, les sciences sociales, les sciences humaines et les beaux-arts) relève de la recherche scientifique. Celle-ci peut prendre la forme de recherche fondamentale, de recherche appliquée ou de développement expérimental. Elle inclut notamment l'analyse des politiques, les services de santé et l'épidémiologie. La recherche scientifique peut être financée par des fonds publics ou privés et menée par des entités publiques ou privées et peut, dans certains cas, être effectuée dans un but lucratif.
- « Recommandation » : le présent document.
- « Responsable de traitement » : personne physique ou morale, autorité publique, agence ou tout autre organisme, seul ou conjointement avec d'autres, qui traite

des données uniquement pour le compte du contrôleur et sur instructions de celui-ci.

- « Souveraineté des données autochtones » : droits et intérêts naturels des peuples autochtones en ce qui concerne la création, la collecte, l'accès, l'analyse, l'interprétation, la gestion, la diffusion, la réutilisation et le contrôle des données les concernant.
- « Système d'information sanitaire » : système fournissant les bases de la prise de décisions et remplissant plusieurs fonctions, telles que la production de données, la compilation, l'analyse, le stockage et la synthèse et la communication et l'utilisation. Le système d'information sanitaire recueille des données du secteur de la santé et d'autres secteurs concernés, analyse les données, assure leur qualité et leur pertinence générales, veille à ce qu'elles soient tenues à jour et convertit les données en informations utiles pour la prise de décisions sanitaires[2].
- « Test génétique » : examen effectué pour les besoins de l'analyse d'échantillons biologiques d'origine humaine et visant spécifiquement à recenser les caractéristiques génétiques d'une personne, qui ont été héritées ou acquises au début du développement prénatal. L'analyse entreprise dans le cadre de tests génétiques est effectuée sur les chromosomes, l'ADN ou l'ARN ou tout autre élément permettant d'obtenir des renseignements équivalents.
- « Traitement des données » : toute opération ou ensemble d'opérations effectué sur des données personnelles, tel que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, la vente, la préservation, l'adaptation ou l'altération, le retrait, l'accès, la consultation, l'utilisation, la divulgation, la diffusion, la mise à disposition, le partage, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction, ou la conduite d'opérations logiques ou arithmétiques sur des données personnelles et le traitement automatisé de données de santé.
- « Transfrontière » : qualifie ce qui traverse les frontières nationales, y compris les frontières infranationales intérieures à un État. Le transfert de données transfrontières se produit chaque fois que : des données sont transférées à travers des frontières nationales ; des données transmises d'un expéditeur à un destinataire situés dans un même État sont acheminées par l'intermédiaire d'un autre État ; une ou plusieurs personnes ont accès aux données, à distance, à partir d'un autre État ou peuvent l'avoir, dans certaines conditions.

Chapitre II

Conditions juridiques applicables au traitement des données de santé

4. Principes applicables au traitement des données de santé

4.1 Le traitement des données de santé est soumis au respect des principes ci-après :

a) Les données de santé doivent être traitées de manière transparente, légale et équitable ;

[2] Organisation mondiale de la Santé, *Cadre et normes applicables aux systèmes nationaux d'information sanitaire*, 2e édition (2008).

b) Les données de santé doivent être recueillies à des fins explicites, précises et légitimes, et ne doivent pas être traitées d'une manière incompatible avec les buts pour lesquels elles ont été initialement recueillies. La poursuite du traitement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ne doit pas être considérée comme étant incompatible avec les buts initiaux et être assortie de garanties appropriées concernant les droits et libertés de la personne concernée ;

c) Le traitement des données de santé doit être nécessaire et limité à l'objectif légitime poursuivi et être effectué conformément aux dispositions de la section 5 ;

d) Les données de santé doivent être recueillies, dans la mesure du possible, auprès de la personne concernée. Lorsque celle-ci n'est pas en mesure de fournir les données et que celles-ci sont indispensables pour les besoins du traitement, elles peuvent être obtenues à partir d'autres sources, conformément aux dispositions de la section 5 ;

e) Les données de santé doivent être adéquates, pertinentes, exactes et à jour et se limiter à remplir l'objectif pour lequel leur traitement doit être effectué. Elles doivent être adaptées à l'usage visé par le traitement des données ;

f) Le traitement des données de santé doit être assorti de dispositions de sécurité et de mesures institutionnelles adéquates. Des mesures de protection doivent garantir le respect des droits de la personne concernée et la sécurité des données de santé. Toute autre garantie éventuelle peut être fournie conformément à la loi qui veille au respect des droits et des libertés fondamentales des personnes concernées et des données relatives à leur santé ;

g) Les droits de la personne concernée doivent être respectés dans tous les cas où ses données de santé font l'objet d'un traitement. Il s'agit notamment des droits d'accès aux données et aux informations, à la rectification, à l'objection, à l'effacement et à la portabilité des données. La personne concernée doit avoir le droit de demander que ses données de santé conservées dans un système de traitement automatisé et/ou de fichiers ou dossiers sur support papier soient transmises à une autre entité de son choix, lorsque cela est techniquement possible à un coût raisonnable.

4.2 Lorsqu'ils concernent la santé, les principes du respect de la vie privée doivent être pris en compte par défaut (vie privée par défaut) et intégrés dans la conception des systèmes d'information (protection de la vie privée dès la conception).

4.3 La conformité avec tous les principes applicables aux données personnelles et aux données de santé, notamment mais non exclusivement, ceux figurant dans la présente recommandation, doit être régulièrement réexaminée. Le contrôleur doit procéder, avant que ne commence le traitement des données et à intervalles réguliers après leur traitement, à une évaluation écrite de l'incidence que pourrait avoir ce traitement sur la protection des données, l'usage fait des données et le respect de la vie privée des personnes concernées, y compris des mesures visant à atténuer tous les risques.

4.4 Les contrôleurs et les responsables du traitement doivent prendre toutes les mesures nécessaires pour s'acquitter de leurs obligations en matière de données de santé, notamment mais non exclusivement, celles figurant dans la présente recommandation, et doivent être capables de démontrer à une autorité de surveillance compétente que tous les traitements de données de santé sont (ou ont été) effectués conformément à toutes les obligations applicables.

4.5 Les contrôleurs et les responsables du traitement n'étant pas tenus de respecter un certain niveau de secret professionnel doivent s'assurer que tout traitement de

données de santé est effectué dans le respect des règles de confidentialité et des mesures de sécurité, de façon à mettre en place un niveau de protection équivalent à celui imposé aux travailleurs sanitaires.

