Commission nationale de l'informatique et des libertés

Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004)

NOR : *CNIL1818709X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » ;

Vu l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « le règlement général sur la protection des données » - RGPD) et notamment l'article 5, point 2, prévoit que le responsable de traitement doit être en mesure de démontrer que les principes du règlement sont respectés. L'article 9, paragraphe 4 du RGPD précise que les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques ou des données concernant la santé.

Ainsi, en application de la loi du 6 janvier 1978 modifiée (ci-après « loi informatique et libertés »), les traitements de données à caractère personnel à des fins de recherche, étude ou évaluation dans le domaine de la santé sont autorisés par la Commission nationale de l'informatique et des libertés.

La Commission peut homologuer et publier des méthodologies de référence, établies en concertation avec le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (ci-après le CEREES) ainsi qu'avec les organismes publics et privés représentatifs des acteurs concernés.

Ces méthodologies, destinées à simplifier la procédure d'autorisation, portent sur les catégories les plus usuelles de traitements automatisés ayant pour finalité les recherches, études ou évaluations dans le domaine de la santé.

Les responsables de traitement qui adressent un engagement de conformité à cette méthodologie de référence sont autorisés à mettre en œuvre les traitements dès lors que ceux-ci répondent aux conditions prévues par ces dispositions.

Décide :

TITRE Ier

DÉFINITIONS ET CHAMP D'APPLICATION

1.1. *Définitions*

Au sens de la présente méthodologie, les termes suivants sont ainsi définis :

– **donnée à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par

référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

– **traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;
– **responsable de traitement** : la personne physique ou morale qui, seule ou conjointement avec d'autres, est responsable d'une recherche, étude ou évaluation n'impliquant pas la personne humaine, en assure la gestion, vérifie que son financement est prévu et qui détermine les finalités et les moyens des traitements nécessaires à celle-ci ;
– **responsable scientifique ou responsable de la mise en œuvre de la recherche** : la personne désignée par le responsable de traitement, et agissant sous sa responsabilité, veillant à la qualité, l'intégrité et la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci ;
– **sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Il s'agit par exemple du centre participant, d'une société de recherche sous contrat ou d'un prestataire de services informatiques, de centres de ressources biologiques ou d'hébergeurs de données de santé ;
– **professionnel(s) intervenant dans la recherche** : la (ou les) personne(s) physiques qui collecte(nt) les données, dirige(nt) ou surveille(nt) la réalisation de la recherche dans un centre participant. Il s'agit notamment des professionnels de santé, du personnel médical et de personnes qualifiées ;
– **centre participant** : organisme détenant, collectant et/ou transmettant des données et/ou des échantillons biologiques utilisés dans le cadre de la recherche, de l'étude ou de l'évaluation ;
– **données génétiques** : données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;
– **protocole :** document indiquant notamment la méthodologie de la recherche, l'objectif du traitement des données à caractère personnel, les catégories de personnes concernées par le traitement, l'origine, la nature et la liste des données à caractère personnel utilisées et la liste des justifications de recours à celles-ci, la durée et les modalités d'organisation de la recherche, de l'étude ou de l'évaluation, la méthode d'analyse des données, ainsi que, lorsque les caractéristiques de l'étude, de la recherche ou de l'évaluation l'exigent, la justification du nombre de personnes et la méthode d'observation ou d'investigation retenue ;
– **recherche** : recherche n'impliquant pas la personne humaine, étude ou évaluation dans le domaine de la santé ;
– **système fils** : système hébergeant ou mettant à disposition des données directement extraites du Système National des Données de Santé (SNDS) central ou d'un système source ou d'un autre système fils ; un système fils fait partie du « SNDS élargi » ;

1.2. *Traitements de données à caractère personnel inclus dans le champ d'application de la présente méthodologie*

Seuls peuvent faire l'objet d'un engagement de conformité à la présente méthodologie de référence les traitements de données à caractère personnel ayant pour finalité la réalisation de recherches, études et évaluations dans le domaine de la santé ne répondant pas à la définition des recherches impliquant la personne humaine telles que définies à l'article L. 1121-1 du CSP et présentant un caractère d'intérêt public. Un protocole de recherche doit être rédigé et validé scientifiquement par le responsable de traitement avant le début de la mise en œuvre du traitement des données.

Ne peuvent bénéficier de la présente méthodologie de référence :

– les recherches impliquant la personne humaine, telles que définies aux articles L. 1121-1 et R. 1121-1 et suivants du code de la santé publique ;
– les recherches en génétique dont l'objet, principal ou secondaire, est l'identification ou la ré-identification des personnes par leurs caractéristiques génétiques ;
– les recherches, études ou évaluations nécessitant un traitement des données depuis des bases médico-administratives, notamment celles du SNDS et de ses composantes ;
– les recherches nécessitant un appariement par le responsable de traitement entre les données déjà existantes d'un même individu issues de plusieurs centres participants ;
– les recherches pour lesquelles, s'agissant de l'information des personnes concernées, il est fait application de l'exception prévue à l'article 14, paragraphe 5, point b) du RGPD ;
– les recherches pour lesquelles l'analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») indique que le traitement présenterait, malgré les mesures prises en application de l'article 35 du RGPD pour atténuer le risque un risque résiduel élevé pour les droits et libertés des personnes concernées ;

– les recherches nécessitant le traitement du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR).