5. Fondements juridiques du traitement des données de santé

5.1 Le traitement des données de santé est licite si, et dans la mesure où il est nécessaire, conformément aux dispositions de la section 4, il obéit aux principes énoncés dans la présente recommandation, et lorsque l'une des situations suivantes s'applique :

a) La personne concernée a donné son consentement libre, précis, éclairé et explicite au traitement de ses données, excepté lorsque la loi interdit à une personne concernée de consentir au traitement de ses données. Lorsque l'exigence de consentement n'est pas exclue par la loi, la personne concernée doit être informée, au moment où son consentement lui est demandé, de son droit de retirer son consentement à tout moment et être informée que tel retrait ne saurait avoir d'incidence sur la licéité du traitement déjà réalisé sur la base du consentement qu'elle a donné avant de le retirer. Il doit être aussi facile pour toute personne concernée de retirer son consentement que de le donner. La personne concernée doit disposer d'informations compréhensibles, claires et complètes lui permettant de prendre la décision de consentir ou de ne prendre aucune décision dans ce sens. Les personnes concernées ont droit au consentement éclairé avant le traitement ou autre utilisation de leurs données de santé ;

b) Le traitement des données est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat ;

c) Le traitement des données est nécessaire au respect d'une obligation légale à laquelle le contrôleur est soumis ;

d) Le traitement des données est nécessaire à la protection des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) Le traitement des données est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité dont est investi le contrôleur ;

f) Le traitement des données est nécessaire aux fins des intérêts légitimes poursuivis par le contrôleur ou par un tiers, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui exigent la protection des données personnelles, en particulier lorsque la personne concernée est un enfant ;

g) L'alinéa f) ne s'applique pas aux activités de traitement de données menées par des autorités publiques dans l'exercice de leurs fonctions.

5.2 Les fins du traitement de données de santé sont légitimes si elles :

a) Présentent des avantages directs pour la personne concernée (par exemple diagnostic, soins, traitement, rééducation ou convalescence) ;

b) Relèvent de la prévention sanitaire ou du diagnostic médical, de l'administration de soins ou de traitements ou de la gestion de services de santé par des agents sanitaires ou des agents du secteur social et médico-social, dans les conditions prévues par la loi ;

c) Relèvent de la santé publique. Le traitement des données peut ainsi concerner les maladies à déclaration obligatoire, la protection contre les risques sanitaires, l'identification et le confinement en cas de maladies transmissibles, les

risques pour l'environnement, l'action humanitaire. Il peut être effectué dans le but d'atteindre une qualité irréprochable et un niveau élevé de sécurité du traitement médical ou de protéger contre les dangers que peuvent présenter certains produits ou appareils médicaux, dans les conditions prévues par la loi ;

d) Concernent la protection des intérêts vitaux de la personne concernée ou d'un autre individu lorsque le consentement ne peut être obtenu auprès de la personne concernée, de l'autre individu, ou des deux à la fois ;

e) Relèvent de raisons relatives aux obligations des contrôleurs ou à l'exercice par la personne concernée de ses droits en matière d'emploi ou de protection sociale, conformément à la loi ou à toute convention collective légale ;

f) Satisfont à l'intérêt que le public porte au respect du principe de responsabilité dans la planification, le financement et la gestion des services de santé, la gestion des demandes de protection sociale et des prestations d'assurance maladie et de services, dans les conditions prévues par la loi ;

g) Relèvent de l'archivage d'intérêt public, tel que défini par la loi, au service de la recherche scientifique ou historique, sous réserve que soient évalués le rôle de l'entité juridique exerçant l'activité, le rôle de(s) l'individu (s) exerçant l'activité, les normes de qualité appliquées, y compris l'utilisation de méthodes scientifiques et de publications scientifiques ou les fins statistiques visées, dans le respect des conditions prévues par la loi pour garantir la protection des droits fondamentaux et des intérêts légitimes des sujets concernés par les données traitées (voir les conditions applicables au traitement des données de santé aux fins de la recherche scientifique, chapitre V) ;

h) Sont indispensables à la reconnaissance, l'exercice ou la défense d'une action en justice concernant des données de santé destinées au traitement ;

i) Sont indispensables à l'identification de personnes portées disparues et à la détermination du lieu où une personne a disparu (lorsque rien ne permet de croire que l'individu souhaite simplement éviter tout contact), lorsque les circonstances suscitent des inquiétudes pour leur sécurité et leur bien-être, en vertu d'une loi prévoyant des mesures spécifiques adaptées protégeant les droits et les intérêts de la personne concernée et des membres de sa famille.

5.3 Le traitement de données de santé déjà manifestement rendues publiques par la personne concernée est autorisé, à moins qu'il ne soit incompatible avec les droits de cette personne aux termes de la présente recommandation ou d'autres dispositions légales (comme dans le cas des conditions applicables à l'assurance). Les informations communiquées par la personne concernée à ses interlocuteurs sur les médias sociaux ne sont pas considérées comme des données de santé étant manifestement rendues publiques.

6. Données de santé des enfants

6.1 Les données de santé et les données génétiques concernant les enfants doivent être protégées au moins au même niveau que les autres données de santé. Chaque fois que le consentement éclairé constitue le fondement juridique du traitement des données personnelles de l'enfant, celui-ci a le droit d'être informé et il importe de prendre en compte la capacité d'un mineur de comprendre pleinement les conséquences du traitement et toutes les lois applicables en la matière.

6.2 Lorsque l'enfant a atteint l'âge de la majorité légale, il convient de lui demander son consentement (ou de renouveler son consentement) à sa participation à des travaux de recherche.

6.3 Les enfants ont le droit de retirer des données de santé de tout système d'information sanitaire lorsqu'ils atteignent l'âge de la majorité légale.

7. Données génétiques

7.1 Le traitement des données génétiques ne peut être effectué que sous réserve de garanties appropriées et lorsqu'il est prescrit par la loi ou avec le consentement de la personne concernée conformément au paragraphe 5.2, sauf lorsque la loi dispose que la personne concernée ne peut consentir à ce type de traitement de ses données génétiques ou n'a pas besoin de le faire.

7.2 Le traitement des données génétiques entrepris à des fins préventives, de diagnostic ou de traitement concernant le sujet des données ou un membre de sa famille biologique ou à des fins de recherche scientifique peut être utilisé dans le but particulier du traitement des données ; ou pour permettre à certaines personnes concernées par les résultats de ce traitement de données génétiques de prendre une décision éclairée, sans que leur soit révélé à traver les résultats la nature de leur degré de parenté avec le sujet des données si cette parenté n'est pas encore connue d'elles. Lorsque ces objectifs ont été atteints, les données génétiques doivent être détruites en l'absence de consentement de la personne concernée.

7.3 Les données prédictives existantes issues de tests génétiques ne doivent pas être traitées à d'autres fins, notamment à des fins d'assurance ou d'application de la loi, excepté dans les cas expressément prévus par une loi nécessaire et proportionnée.

7.4 La personne concernée a le droit de connaître ou d'ignorer les informations relatives à ses données génétiques résultant du traitement de ces données. Les personnes doivent être informées, préalablement à tout traitement de données, de la possibilité de ne pas être informées des résultats, y compris d'éventuelles découvertes fortuites.

8. Mise en commun de données de santé dans le but de dispenser et d'administrer des soins de santé

8.1 Lorsque des données de santé sont transférées par un travailleur sanitaire à un autre, pour dispenser et administrer des soins de santé à un individu, ce dernier doit en être informé avant que l'échange d'informations n'ait lieu, excepté lorsque cela s'avère impossible en raison d'une situation d'urgence ou en application du paragraphe 11.4.

8.2 Des données de santé ne peuvent être communiquées à un/des destinataire(s) agréé(s), que si des garanties appropriées sont prévues par la loi, sous réserve des règles de confidentialité.