TITRE II

TRAITEMENTS RELATIFS AUX DONNÉES DES PERSONNES CONCERNÉES PAR DES RECHERCHES

2.1. *Finalité des traitements*

Les traitements de données à caractère personnel des personnes concernées doivent avoir pour seule finalité la réalisation des recherches n'impliquant pas la personne humaine, études ou évaluations présentant un intérêt public décrites à l'article 1.2 ci-dessus.

2.2. *Origine et nature des données*

2.2.1. Nécessité du recours à des données à caractère personnel

L'identification des personnes concernées ne peut être réalisée, dans les bases de données comportant des données de santé à caractère personnel constituées pour la réalisation de la recherche, qu'au moyen d'un numéro d'ordre ou d'un code alphanumérique, établi conformément à l'article 2.2.3, et à l'exclusion de toute donnée à caractère personnel directement identifiante.

Seuls les professionnels et ses collaborateurs intervenant dans la recherche dans un centre peuvent conserver le lien entre l'identité codée des personnes concernées par la recherche et leurs nom(s) et prénom(s) (table de correspondance conservée de façon sécurisée).

L'identification des personnes concernées au moyen d'un numéro d'ordre ou d'un code alphanumérique est nécessaire pour :

– certifier que, pour chaque personne concernée, les informations recueillies successivement au cours de la recherche la concernent ;
– vérifier, par la réalisation de contrôles de validité et de cohérence, la concordance des données recueillies au cours de la recherche avec celles des documents sources.

S'agissant des recherches portant sur la réutilisation de données :

– seules les personnes habilitées initialement à accéder aux données nominatives peuvent détenir la correspondance ;
– le numéro d'ordre affecté à la personne pour l'étude est différent du numéro identifiant le patient dans la base initiale. La correspondance, si nécessaire, sera détenue par le responsable de la base de données initiale.

2.2.2. Origine des données à caractère personnel

Les données relatives aux personnes concernées doivent provenir exclusivement :

– des intéressés eux-mêmes et/ou de leur(s) représentant(s) légal(-aux) ;
– des professionnels intervenant dans la recherche ;
– des bases de données et/ou de collections d'échantillons biologiques, légalement constituées et ayant fait l'objet des formalités nécessaires auprès des autorités compétentes.

2.2.3. Nature des données à caractère personnel

En application de l'article 5, paragraphe 1, point c) du RGPD, les données traitées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données). À cet égard, le responsable de traitement s'engage à ne collecter ou traiter que les données strictement nécessaires et pertinentes au regard des objectifs de la recherche. Dès lors, chacune des catégories de données ne peut être traitée que si leur traitement est justifié scientifiquement dans le protocole de recherche.

Les seules catégories de données à caractère personnel relatives aux personnes incluses dans la recherche pouvant faire l'objet du traitement sont les suivantes :

– identification :
  – âge ou date de naissance (mois et année de naissance, voire jour de naissance si ce dernier est nécessaire à la réalisation d'une recherche impliquant des personnes âgées de moins de deux ans), lieu de naissance, sexe, pays et département de résidence ; numéro d'ordre ou code alphanumérique à l'exclusion des nom(s), prénom(s) et du numéro d'inscription au répertoire national d'identification des personnes physiques. Lorsque le code alphanumérique se compose de lettres correspondant aux nom et prénom des personnes concernées par la recherche, il peut correspondre aux deux premières lettres du nom et à la première lettre du prénom. Il est toutefois recommandé de se limiter aux seules initiales, c'est-à-dire à la première lettre du nom et à la première lettre du prénom. Ces initiales peuvent être complétées d'un numéro d'inclusion et/ou d'un numéro de centre participant ;