8.3 L'échange et la divulgation de données entre agents de santé doivent se limiter aux informations nécessaires à la coordination ou à la continuité des soins, à la prévention ou au suivi médico-social et social de l'individu. Les agents sanitaires doivent être en mesure de divulguer ou de recevoir les données de santé qui leur sont nécessaires pour soigner le patient et exercer leurs fonctions.

8.4 Pour tout échange et divulgation de données de santé, des mesures de sécurité physiques, techniques ou administratives doivent être adoptées pour garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des données.

9. Divulgation de données de santé à des fins autres que celles de dispenser et d'administrer des soins de santé

9.1 Des données de santé peuvent être révélées à des destinataires autorisés et tenus par la loi d'avoir accès à des données de santé et d'en avoir la possession, afin de

faciliter ou de mener des travaux de recherche sur des questions relatives à la santé ; aux fins de la planification, de l'amélioration et de la gestion de systèmes de santé ; et/ou de l'élaboration, de l'évaluation ou du suivi d'activités et de programmes de soins de santé. Pareil traitement ne peut être autorisé que sur la base de critères nécessaires et proportionnés définis par la loi.

9.2 Les compagnies d'assurance, les employeurs et les entrepreneurs ne peuvent pas être considérés comme des bénéficiaires autorisés à accéder à des données de santé personnelles, à moins qu'une loi assortie de garanties appropriées ne l'autorise et que les dispositions de la section 5 ne soient respectées.

10. Stockage des données de santé

10.1 Les données de santé ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été recueillies.

Chapitre III

Droits de la personne concernée

11. Droit à la transparence du traitement

11.1 Le contrôleur doit informer la personne concernée de son droit à un traitement équitable et transparent de ses données de santé et, en particulier, d'avoir connaissance des éléments suivants :

a) L'identité et les coordonnées du/des contrôleur(s) et de tous les responsables du traitement ;

b) La source des données de santé en cours de traitement (le cas échéant) ;

c) Les catégories de données de santé concernées par le traitement ;

d) L'objectif du traitement et la base juridique sur laquelle il repose ;

e) La durée pendant laquelle les données de santé seront stockées ou, si cela n'est pas possible, les critères déterminants ;

f) Les destinataires (ou catégories de destinataires) des données de santé et les transferts prévus dans un pays autre que celui d'où elles proviennent ou dans une organisation internationale (dans ce cas, les données ne peuvent être transférées qu'à une organisation internationale qui les accepte), ceux-ci devant être conformes aux dispositions de la présente recommandation ;

g) La possibilité, s'il y a lieu, de s'opposer au traitement de leurs données de santé, dans les conditions prévues au paragraphe 12.2 ;

h) Les conditions et les moyens disponibles pour exercer leurs droits d'accès, de rectification et d'effacement de leurs données de santé ;

i) Le fait que leurs données de santé peuvent faire l'objet d'un traitement ultérieur, si celui-ci est effectué dans un but compatible avec l'intérêt public ou à des fins d'archivage ou de recherche scientifique ou historique ou à des fins statistiques, conformément aux garanties appropriées prévues par la loi et aux conditions énoncées à l'alinéa b) du paragraphe 4.1. ;

j) L'existence de décisions automatisées, y compris le profilage, uniquement autorisées lorsqu'elles sont prescrites par la loi et sous réserve des garanties appropriées qui peuvent être formulées en ce qui concerne les données de santé ;

k) Les risques que présente le traitement des données prévu, ainsi que les voies de recours possibles en cas d'atteinte à la protection des données de santé ;

l) Les mécanismes de plainte concernant le traitement de leurs données de santé, notamment à qui cette plainte doit être adressée dans chaque juridiction où le traitement des données intervient ;

m) L'identité et les coordonnées des fonctionnaires chargés de la protection des données ou les contrôleurs des données auprès desquels le sujet des données peut demander des informations complémentaires concernant le projet de traitement des données en question ;

n) Les juridictions proposées pouvant intervenir au sujet du traitement des données de santé et les droits dont la personne concernée pourra se prévaloir au regard de leur domaine de compétence.

11.2 Les renseignements énumérés au paragraphe 11.1 doivent être communiqués avant le traitement des données de santé.

11.3 Les renseignements doivent être intelligibles, facilement accessibles, rédigés dans un langage simplifié et adaptées aux circonstance afin d'en permettre une bonne compréhension par le sujet des données.

11.4 Le contrôleur n'est pas tenu de fournir les informations énoncées au paragraphe 11.1 lorsque :

a) La personne concernée dispose déjà de ces informations ;

b) Il est permis que ces données ne soient pas recueillies directement auprès de la personne concernée ;

c) Le traitement de ces données de santé est expressément prescrit par la loi ;

d) Il est impossible de se mettre en rapport avec la personne concernée.

11.5 Lorsque le traitement des données de santé est effectué aux fins d'archivage dans l'intérêt général, et qu'il est impossible de contacter le sujet des données, le traitement des données à ces fins peut être entrepris à condition que les données en question soient pseudonymisées ou anonymisées avant d'être traitées, sauf disposition contraire de la loi.

12. Accès aux données de santé, transférabilité, rectification et suppression de données de santé et objection au traitement de données de santé

12.1 La personne concernée a le droit de savoir si ses données de santé font l'objet d'un traitement et, dans l'affirmative, d'obtenir qu'elles lui soient communiquées sans délai ou frais excessifs et sous une forme intelligible et d'avoir accès, dans les mêmes conditions, au moins aux informations suivantes :

a) Le(s) but(s) du traitement des données de santé ;

b) Les catégories de données de santé visées ;

c) Les destinataires ou les catégories de destinataires des données de santé et les transferts de données envisagés vers un/des pays tiers, ou une/des organisation(s) internationale(s) ;

d) La période durant laquelle le traitement des données de santé aura lieu, y compris le stockage ;

e) Le raisonnement qui sous-tend le traitement des données de santé lorsque les résultats de ce traitement leur sont appliqués, notamment dans le but du profilage,

qui ne peut intervenir que lorsqu'il est prescrit par la loi et sous réserve de garanties appropriées.

12.2 Les personnes concernées ont le droit :

a) De faire effacer leurs données de santé si elles sont traitées contrairement à la présente recommandation ;

b) De faire rectifier leurs données de santé si elles sont inexactes ou trompeuses ;

c) De contester le traitement de leurs données de santé pour des motifs liés à leur vie et à leur bien-être. Lorsqu'un contrôleur est autorisé par la loi à entreprendre le traitement des données de santé en dépit de l'objection, il doit informer l'autorité de surveillance compétente du projet de traitement et de l'objection formulée par le sujet des données de manière à ne pas identifier ce dernier (sauf s'il consent à être identifié).

12.3 Si la rectification ou la suppression est rejetée, la personne concernée doit être en mesure de réexaminer cette décision, et avoir accès à un recours approprié si une violation des données de santé a eu lieu.

12.4 Les personnes concernées ont le droit de ne pas faire l'objet d'une décision qui les affecte de manière considérable uniquement sur la base d'un traitement automatisé, y compris le profilage, des données relatives à leur santé. Une dérogation à cette interdiction n'est autorisée que par une loi proportionnée au but visé, comme le respect du droit à la protection des données, le droit à la vie privée et de prévoir des garanties appropriées et spécifiques pour protéger les droits et libertés fondamentaux de la personne concernée. Le profilage pour des raisons de santé doit remplir des critères généralement acceptés de validité scientifique et clinique et d'utilité clinique et faire l'objet de programmes appropriés d'assurance de la qualité.

12.5 Sous réserve des conditions prévues par la loi, lorsque le traitement des données de santé est automatisé, les personnes concernées peuvent obtenir du contrôleur des informations sur la transmission de leur données, de manière structurée, interopérable et sous un format lisible par machine, afin de pouvoir les transmettre à un autre contrôleur. La personne concernée peut également demander au contrôleur de transmettre sans retard ses données directement à un autre contrôleur de son choix.

12.6 Les droits de la personne concernée peuvent faire l'objet de restrictions prévues par la loi lorsque cette loi constitue une mesure nécessaire et proportionnée à la fois, dans l'intérêt de :

a) La protection de la sécurité de l'État, de la sécurité publique, des intérêts économiques de l'État ou de la répression d'infractions pénales ;

b) La protection de la personne concernée ou des droits et libertés d'autrui, des garanties appropriées devant être prévues pour assurer le respect des droits de la personne concernée.

Chapitre IV

Sécurité et interopérabilité

13. Sécurité

13.1 Le traitement des données de santé doit être effectué en toute sécurité.

13.2 La disponibilité du système, à savoir le bon fonctionnement du système d'information sanitaire, doit s'accompagner de mesures garantissant que l'accès aux

données de santé est sûr et conforme au niveau d'autorisation des personnes habilitées.

13.3 Pour garantir l'intégrité de tout traitement de données sanitaires, il faut : des mécanismes permettant de vérifier les actions menées au fin du traitement ; des dispositifs visant à contrôler l'accès aux données et leur utilisation, pour que seules les personnes autorisées soient en mesure d'y accéder, de les utiliser et de les traiter. Les systèmes contenant ces données doivent pouvoir être audités et permettre l'identification de (s) l'utilisateur (s) ayant entrepris toute action ou traité des données.

14. Interopérabilité

14.1 L'interopérabilité doit être pleinement conforme aux principes énoncés dans la présente recommandation.

14.2 Les cadres de référence offrant un cadre technique facilitant l'interopérabilité doivent garantir un niveau de sécurité élevé et être régulièrement audités.

Chapitre V

Recherche scientifique

15.1 Le traitement des données de santé à des fins de recherche scientifique doit faire l'objet de garanties appropriées prévues par la loi, être conforme aux dispositions de la présente recommandation et de tous les autres droits et libertés fondamentaux de la personne concernée et être effectué dans un but légitime. Nul ne peut être tenu ou contraint de participer à la recherche scientifique sans avoir préalablement donné son consentement libre, explicite et éclairé.

15.2 Le consentement à la participation à la recherche n'équivaut pas au consentement au traitement des données. Les conditions dans lesquelles le traitement des données de santé est effectué pour le besoins de la recherche scientifique doivent être évaluées par un organisme indépendant compétent (par exemple, un comité de déontologie ou un responsable des données indépendant) comprenant des membres non spécialistes, avant que le traitement ne commence. Ces évaluations doivent être revues par l'autorité de surveillance compétente ou un autre comité de déontologie ou un autre responsable des données indépendant afin de garantir le respect des conditions de l'approbation et l'effectivité de l'approbation.

15.3 Outre le consentement à la participation à la recherche, une base juridique distincte pour le traitement des données est requise conformément aux dispositions du paragraphe 15.5 de la présente recommandation. La base légale pour le traitement des données dans le domaine de la recherche scientifique peut, mais ne doit pas nécessairement être, le consentement, soit parce que les conditions de validité du consentement au traitement des données ne peuvent être satisfaites, soit parce que le traitement des données est prescrit par la loi.

15.4 La nécessité d'effectuer le traitement des données de santé aux fins de la recherche scientifique doit être évaluée à la lumière des objectifs de la recherche scientifique, des connaissances scientifiques, du respect des règles éthiques, des avantages présumés, des contraintes imposées au traitement des données, des risques pour la personne concernée, des risques de préjudice pour le groupe, et en ce qui concerne les données génétiques, du risque pour la famille biologique partageant certaines de ces données avec le sujet des données, et des risques d'établissement de la non-paternité ou d'un autre degré de parenté familiale inattendu. Les dérogations

aux droits des patients de s'engager dans la recherche ne peuvent être utilisées que si cela est nécessaire et proportionné.

15.5 Le traitement des données de santé dans un projet de recherche scientifique ne peut être entrepris que si la personne concernée y a consenti conformément au paragraphe 5.2, sauf dans les cas où il est prévu par la loi. Toute loi prévoyant le traitement de données sanitaires à des fins de recherche scientifique sans le consentement de la personne concernée doit : être nécessaire, proportionnée et dans l'intérêt public ; respecter le droit à la protection des données ; prévoir des garanties appropriées et spécifiques pour protéger les droits et libertés de la personne concernée. Ces garanties doivent veiller au respect du principe de minimisation des données conformément à l'alinéa e) du paragraphe 4.1 et peuvent comprendre des mesures techniques et institutionnelles.

15.6 La personne concernée doit, outre les dispositions du chapitre III (notamment le paragraphe 11.1 mais non exclusivement), recevoir au préalable des informations transparentes et compréhensibles aussi raisonnablement précises que possible, sur :

a) La nature de la recherche scientifique ; les options dont elle dispose ; toute condition pertinente régissant l'utilisation des données de santé, y compris les éventuelles informations en retour et les reprises de contact concernant les résultats/conclusions ;

b) Les moyens et la capacité d'extraire de nouvelles formes de données de santé et l'incertitude concernant ce qui pourrait être extrait à l'avenir ;

c) Les conditions applicables au stockage des données de santé ;

d) Les droits et garanties prévus par la loi, et en particulier le droit de refuser de consentir au traitement des données au profit de la recherche scientifique et le droit de retirer un consentement à la participation selon les mêmes dispositions que celles qui figurent au paragraphe 5.2 à tout moment ; l'éventuelle impossibilité de détruire des données de santé déjà analysées et/ou publiées avant le retrait du consentement conformément aux paragraphes 15.11 et 15.12 ;

e) Les objectifs, méthodes et sources de financement, les éventuels conflits d'intérêts, les affiliations institutionnelles du chercheur, les avantages escomptés et les risques potentiels de l'étude et les inconvénients qu'elle peut causer, les dispositions à prendre après l'étude, ainsi que tout autre aspect pertinent de l'étude ;

f) L'identité des tiers qui auront accès aux données ou qui peuvent légalement demander cet accès à d'autres fins, et dans quelle mesure ces fins sont limitées ;

g) Le transfert transnational planifié des données, y compris le fondement juridique pour le transfert conformément au paragraphe 17.1 ;

h) La publication proposée pour les données de santé et tout dépôt envisagé dans les répertoires de données de recherche.