  - dans le strict respect des conditions prévues à l'article 2.3.2. de la présente méthodologie : données administratives d'identification des personnes concernées (nom, prénom, coordonnées postales, électroniques et téléphoniques, coordonnées bancaires) ;
- santé : les données strictement nécessaires à la réalisation de la recherche et relatives à la santé de la personne qui s'y prête (par exemple : poids, taille, thérapie suivie dans le cadre de la recherche et concomitante, résultats d'examens, résultats issus d'analyse d'échantillons biologiques, imagerie médicale, données relatives aux effets et événements indésirables, antécédents personnels ou familiaux, maladies ou événements associés, données relatives à un état de santé susceptible d'influencer les résultats ou de rendre impossible la participation en application de contre-indications médicales) ;
- photographie et/ou vidéo et/ou enregistrements vocaux ne permettant pas l'identification des personnes concernées par la recherche (par exemple avec masquage du visage, des yeux, des signes distinctifs) et recueillies dans des conditions conformes aux dispositions applicables en matière de droit à l'image et de droit à la voix ;
- dates relatives à la conduite de la recherche (notamment la date d'inclusion et les dates de visites ou de recueil des données) ;
- origine ethnique ;
- données génétiques strictement nécessaires pour répondre aux objectifs ou finalités de la recherche, ne pouvant en aucun cas être utilisées aux fins d'identification ou de réidentification des personnes, et dont le traitement s'effectue dans les conditions suivantes :
  - réutilisation de données génétiques, obtenues dans le cadre de la prise en charge médicale ou lors d'une recherche antérieure selon les dispositions législatives applicables alors en vigueur ou,
  - réalisation d'un examen des caractéristiques génétiques selon les conditions prévues au premier alinéa de l'article L.1131-1-1 du CSP ;
- situation familiale ;
- niveau de formation (par exemple, primaire, secondaire, supérieur) ;
- catégorie socioprofessionnelle (par exemple, les catégories INSEE) ;
- vie professionnelle (par exemple : profession actuelle, historique, chômage, trajets et déplacements professionnels, expositions professionnelles) ;
- régime d'affiliation à la sécurité sociale (à l'exclusion du numéro d'inscription au répertoire national d'identification des personnes physiques), assurance complémentaire (mutuelle, assurance privée) ;
- participation à d'autres recherches ou études, en vue de s'assurer du respect des critères d'inclusion ;
- déplacements (par exemple vers le lieu de soin ou de la recherche : mode, durée, distance) ;
- consommation de tabac, alcool, drogues ;
- habitudes de vie et comportements, par exemple : dépendance (seul, en institution, autonome, grabataire), assistance (aide-ménagère, familiale), exercice physique (intensité, fréquence, durée), régime et comportement alimentaire, loisirs ;
- mode de vie, par exemple : urbain, semi-urbain, nomade, sédentaire ; habitat (maison particulière ou immeuble, étage, ascenseur, etc.) ;
- vie sexuelle ;
- statut vital, lorsque cette information figure dans le document source ou est connue du professionnel intervenant dans la recherche ;
- remboursement des frais engagés par la personne concernée, liés à la recherche ;
- échelle de qualité de vie ou autres informations sur la qualité de vie de la personne.

2.3. *Destinataires des données à caractere personnel traitées*

Sous la responsabilité du responsable de traitement ou en application de dispositions légales ou réglementaires spécifiques, les catégories de personnes décrites ci-après ont accès aux données traitées, dans les limites de leurs habilitations au regard de leurs fonctions et dans des conditions conformes à la réglementation.

Ces catégories de personnes sont soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal.

2.3.1. Destinataires de données indirectement identifiantes

Peuvent être destinataires de données indirectement identifiantes relatives aux personnes concernées par la recherche :

- le responsable de traitement et ses sous-traitants ;
- le responsable scientifique de la recherche ;
- les professionnels intervenant dans la recherche et les personnels agissant sous leur responsabilité ou leur autorité ;
- le personnel des sociétés du groupe auquel appartient le responsable de traitement et participant au recueil et à l'analyse des données dans le cadre de la recherche ;
- les personnes chargées de la collecte, du contrôle qualité, du traitement et de l'analyse des données ;

- les personnes chargées des affaires réglementaires et de l'enregistrement de la recherche auprès des autorités compétentes ;
- le personnel d'autorités sanitaires et d'autorités publiques de contrôle légalement habilité, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ;
- le personnel habilité agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du responsable de traitement ;
- les experts indépendants chargés de ré-analyser les données pour vérifier les résultats de la recherche, dans le strict respect des conditions mentionnées au paragraphe 2.4 de la présente méthodologie.

2.3.2. Destinataires de données directement identifiantes

Peuvent être destinataires de données directement identifiantes relatives aux personnes concernées par la recherche :