15.7 Le contrôleur ne doit pas être tenu de fournir les données directement à chaque sujet des données si les conditions du paragraphe 11.4 ou 11.5 sont respectées. Lorsque le paragraphe 11.4 ou 11.5 s'applique, l'information doit néanmoins être mise à la disposition des personnes concernées d'une manière accessible au public.

15.8 À des fins de recherche scientifique, lorsqu'il n'est pas possible de déterminer les fins spécifiques du traitement des données au moment de la collecte, les sujets des données doivent être en mesure d'exprimer leur consentement au traitement des données au profit de certains domaines de recherche ou certaines parties des projets de recherche ou aux fins d'une base de données de biobanque et dans la mesure

admise par le but envisagé, compte dûment tenu des normes éthiques reconnues. Lorsqu'il devient possible de préciser davantage le but poursuivi, la personne concernée doit en être informée conformément aux paragraphes 11.1, 15.6 et 15.7. Le consentement dynamique numérique peut être utilisé à ces fins. Cette disposition ne diminue en rien les exigences de consentement énoncées au paragraphe 5.2 car elles sont applicables à la recherche scientifique. Les personnes concernées peuvent également donner leur consentement préalable à l'utilisation future de leurs données de santé aux fins de la recherche scientifique après leur décès.

15.9 Les chercheurs détenant des données de santé seront responsables de toute atteinte à la protection de ces données tant qu'elles seront en leur possession ou sous leur contrôle. Des garanties complémentaires déterminées par la loi, telles que l'exigence de consentement explicite ou l'évaluation de l'organe compétent désigné par la loi doivent être mises en place avant que d'autres scientifiques ne puissent acquérir ces données.

15.10 Lorsque cela est techniquement possible et réalisable, les données de santé doivent être anonymisées. S'il n'est pas techniquement possible et/ou réalisable d'anonymiser, la pseudonymisation des données de santé et l'intervention d'une tierce partie de confiance au stade de la séparation des données d'identification doit être mise en œuvre afin de protéger les droits et les libertés fondamentales de la personne concernée. Le contrôleur ne peut pas faire office de tierce partie de confiance en plus de ses fonctions. Cela doit être fait lorsque les objectifs de la recherche scientifique peuvent être atteints par le traitement supplémentaire de données de santé ne permettant pas ou plus l'identification des personnes concernées.

15.11 Lorsqu'une personne concernée retire son consentement conformément aux dispositions du paragraphe 5.2 ou s'oppose au traitement conformément aux dispositions du paragraphe 12.4, les données de santé la concernant traitées dans le cadre de cette recherche scientifique doivent être détruites conformément à son souhait, à condition de ne pas contrevenir à la loi. Si la destruction est contraire à la loi, la personne concernée doit en être informée, ainsi que de la loi exigeant de conserver les données de santé. Lorsque l'anonymisation des données peut être entreprise de manière à ne pas compromettre la valeur scientifique de la recherche mais à garantir que le sujet des données ne peut pas être identifié, même au moyen d'autres ensembles de données, cela peut être entrepris en tant que solution de rechange à la destruction et le sujet des données doit en être informé. Lorsque la personne concernée continue à exiger la destruction plutôt que l'anonymisation des données de santé, le respect de cette décision est requis. Si les données de santé ont été analysées alors que le fondement juridique du traitement existait, la destruction des données peut ne pas être possible dans la pratique et peut nuire à l'intégrité de l'ensemble des données destinées à la recherche scientifique. Dans de tels cas, à condition qu'il soit essentiel d'atteindre les résultats d'une étude scientifique menée dans l'intérêt public ou lorsque la destruction aurait une incidence importante sur la valeur scientifique de la recherche scientifique, le traitement des données de santé doit être strictement limité à ce qui est nécessaire pour réaliser ces objectifs mais les données ne doivent pas être détruites. S'il n'est pas possible de supprimer les données provenant de travaux de recherche déjà réalisés, les renseignements concernant le participant ne doivent pas être utilisés pour d'autres travaux de recherche.

15.12 Les données de santé utilisées à des fins scientifiques ne doivent pas être publiées sous une forme permettant d'identifier la personne concernée, excepté :

a) Lorsque la personne concernée y a consenti et si le consentement n'a pas été retiré ;

b) Lorsque la loi permet cette publication à condition qu'elle soit indispensable pour la présentation des résultats de la recherche et uniquement dans la mesure où l'intérêt de publier ces données l'emporte sur les intérêts et les droits et libertés de la personne concernée ;

c) Dans le cas où le consentement de la personne concernée à la publication de données de santé permettant de l'identifier est retiré, le contrôleur et/ou les responsables du traitement doivent détruire ou rendre inaccessibles les données de santé, si cela est concrètement possible.

Chapitre VI

Applications mobiles

16.1 Les données de santé recueillies par des applications mobiles jouissent de la même protection juridique et confidentialité que les autres données de santé au titre de la présente recommandation.

Chapitre VII

Transfert transfrontières des données de santé

17.1 Le transfert transfrontières des données de santé ne peut avoir lieu que si l'exigence d'un niveau approprié de protection des données est remplie, soit sur la base des dispositions ci-après :

a) La personne concernée a donné son consentement explicite, spécifique et libre au transfert, conformément au paragraphe 5.2, après avoir été informée de la loi applicable et des risques associés en cas d'absence d'un niveau de protection des données approprié ;

b) Les intérêts spécifiques de la personne concernée l'exigent dans ce cas particulier ;

c) Le transfert sert des intérêts publics importants, y compris la recherche scientifique, prévus par la loi et constitue une mesure nécessaire et proportionnée ;

d) Le transfert est nécessaire pour les intérêts légitimes supérieurs poursuivis par le contrôleur, qui ne sont pas supplantés par les intérêts ou les droits et libertés de la personne concernée, et le contrôleur a évalué toutes les circonstances entourant le transfert de données et sur la base de cette évaluation a fourni des garanties de protection appropriées. Le contrôleur devra informer l'autorité de surveillance du transfert. Il devra, outre le fait de fournir les informations visées au paragraphe 11.1, informer la personne concernée du transfert et des intérêts légitimes supérieurs poursuivis ;

e) Le transfert constitue une mesure nécessaire et proportionnée pour la liberté d'expression.

17.2 Pour les données de santé traitées dans les logiciels, ou la plateforme transnationale d'informatique en nuage, et en l'absence d'une obligation en vertu du droit international d'exercer sa compétence, un État peut uniquement exercer sa compétence dans les cas suivants :

a) Lorsqu'il existe un lien étroit entre la question et l'État qui souhaite exercer sa compétence ;

b) Lorsque l'État qui cherche à exercer sa compétence a un intérêt légitime en la matière ;

c) Lorsque l'exercice de la compétence est raisonnable compte tenu de l'équilibre existant entre les intérêts légitimes de l'État et d'autres intérêts.

Chapitre VIII

Dossiers médicaux électroniques

18.1 Tous les individus ont droit à la protection de leur vie privée et la confidentialité et la protection des données relatives à leur santé dans les systèmes de dossiers médicaux électroniques doit être rigoureusement gérée.

18.2 Le traitement médical ne peut être refusé au motif qu'une personne n'a pas de dossier médical électronique.

18.3 Un sujet des données peut choisir d'empêcher la divulgation de ses données de santé dans un dossier médical électronique, enregistré par un agent sanitaire au cours du traitement, à d'autres professionnels de la santé.

18.4 Tout système de dossier médical électronique doit être auditable et comprendre un protocole électronique permettant de surveiller qui a eu accès aux données s'y trouvant, la durée de l'accès et les modifications apportées et comprendre des protocoles visant à empêcher l'accès non autorisé et garantir que les personnes concernées aient connaissance des personnes ayant eu accès à leurs données.

18.5 La preuve que le patient a donné son consentement (ou l'a retiré) à la consultation de ses données dans le dossier médical électronique est nécessaire. Elle doit être consignée électroniquement à des fins d'audit.

18.6 Le traitement des données de santé dans les systèmes de dossiers médicaux électroniques aux fins de la recherche scientifique et à des fins statistiques est autorisé lorsqu'il est nécessaire à des fins spécifiques précédemment établies afin de protéger les droits des individus et est prévu par une loi existante. Les données de santé provenant de systèmes de dossiers médicaux électroniques doivent être utilisées à des fins de recherche sous une forme anonymisée.

18.7 Toute personne concernée doit avoir accès aux données relatives à sa santé qui figurent dans un système de dossiers médicaux électroniques. Les données de santé ne doivent pas être stockées dans un dossier médical électronique au-delà du temps nécessaire au but pour lequel elles ont été recueillies.

18.8 L'audit des protocoles d'accès à tout dossier médical électronique doit avoir lieu régulièrement et être rendu publique.

Chapitre IX

Données de santé, données génétiques et assurance

19. Données de santé, données génétiques et assureurs

19.1 Les données génétiques ne peuvent être divulguées à des assureurs sauf lorsqu'il existe un important intérêt public prévu par la loi conformément au droit international des droits de l'homme ou avec le consentement de la personne concernée.

19.2 Des données de santé et des données génétiques obtenues à des fins de recherche scientifique ne peuvent être utilisées aux fins de l'assurance des sujets des données ou des membres de leur famille.

20. Les assureurs doivent justifier le traitement des données de santé

20.1 Les données personnelles de santé peuvent uniquement être traitées à des fins d'assurance, à condition que :

a) L'objectif du traitement ait été précisé et la pertinence des données ait été dûment justifiée et la personne concernée ait été informée de la pertinence au regard du risque et de sa justification ;

b) La qualité et la validité du projet de traitement des données de santé soient conformes aux normes scientifiques et cliniques généralement acceptées ;

c) Les données résultant d'un examen prédictif aient une valeur prédictive très élevée ;

d) Le traitement soit dûment justifié, conformément au principe de la proportionnalité, en ce qui concerne la nature et l'importance du risque en question ;

e) La qualité et la validité des données de santé traitées à des fins d'assurance soient conformes aux normes scientifiques et cliniques généralement acceptées.

20.2 Les données de santé des membres de la famille de la personne assurée ne peuvent être traitées à des fins d'assurance, à moins que ce ne soit expressément autorisé par la loi.

20.3 Il est interdit de traiter des données de santé obtenues dans le domaine public dans le but d'évaluer des risques ou de calculer des primes.

21. Les assureurs ne doivent pas traiter des données de santé sans le consentement de l'assuré ou de la personne concernée

21.1 Les données de santé ne doivent pas être traitées à des fins d'assurance sans le consentement de l'assuré, conformément au paragraphe 5.2.

21.2 Les données de santé doivent être recueillies auprès de l' assuré.

22. Les assureurs doivent bénéficier des garanties adéquates pour le stockage des données de santé

22.1 Les assureurs ne peuvent pas stocker des données de santé qui ne sont plus nécessaires au but pour lequel elles ont été recueillies. Les compagnies d'assurances ne peuvent pas stocker les données de santé si une demande d'assurance a été rejetée ou si le contrat a expiré et les réclamations ne peuvent plus être formulées, sauf si ce stockage est exigé par une loi nécessaire et proportionnée.

23. Les assureurs ne doivent pas exiger de tests génétiques à des fins d'assurance

23.1 Les tests génétiques prédictifs ne doivent pas être effectués à des fins d'assurance.

23.2 Le traitement des données provenant de données génétiques prédictives ne peut pas être traité à des fins d'assurance, sauf s'il est expressément autorisé de plein droit. Lorsqu'il est autorisé, le traitement des données requis n'est autorisé qu'après une évaluation indépendante de la conformité aux critères énoncés au paragraphe 20.1 par type de test et au regard du risque particulier visé au titre de l'assurance.

23.3 Les données existantes provenant de tests génétiques des membres de la famille de l'assuré ne peuvent pas être traitées à des fins d'assurance et doivent être détruites par un assureur.

24. Les assureurs doivent tenir compte des nouvelles connaissances scientifiques

24.1 Les assureurs doivent mettre à jour régulièrement les bases actuarielles conformément aux nouvelles connaissances scientifiques et fournir des informations et justifications pertinentes à tout assuré concernant le calcul de la prime, l'augmentation supplémentaire d'une prime ou toute exclusion totale ou partielle de l'assurance.

25. Les États doivent assurer la médiation, la consultation et le suivi de manière adéquate

25.1 Des procédures de médiation, de consultation et de suivi doivent être mises en place pour assurer un règlement équitable et objectif des différends, permettre des relations équilibrées entre les parties et garantir une évaluation rigoureuse de la conformité à la présente recommandation y compris par une autorité de contrôle compétente.

Chapitre X

Données de santé et employeurs

26.1 Un contrôleur de données de santé peut être un employeur. Cet employeur est responsable vis-à-vis de la personne concernée de toute atteinte à la protection de ses données de santé.

26.2 Un employeur ne peut exiger d'un demandeur d'emploi qu'il lui communique des données sur sa santé tant qu'il ne lui a pas offert d'emploi, sauf :

a) Pour permettre des ajustements raisonnables sur le lieu de travail pour faciliter l'emploi de l'individu ;

b) Pour déterminer si le demandeur peut exercer une fonction indissociable des travaux en question ;

c) Pour observer la diversité du personnel et faciliter l'embauche des personnes en situation de handicap.

26.3 Les employés doivent être informés par leur employeur de leurs droits et des objectifs du traitement des données relatives à leur santé.

26.4 Les employés ont le droit d'accéder à leurs dossiers médicaux afin de pouvoir vérifier s'ils sont exacts et de corriger toute information inexacte ou incomplète.

26.5 Les employeurs doivent s'assurer que les données de santé des employés ne soient pas conservées plus longtemps que nécessaire.

Chapitre XI

Données de santé et souveraineté des données autochtones

27.1 Les peuples autochtones et les Premières Nations ont droit à la souveraineté des données autochtones et à la gouvernance autochtone en ce qui concerne les données les touchant.

Chapitre XII

Données de santé et données publiques

28.1 Aucune donnée de santé enregistrée individuellement ne peut être publiée en tant que donnée publique. De même, aucune donnée pseudonymisée ne peut être publiée en tant que donnée publique, sans le consentement préalable, en connaissance de cause, de chaque individu susceptible d'être affecté. Dans le cas de données génétiques, les individus susceptibles d'être touchés comprennent les parents biologiques de la personne qui propose de divulguer ses données génétiques.