- les professionnels intervenant dans la recherche et les personnels agissant sous leur responsabilité ou leur autorité, concernant les personnes dont ils assurent la prise en charge ;
- les personnes responsables du contrôle et de l'assurance de qualité, lors de la visite ou du contrôle au sein des centres investigateurs chargées de contrôler et d'évaluer la qualité et l'authenticité des données collectées, et notamment par la comparaison des données enregistrées avec le contenu des documents sources. Ces personnes veillent également, sous la responsabilité du responsable de traitement, au respect des dispositions relatives à l'intégrité et à la protection des personnes. Ainsi, les contrôles menés pour s'assurer de la qualité de la recherche (par exemple : accès des attachés de recherche clinique (ARC) et techniciens d'étude clinique (TEC) aux dossiers médicaux des patients) doivent répondre aux règles suivantes en matière de confidentialité :
  - ils doivent être réalisés sous la direction et la surveillance d'un professionnel intervenant dans la recherche ;
  - les personnes destinataires des données doivent être mandatées et habilitées par le responsable de traitement ;
  - la personne concernée par la recherche est préalablement informée et ne s'oppose pas à la réalisation du contrôle ;
  - la personne chargée du contrôle qualité ne peut avoir accès qu'aux données individuelles nécessaires à ce contrôle ;
  - les données consultées servent à vérifier l'authenticité et la cohérence des informations recueillies et si nécessaire à les corriger, compléter, pour autant que les règles de confidentialité soient respectées ;
- le délégué à la protection des données du responsable de traitement, tel que prévu à l'article 37 du RGPD, uniquement dans le cas où la personne concernée entrerait volontairement en contact avec lui ;
- le personnel d'autorités sanitaires et d'autorités publiques de contrôle légalement habilité, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ;
- le personnel habilité agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du promoteur.

Les sous-traitants agissant pour le compte du responsable de traitement, et n'ayant pas la qualité de centre participant, peuvent être destinataires des données administratives d'identification des personnes concernées par la recherche (nom, prénom, coordonnées postales, électroniques et téléphoniques et coordonnées bancaires) dans le strict respect des conditions cumulatives suivantes :

- l'accès aux données à caractère personnel a pour objet de permettre :
  - le remboursement des frais de transport des personnes concernées ou ;
  - le suivi des personnes concernées tel qu'il est précisé dans le protocole de recherche (par exemple : envoi d'un message textuel (SMS) pour compléter un questionnaire en ligne, activation d'un compte informatique en vue de l'utilisation d'une application connectée) ;
- le sous-traitant n'a pas accès aux données de santé relatives aux personnes concernées par la recherche. A l'exception de l'identité du responsable de traitement, la référence de la recherche transmise à l'organisme ne doit pas permettre de révéler une pathologie ou un état de santé sur les personnes concernées ;
- les personnes concernées par la recherche ont été préalablement informées de l'identité du sous-traitant, des catégories de données à caractère personnel les concernant auxquelles il aura accès et des missions qui lui ont été confiées par le responsable de traitement ;
- les données sont conservées par le sous-traitant pendant une durée qui n'excède pas la durée nécessaire à la réalisation de ses missions ;
- une table de correspondance spécifique à la réalisation de ces missions est établie et conservée de manière sécurisée par le sous-traitant.

2.4. *Publication des résultats*

Conformément aux dispositions de la loi « informatique et libertés », la présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées par la recherche.

En cas de publication des résultats de la recherche dans un média scientifique, l'accès aux données par un expert indépendant, mandaté notamment par un éditeur scientifique, ne peut s'effectuer que par l'interface mise à disposition ou déterminée par le responsable de traitement pour la consultation et la manipulation des données, et aux seules fins de ré-analyses des résultats.

Les responsables de traitement ou les personnes agissant pour leur compte doivent s'assurer :

- de la mise en œuvre d'une solution technique ou de l'adhésion à une solution technique mutualisée permettant de mettre les données à disposition sans que les personnes y accédant ne puissent procéder à leur extraction. Une telle solution devra assurer la sécurité des données conservées, notamment :
  - par la délivrance d'habilitations offrant des accès différenciés aux données ;
  - par une authentification fiable des utilisateurs ;
  - par le recours à des canaux de communication chiffrés assurant l'authentification de la source et du destinataire ;
  - par le recours à des algorithmes de chiffrement et des procédures de gestion des secrets à l'état de l'art ;
  - par la mise en œuvre de mesures de traçabilité des accès aux données.
- le cas échéant, de la conformité de l'accès distant aux données aux dispositions relatives au transfert des données hors de l'Union européenne décrites dans la présente méthodologie de référence ;
- de l'information des personnes concernées sur ces destinataires potentiels ;
- que les données sont strictement nécessaires pour reproduire les statistiques publiées ;
- que les données ne contiennent aucune donnée directement identifiante et que le principe de minimisation des données est respecté. À cet effet, les mesures suivantes doivent être mises en place :
  - retirer les informations qui pourraient identifier explicitement un lieu de recherche (nom de centre, code alphabétique de centre) ;
  - retirer les initiales des participants, des investigateurs ;
  - remplacer la date de naissance (mois/année) par l'âge ou par des classes d'âge ;
  - remplacer toutes les dates par des délais par rapport à une date charnière de l'étude (inclusion, randomisation, etc.) ;
  - limiter les données transmises aux données utilisées dans la publication.

2.5. *Information et droits des personnes concernees par la recherche*

2.5.1. Information des personnes

En application des dispositions de la loi informatique et libertés, une information générale sur l'éventualité que les données des personnes puissent être utilisées à des fins de recherche, doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins.

En outre, les personnes concernées par la recherche et/ou leurs représentants légaux sont préalablement et individuellement informés lors d'un traitement de leurs données à caractère personnel, ayant pour fin une recherche visée dans la présente méthodologie. L'information dispensée est conforme aux dispositions de l'article 13 du règlement général sur la protection des données, lorsque les données sont collectées auprès des personnes concernées. L'information dispensée est conforme aux dispositions de l'article 14 du RGPD, lorsque les données ne sont pas collectées auprès des personnes concernées ou ont été préalablement collectées.

Dans le cas de la réalisation d'un examen des caractéristiques génétiques réalisé conformément à l'article L. 1131-1-1 du CSP, les personnes concernées sont également informées du projet de recherche selon les dispositions de cet article.

Les personnes concernées par la recherche et/ou leurs représentants légaux sont également préalablement informées du caractère facultatif de leur participation, lorsque les données sont collectées auprès des personnes concernées et des modalités d'exercice de leurs droits.

Dans l'hypothèse du recueil d'informations par questionnaire remis à la personne concernée par la recherche et/ou à ses représentants légaux, ces informations sont mentionnées sur le questionnaire, la lettre jointe ou la note d'information relative à la recherche.

Lorsque les données à caractère personnel sont recueillies oralement, le professionnel intervenant dans la recherche remet ou fait préalablement parvenir aux personnes concernées par la recherche et/ou leurs représentants légaux un document contenant ces informations.

Des données et/ou des échantillons biologiques recueillis non spécifiquement pour la recherche peuvent faire l'objet d'une réutilisation sans qu'il soit procédé à une nouvelle information individuelle des personnes concernées :

- lorsque la personne concernée dispose déjà des informations prévues aux articles 13 ou 14 du RGPD ;
- ou lorsque l'information délivrée lors de la collecte des données et / ou des échantillons biologiques prévoit la possibilité de réutiliser les données et/ou les échantillons, et renvoie à un dispositif spécifique d'information auquel les personnes concernées pourront se reporter préalablement à la mise en œuvre de chaque nouveau traitement de données.

S'agissant du traitement de données de personnes décédées, sous réserve que le professionnel participant à la recherche ait connaissance du statut vital de la personne concernée et qu'elle ne s'y soit pas opposé de son vivant

par écrit, les données à caractère personnel qui la concernent peuvent faire l'objet d'un traitement à des fins de recherche.

La présente méthodologie de référence n'est pas applicable dans le cas où, s'agissant de l'information des personnes concernées, il est fait application de l'exception prévue à l'article 14, paragraphe 5, point b) du RGPD.

2.5.2. Modalités d'exercice des droits des personnes concernées par la recherche

Le droit d'accès, prévu par l'article 15 du RGPD, peut être exercé à tout moment auprès du professionnel intervenant dans la recherche, directement ou par l'intermédiaire d'un médecin désigné à cet effet par la personne concernée.

Conformément aux dispositions de l'article 16 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes et le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

La personne qui entend s'opposer au traitement des données à caractère personnel la concernant à des fins de recherche dans le domaine de la santé peut exprimer, à tout moment et sans avoir à justifier sa décision, son opposition par tout moyen auprès soit du responsable de la recherche, soit du centre participant ou du professionnel détenteur de ces données, conformément à la loi « informatique et libertés ».

Le droit à l'effacement prévu par l'article 17 du RGPD s'applique lorsque la personne concernée exerce son droit d'opposition et demande également l'effacement des données la concernant déjà collectées. Sous réserve d'une information préalable appropriée par le responsable de traitement, certaines données préalablement collectées peuvent cependant ne pas être effacées, si cette suppression est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de la recherche.

Le droit à la limitation du traitement prévu par l'article 18 du RGPD s'exerce conformément aux dispositions de cet article.

Conformément à l'article 12 du RGPD, le responsable de traitement s'engage à mettre en œuvre des procédures permettant qu'il soit donné suite à ces demandes dans un délai maximal d'un mois à compter de la réception de la demande. Ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Cette prolongation est portée à la connaissance de la personne dans un délai d'un mois à compter de la réception de la demande.

2.6. *Durée de conservation*

Les données à caractère personnel relatives aux personnes concernées par une recherche et traitées à cette fin ne peuvent être conservées dans les systèmes d'information du responsable de traitement, du centre participant ou du professionnel intervenant dans la recherche que jusqu'à deux ans après la dernière publication des résultats de la recherche ou, en cas d'absence de publication, jusqu'à la signature du rapport final de la recherche. Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une durée de vingt ans maximum ou pour une durée conforme à la réglementation en vigueur.