28.2 Lorsque des données de santé sont divulguées sous forme de données publiques et si une atteinte à la protection des données de santé découle de cette publication, la partie qui traite les données de santé et celle qui les divulgue sous forme de données publiques (lorsqu'elles ne sont pas identiques) sont toutes deux responsables vis-à-vis des personnes concernées.

Chapitre XIII

Données concernant la santé et automatisation de la prise de décisions

29.1 La personne concernée a le droit de ne pas faire l'objet d'une décision ayant trait à sa santé et la touchant considérablement, si la décision repose uniquement sur le traitement automatisé, y compris le profilage. La personne concernée a également le droit de faire en sorte que la décision initiale prise par traitement automatisé soit réexaminée et reformulée par une personne.

29.2 Le paragraphe 29.1 ne s'applique pas si la décision :

a) Est nécessaire pour signer, ou exécuter, un contrat entre la personne concernée et un contrôleur des données ;

b) Est autorisée par une loi à laquelle le contrôleur des données est soumis, cette loi devant également prévoir les mesures appropriées pour sauvegarder les droits, libertés et intérêts légitimes de la personne concernée ;

c) Est fondée sur le consentement explicite de la personne concernée, celle-ci ayant été informée avant de donner son consentement que le droit d'avoir recours à une vérification humaine pour prendre une nouvelle décision serait perdu si le consentement était donné.

29.3 Lorsque les dispositions des alinéas a) et c) du paragraphe 29.2 s'appliquent, le contrôleur doit mettre en œuvre les mesures adéquates pour sauvegarder les droits, libertés et intérêts légitimes de la personne concernée.

Chapitre XIV

Notification obligatoire des atteintes à la protection des données de santé

30.1 Les contrôleurs doivent rendre compte de toute atteinte importante à la protection des données de santé à une autorité de surveillance compétente et aux personnes affectées, au plus tard 72 heures après avoir pris connaissance de l'atteinte.

Chapitre XV

Droit de recours en cas d'atteinte à la protection des données de santé

31.1 Une personne concernée a droit à un recours utile, notamment sous forme d'une indemnisation, lorsqu'elle a subi un préjudice résultant d'une atteinte à la protection de ses données de santé ou de l'utilisation d'un algorithme médical.

Chapitre XVI

Protection des personnes qui signalent des atteintes à la protection des données de santé

32.1 Toute personne qui estime, en toute honnêteté, sur la base de motifs raisonnables, qu'un contrôleur ou une autre personne en possession de données de santé a engagé, exerce ou entend exercer une activité susceptible de constituer une atteinte à la protection des données de santé ou d'entraîner pareille atteinte, a le droit de le signaler dans des conditions protégées à une autorité indépendante et de bénéficier d'une protection contre les représailles qui pourraient suivre ce signalement.

Chapitre XVII

Responsabilité civile en cas d'atteinte à la protection des données de santé

33.1 Les États Membres, s'agissant de l'attribution de la responsabilité civile en cas d'atteinte à la protection des données de santé, doivent tenir compte des principes ci-après :

a) La responsabilité civile vis-à-vis de la personne concernée ne doit pas être indûment limitée, notamment en vertu du droit de la responsabilité civile délictuelle, et permettre à toute personne concernée de soumettre une demande d'indemnisation à l'encontre des entités responsables ;

b) Les représentants des patients et des agents sanitaires doivent être consultés avant l'adoption de la législation concernant la responsabilité civile, y compris la législation concernant les algorithmes médicaux applicables ;

c) Les algorithmes médicaux doivent être utilisés en tant qu'outil de « recommandation ». Les agents sanitaires ainsi que les organisations dont ils relèvent demeurent responsables des décisions prises à l'aide de ces outils vis-à-vis des personnes concernées.

Chapitre XVIII

Intelligence artificielle, transparence algorithmique et mégadonnées

34.1 Les algorithmes médicaux doivent être réglementés de manière transparente, équitable et prévisible afin de :

a) Garantir un niveau élevé de qualité, d'équité et de sécurité (à tous les groupes d'une population) ;

b) Faciliter le développement technologique par la communication de données vérifiables aux chercheurs, informaticiens, concepteurs, agents sanitaires et hôpitaux.

34.2 Les exigences applicables à tous les traitements médicaux qui doivent être surveillés pour les besoins de l'efficacité des résultats ne doivent pas être baissées pour faciliter le déploiement ou le développement d'algorithmes, de mégadonnées ou de l'intelligence artificielle. Les formes de traitement qui n'ont pas encore fait la preuve de leur efficacité dans la transparence sont soumises aux dispositions de la présente recommandation applicables à la recherche scientifique.

34.3 Tous les algorithmes ainsi que l'intelligence artificielle doivent faciliter le suivi des effets néfastes notamment les caractéristiques protégées par les lois applicables et les conventions de l'ONU. Cette disposition ne peut pas être utilisée pour demander, exiger ou enregistrer d'autres données démographiques.

34.4 Les processus et systèmes doivent être conçus et mis en œuvre pour identifier et traiter les distorsions algorithmiques. Toute distorsion doit être communiquée aux sujets des données et prise en compte par les agents sanitaires utilisant des outils algorithmiques.

34.5 Toute décision prise à l'aide d'un algorithme, de données ou de l'intelligence artificielle doit être explicable en vertu des exigences existantes de l'état de droit, satisfaire aux critères énoncés dans la liste de vérification du respect de la primauté du droit établie par la Commission de Venise du Conseil de l'Europe. Si un algorithme n'est pas suffisamment explicable, il ne peut être utilisé qu'à l'appui d'une décision. Tout agent sanitaire qui s'appuie sur un outil algorithmique doit répondre de cette décision.

Chapitre XIX

Données de santé en milieu non sanitaire

35. Accès aux données de santé ou aux données génétiques à partir de bases de données à usage lié à la santé et/ou à la recherche à des fins d'identification, de procédure judiciaire et/ou d'enquête

35.1 Les données génétiques doivent être recueillies à des fins explicites, précises et légitimes et ne doivent pas être traitées d'une manière incompatible avec les objectifs pour lesquels elles ont été initialement recueillies.

35.2 L'accès à des données de santé ou à des données génétiques provenant de bases de données qui n'ont pas de but criminalistique spécifié, pour prévenir ou détecter une infraction spécifique, ou procéder à des poursuites doit faire l'objet d'un contrôle judiciaire. Cet accès ne peut être fourni que lorsqu'il est nécessaire, proportionné, et si des garanties suffisantes existent dans la loi pour protéger les droits et intérêts de la personne concernée. L'accès doit être limité aux données nécessaires pour atteindre l'objectif visé. Un accès général pour les besoins de la sécurité nationale ou à des fins de prévention de la criminalité n'est pas autorisé.