Les personnes énumérées à l'article 2.3 peuvent, en tant que de besoin, accéder à ces données afin d'effectuer des analyses complémentaires ou dans le cadre de nouvelles demandes d'enregistrement auprès des autorités compétentes des médicaments, dispositifs et produits visés, dès lors que les traitements ainsi mis en œuvre le sont pour une finalité compatible avec la finalité initiale, conformément à l'article 5, paragraphe 1, point b) du RGPD et font l'objet de formalités préalables distinctes.

TITRE III

TRAITEMENTS RELATIFS AUX DONNÉES DES PROFESSIONNELS INTERVENANT DANS LA RECHERCHE

3.1. *Finalité des traitements*

Les traitements de données des professionnels intervenant dans la recherche doivent avoir pour seule finalité la mise en place, la réalisation de la recherche et le respect des obligations légales du responsable de traitement.

Les données à caractère personnel des professionnels intervenant dans la recherche peuvent alimenter d'autres traitements de données à caractère personnel mis en œuvre par le responsable de traitement et relatifs à la gestion des ressources humaines et de la formation.

3.2. *Origine et nature des données*

3.2.1 Nécessité du recours à des données à caractère personnel

Le suivi des professionnels intervenant dans la recherche ne peut s'opérer qu'au moyen de données à caractère personnel comportant des données directement identifiantes.

3.2.2. Origine des données

Les données relatives aux professionnels intervenant dans la recherche proviennent des intéressés eux-mêmes, de listes publiques ou de toute autre liste constituée à cette fin dans le respect des dispositions applicables.

3.2.3 Nature des données

En application de l'article 5, paragraphe 1, point c) du RGPD, les données traitées doivent être adéquates, pertinentes et non excessives et limitées à ce qui est strictement nécessaire au regard des finalités du traitement. A cet égard, le responsable de traitement s'engage à ne collecter que les données strictement nécessaires et pertinentes au regard des objectifs de la recherche.

Les seules catégories de données à caractère personnel relatives aux professionnels intervenant dans la recherche pouvant faire l'objet du traitement sont les suivantes :

- identité : nom, prénom(s), sexe, adresse, coordonnées professionnelles postales, électroniques et téléphoniques, coordonnées bancaires ;
- formation – diplôme(s) ;
- vie professionnelle (notamment cursus professionnel, mode et type d'exercice, éléments nécessaires à l'évaluation des connaissances dont ils disposent pour réaliser la recherche) ;
- le cas échéant, numéro d'identification dans le Répertoire partagé des professionnels de santé ;
- montant des indemnités et rémunérations perçues ;
- collaboration à d'autres études ;
- historique des accès et des connexions aux données médicales des personnes participant à une recherche.

3.3. *Destinataires des données à caractère personnel traitées*

Sous la responsabilité du responsable de traitement ou en application des dispositions légales ou réglementaires spécifiques, ont accès aux données traitées, dans les limites de leurs habilitations au regard de leur fonction et dans des conditions conformes à la règlementation, les catégories de personnes suivantes :

- le responsable de traitement, et ses sous-traitants y compris les administrateurs systèmes et les responsables de la sécurité du système d'information ;
- le responsable scientifique de la recherche et ses collaborateurs ;
- les professionnels intervenant dans la recherche, et les personnels agissant sous leur surveillance ou sous leur autorité ;
- les personnes chargées des affaires réglementaires et de l'enregistrement de la recherche auprès des autorités compétentes agissant pour le compte du responsable du traitement ou appartenant aux sociétés de son groupe ;
- le personnel des sociétés du groupe auquel appartient le responsable de traitement ;
- le personnel d'autorités sanitaires et d'autorités publiques de contrôle légalement habilité, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ;
- le personnel habilité agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du responsable de traitement.

Ces catégories de personnes, soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal, peuvent relever du responsable de traitement, des centres participant à la recherche ou de structures agissant pour le compte du responsable de traitement.

3.4. *Information et droits des professionnels intervenant dans la recherche*

3.4.1. Information des professionnels intervenant dans la recherche

L'information est délivrée par une mention figurant sur des documents remis aux personnes concernées ou sur les conventions signées par les professionnels intervenant dans la recherche. Cette information reprend les mentions prévues à l'article 13 du règlement général sur la protection des données.

3.4.2. Modalités d'exercice des droits des professionnels intervenant dans la recherche

Le droit d'accès, de rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit à la portabilité des données et le droit d'opposition s'exercent à tout moment auprès du responsable de traitement, conformément aux articles 15, 16, 17, 18, 20 et 21 du RGPD.

3.5. *Durée de conservation*

Les données à caractère personnel des professionnels intervenant dans la recherche ne peuvent être conservées au-delà d'un délai de quinze ans après la fin de la dernière recherche à laquelle ils ont participé.

Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur.

Les personnes énumérées à l'article 3.3 peuvent en tant que de besoin accéder à ces données afin d'effectuer des analyses complémentaires ou dans le cadre de nouvelles demandes d'enregistrement auprès des autorités compétentes ou pour solliciter la personne pour participer à de nouveaux travaux de recherche.

TITRE IV

MISE EN ŒUVRE ET SECURITÉ

La mise en œuvre de traitements de données à caractère personnel intervenant dans le cadre de la recherche s'effectue sous la responsabilité du responsable de traitement, et/ou chez des tiers agissant pour son compte, dans le respect des dispositions des articles 25, 32 à 35 du règlement général sur la protection des données.

En particulier, le responsable de traitement effectue une analyse d'impact relative à la protection des données, menée conformément aux dispositions de l'article 35 du règlement général sur la protection des données, qui doit couvrir en particulier les risques sur les droits et libertés des personnes concernées. Il met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques identifiés. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques similaires.

Afin de cadrer cette démarche et de justifier de sa mise en œuvre, le responsable de traitement est invité à procéder comme suit à :

- la réalisation d'un schéma fonctionnel avec les flux de données personnelles et leurs supports ;
- l'identification des mesures de sécurité mises en œuvre ;
- l'identification des violations potentielles des données, en précisant la gravité des impacts sur les personnes concernées et la vraisemblance des menaces rendant possibles ces violations.

Le responsable de traitement prend toutes les précautions utiles pour préserver la sécurité des données traitées, en particulier leur confidentialité, leur intégrité et leur disponibilité.

Pour ce faire, il définit, met en œuvre et contrôle l'application d'une politique de sécurité et de confidentialité. Celle-ci pourra notamment décrire, pour la partie concernant les mesures techniques et organisationnelles visant à réduire les risques :

- les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;
- les modalités d'accès aux données, en particulier la gestion des habilitations, les mesures d'identification et d'authentification, les procédures ;
- les mesures de traçabilité des accès aux informations médicales ainsi que l'historique des connexions ;
- les mesures de sécurité devant être mises en œuvre pour les transmissions de données.

Sans préjuger des résultats de la démarche, les particularités du traitement appellent l'attention sur la nécessité de certaines mesures de sécurité :

- les données peuvent faire l'objet d'une informatisation ou, le cas échéant, faire l'objet d'une saisie sur support « papier » renseignés par les professionnels intervenant dans la recherche ou sous leur responsabilité. Lors de la saisie, les données sont identifiées par un numéro d'ordre ou un code alphanumérique, tel que défini à l'article 2.2.3 ;
- l'ensemble des données est saisi soit au fur et à mesure de l'avancement de la recherche, soit globalement lorsque la recherche est terminée ;
- la saisie peut également être réalisée par les professionnels de santé, les laboratoires d'analyses de biologie médicale ou les autres professionnels intervenant dans la recherche et ayant à traiter des données dans le cadre des missions qui leur sont confiées par le responsable de traitement ou la personne agissant pour son compte. Elle peut résulter en particulier d'enregistrements automatiques de paramètres d'examens complémentaires ;
- les données d'une recherche ne doivent pas être saisies, même temporairement, en dehors d'outils faisant partie du traitement ;
- dans le cas de la saisie directe des données par les professionnels intervenant dans la recherche ou chez un sous-traitant, l'outil de saisie distante doit être sécurisé en particulier par l'authentification des utilisateurs et le chiffrement des flux de données ;
- dans le cas de l'utilisation de cahiers d'observation papier, ceux-ci doivent être remis par tout moyen permettant d'en garantir la sécurité et la confidentialité et d'en accuser réception par les personnes habilitées pour la saisie des données ;
- dans le cas de cahiers d'observation numériques installés sur des dispositifs nomades (tablettes, etc.), les données du traitement doivent être chiffrées dans l'appareil et être protégées par une authentification spécifique de l'utilisateur. Elles doivent pouvoir être transférées uniquement vers le traitement, à travers une liaison sécurisée par authentification et chiffrement des flux ;
- tous les échanges électroniques de messages comprenant des données à caractère personnel des personnes concernées par la recherche doivent s'effectuer de manière sécurisée (par exemple : envoi d'un fichier chiffré ou protégé par un mot de passe, messagerie sécurisée, plate-forme dédiée appliquant des droits d'accès spécifiques, etc.) ;
- les outils d'exploitation des données recueillies doivent tenir compte du risque de réidentification des personnes en limitant les possibilités de recherches ciblées et les listes de résultats détaillées.

Le traitement automatisé une fois achevé, les données sont récupérées au format défini par le service en charge du traitement des données de la recherche et sont stockées temporairement - le temps de préparer notamment

l'archivage - sur un répertoire dont l'accès est techniquement restreint aux personnes dûment habilitées et authentifiées.