35.3 Le traitement de données génétiques aux fins de l'application du droit pénal ne peut être entrepris que par les autorités compétentes à des fins de prévention, d'enquête, de détection ou de poursuites portant sur des infractions pénales et s'il n'existe pas d'autre solution ou de moyens moins contraignants pour établir l'existence d'un lien génétique dans le cadre d'éléments de preuve, pour prévenir un

danger réel et immédiat ou en cas de poursuites pour une infraction pénale déterminée.

35.4 Les données génétiques à utiliser pour toute procédure ou enquête judiciaire doivent être recueillies auprès de la personne concernée. Il n'est pas autorisé de les prélever dans des bases de données ou des biobanques qui n'ont pas de finalité criminalistique établie. Ce n'est qu'en cas d'impossibilité de recueillir les données auprès d'une personne concernée que l'accès aux données provenant de bases de données ayant des objectifs de soins de santé et/ou de recherche peut être accordé sur la base d'une décision de justice.

35.5 Les données génétiques ne peuvent être traitées à des fins d'identification de personnes lors d'une crise humanitaire, en cas d'accident à lourd bilan humain, ou pour aider à identifier des personnes portées disparues que lorsque des garanties appropriées sont prévues par la loi ou qu'il s'agit de l'intérêt supérieur manifeste de la personne concernée.

36. Données de santé et immigration

36.1 Lorsque l'état de santé est pris en considération pour prendre des décisions relatives à l'immigration légale et que des données de santé sont recueillies à cette fin, les mêmes conditions s'appliquent à la collecte, l'utilisation, le partage et la conservation de ces données que celles qui s'appliquent aux données de même type recueillies auprès des citoyens de cet État ou les concernant.

36.1 Dans le cas de réfugiés et des personnes entrées sans autorisation, une condition préalable pour la collecte de données de santé est la dignité et l'intégrité du processus d'établissement de l'identité des individus concernés.

36.2 Les personnes entrées avec ou sans autorisation et les réfugiés dans le cadre des juridictions nationales ont le droit d'accéder aux services de soins de santé selon les normes minimales applicables aux citoyens de ce pays.

36.3 La mise en commun des données de santé entre organisations internationales chargées de la gestion des migrations internationales et des programmes relatifs aux réfugiés ne peut être entreprise que si toutes les parties à l'échange de données s'engagent à respecter les dispositions de la présente recommandation.

37. Données de santé et personnes à la charge de l'État

37.1 La présente section s'applique à des institutions de l'État financées par des fonds publics et privés. Les données de santé jouent un rôle vital dans la gestion de la vie des individus lorsque le contrôle des décisions concernant leur santé a été supprimé. Ces personnes ont le droit au même niveau de soins de santé que celui qui est accordé à tout un chacun, l'institutionnalisation, la détention ou l'incarcération pouvant cependant limiter le choix des services.

37.2 Ces principes s'appliquent aux individus se trouvant sous la responsabilité directe d'établissements gérés par l'État ou lui appartenant et aux individus se trouvant sous la responsabilité d'agents du secteur non publique auxquels l'État a délégué sa responsabilité.

37.3 L'accès aux données de santé de ces personnes doit être conforme aux dispositions de la présente recommandation et servir les intérêts de l'individu et ne pas être subordonné à l'intérêt invoqué par l'État ou l'institution.

38. Données de santé et commercialisation

38.1 Les fournisseurs de renseignements et les prestataires de services d'information ne doivent faciliter le profilage ou la commercialisation basés sur des données de santé que si :

a) Les droits des sujets des données au respect de la vie privée et à la confidentialité sont respectés ;

b) L'existence et le but du profilage et/ou de la commercialisation ont été clairement communiqués ;

c) Le consentement a été donné et enregistré et peut être retiré aussi facilement qu'il a été donné.

38.2 Les tierces parties qui recueillent et vendent des données de santé doivent respecter la vie privée et la confidentialité des personnes concernées. L'établissement d'un lien entre des données de santé et d'autres données identifiables pour établir des listes de personnes présentant des maladies ou des troubles particuliers exige le consentement de ces personnes.

38.3 Les plateformes publicitaires ne doivent pas autoriser le profilage ou le ciblage sur la base de caractéristiques sanitaires, ou de procurations pour ces caractéristiques, notamment par le biais de l'échange, d'un autre accès, de la transmission ou de la copie.

38.4 Les données de santé recueillies ou révélées par des appareils ou des applications mobiles de culture physique jouissent des mêmes protections juridiques et droits à la confidentialité applicables au traitement des autres données de santé, en ce qui concerne leur utilisation à des fins de profilage et de commercialisation.

39. Données de santé et capacités réduites

39.1 Le droit d'une personne à capacités réduites de prendre des décisions doit être le moins limité possible. Une personne à capacités réduites a le droit à un accompagnement pour prendre des décisions.

39.2 La mesure dans laquelle une personne a une capacité réduite de prendre des décisions ou n'a pas la capacité de le faire doit être établie par une procédure équitable.

39.3 Une personne peut désigner une autre personne ou entité qu'elle autorise à prendre des décisions à sa place. Ces décisions doivent être prises de la manière la moins restrictive possible pour les droits de la personne concernée et de manière compatible avec la dignité, la prise en charge appropriée et la protection de la personne.

Chapitre XX

Personnes en situation de handicap et données de santé

40.1 Les droits et obligations découlant de la présente recommandation s'appliquent à tous les individus, y compris les personnes en situation de handicap. La discrimination ou la stigmatisation des personnes en situation de handicap est inadmissible.

40.2 Les individus ne peuvent pas être contraints de révéler leur situation de handicap ou leurs données de santé en rapport avec cette invalidité. Lorsque la certification du fait du handicap est nécessaire pour accéder à un avantage ou un service, la

certification d'un handicap par une autorité est suffisante pour établir le droit à prestations.

40.3 L'accès aux données de santé des personnes en situation de handicap doit satisfaire aux dispositions de la présente recommandation et servir les intérêts des personnes concernées. L'accès aux données de santé d'une personne en situation de handicap doit se faire sous une forme accessible à cette personne.

Chapitre XXI

Questions de genre, expression du genre et données de santé

41.1 Toutes les mesures administratives nécessaires et autres mesures doivent être prises pour gérer les données de santé de manière à garantir le droit de jouir du meilleur état de santé possible sans discrimination fondée sur le genre, l'identité ou l'expression du genre.

41.2 Des précautions particulières doivent être prises lors de la collecte et de la gestion des données de santé, notamment des catégories utilisées comme marqueurs de genre.

Chapitre XXII

Intersectionnalité et données de santé

42.1 L'intersectionnalité dans les soins de santé s'applique aux praticiens et aux demandeurs de soins de santé. L'interaction de multiples facteurs peut avantager ou désavantager des individus. Indépendamment de tel ou tel groupe ou de l'ensemble des groupes sociaux dont un individu fait partie, chaque personne doit bénéficier de soins de santé de même qualité.

Chapitre XXIII

Données de santé et maladies à déclaration obligatoire

43.1 Le traitement des données de santé nécessaires pour des raisons d'intérêt public dans le domaine de la santé publique, tel que la notification des maladies à déclaration obligatoire, doit être mené conformément aux dispositions des chapitres II et III, et accompagné des mesures adaptées et déterminées visant à protéger les droits et les libertés et à prévenir la discrimination.