TITRE V

SYSTÈMES FILS INCLUANT DES DONNÉES ISSUES DU SNDS

Dans le cadre de la présente méthodologie, seules peuvent faire l'objet d'une utilisation les données provenant de systèmes fils conformes aux dispositions des articles L. 1461-1 et suivants du code de la santé publique, ainsi qu'au référentiel de sécurité applicable au SNDS prévu par l'arrêté du 22 mars 2017.

L'utilisation de telles données dans le cadre des recherches visées par la présente méthodologie est soumise aux dispositions précitées.

TITRE VI

TRANSFERTS DE DONNÉES HORS DE L'UNION EUROPÉENNE

Les données indirectement identifiantes des personnes concernées par la recherche et les données directement ou indirectement identifiantes des professionnels intervenant dans la recherche peuvent faire l'objet d'un transfert hors de l'Union européenne lorsque le transfert est strictement nécessaire à la mise en œuvre de la recherche ou à l'exploitation de ses résultats et dans les conditions prévues au Chapitre V du RGPD.

Le transfert peut être effectué dans le cadre de l'engagement de conformité à la présente méthodologie de référence lorsque l'une des conditions suivantes est réunie :

- le transfert s'effectue à destination d'un pays ou une organisation internationale reconnus par la Commission européenne comme assurant un niveau de protection adéquat, conformément à l'article 45 du RGPD (décision d'adéquation) ;
- le transfert s'effectue moyennant des garanties appropriées, listées à l'article 46, paragraphe 2 du RGPD (notamment : clauses contractuelles types approuvées par la commission européenne, règles d'entreprise contraignantes, code de conduite, mécanisme de certification) ;
- en l'absence d'une décision d'adéquation ou de garanties appropriées, le transfert peut être fondé sur l'une des exceptions prévues à l'article 49 du RGPD lorsqu'un tel transfert n'est pas répétitif, massif ou structuré.

Le responsable de traitement doit avoir préalablement informé les personnes concernées du transfert de leurs données à caractère personnel vers des pays tiers à l'Union européenne, de l'existence ou de l'absence d'une décision d'adéquation ou de garantie appropriée et enfin des moyens d'en obtenir une copie conformément à l'article 13, paragraphe 1, point f du règlement général sur la protection des données.

TITRE VII

SOUS-TRAITANTS

Lorsque le responsable de traitement fait appel à un ou des sous-traitants, il s'assure que celui-ci présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD, de la loi « informatique et libertés » et garantisse la protection des droits de la personne concernée.

Le responsable de traitement établit avec le sous-traitant un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD. En particulier, le contrat doit prévoir que le sous-traitant :

- ne traite les données que sur instruction documentée du responsable de traitement et prend toutes les mesures de sécurité requises ;
- ne sous-traite pas sans autorisation écrite du responsable de traitement ;
- aide le responsable de traitement à garantir le respect de ses diverses obligations (droits des personnes, sécurité du traitement, notification de violation, analyses d'impact, etc.) ;
- met à disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits ;
- informe immédiatement le responsable de traitement en cas d'instruction qui, selon lui, constitue une violation du règlement général sur la protection des données ou de la loi informatique et libertés ;

En outre, le sous-traitant :

- désigne, le cas échéant, un délégué à la protection des données conformément à l'article 37 du RGPD ;
- tient un registre des catégories de traitements effectués pour le compte du responsable de traitement, conformément à l'article 30 du RGPD.

Pour tout projet commencé avec un nouveau sous-traitant (n'ayant pas la qualité de centre participant), un audit est effectué. Il couvre notamment la vérification des plans qualité et sécurité du sous-traitant, la validation des systèmes informatiques avec l'existence d'un système de sauvegarde et de récupération des données, et de mesures destinées à garantir leur confidentialité et leur intégrité.

TITRE VIII

MISE EN ŒUVRE DU PRINCIPE DE RESPONSABILITÉ

Chaque responsable de traitement désigne un délégué à la protection des données, en application de l'article 37 du RGPD. Ce délégué à la protection des données aura notamment pour mission de vérifier le respect de la conformité des traitements mis en œuvre selon la présente méthodologie.

Les responsables de traitement adressent à la Commission nationale de l'informatique et des libertés un seul engagement de conformité à la présente méthodologie pour l'ensemble des traitements qu'ils mettent en œuvre dès lors qu'ils sont réalisés en conformité avec l'ensemble des dispositions de la méthodologie. Une demande d'avis auprès du CEREES n'est pas requise.

Conformément à l'article 30 du RGPD, le responsable de traitement tient à jour, au sein du registre des activités de traitement, la liste des traitements mis en œuvre dans le cadre de la présente méthodologie.

Le responsable de traitement est tenu d'enregistrer son traitement de données auprès du répertoire public mis à disposition par l'Institut national des données de santé.

TITRE IX

ENTRÉE EN VIGUEUR

La présente méthodologie de référence entre en vigueur à compter de sa publication au *Journal officiel*.

La présidente,
I. Falque-Pierrotin