Commission nationale de l'informatique et des libertés

Délibération n° 2016-263 du 21 juillet 2016 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée (MR-003)

NOR : *CNIX1622885X*

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° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/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, notamment son article 54, alinéa 5 ;

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

Vu l'ordonnance n° 2016-800 du 16 juin 2016 relative aux recherches impliquant la personne humaine ;

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 ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

En application de l'article 54 de la loi du 6 janvier 1978 modifiée (ci-après loi informatique et libertés), la commission peut homologuer et publier des méthodologies de référence, établies en concertation avec le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (ci-après le CCTIRS) ainsi qu'avec les organismes publics et privés représentatifs.

Ces méthodologies, destinées à simplifier la procédure de demande d'autorisation recherche du chapitre IX, portent sur les catégories les plus usuelles de traitements automatisés ayant pour finalité la recherche dans le domaine de la santé et qui portent sur des données ne permettant pas une identification directe des personnes concernées.

Dans la mesure où certaines recherches ne nécessitant pas le recueil d'un consentement exprès de la personne concernée sont conduites dans le cadre d'exigences législatives et réglementaires strictes, selon des méthodologies standardisées, la commission a estimé qu'il était possible procéder à l'homologation d'une méthodologie de référence établie en concertation avec le comité consultatif, en application de l'article 54 de la loi informatique et libertés.

Ainsi, les responsables de traitement qui adresseront un engagement de conformité à cette méthodologie de référence seront autorisés à mettre en œuvre les traitements dès lors que ceux-ci répondraient aux conditions fixées par celle-ci.

Décide :

TITRE Ier

DÉFINITIONS ET CHAMP D'APPLICATION

1.1. **Définitions**

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

– responsable de traitement : la personne physique ou morale qui prend l'initiative d'une recherche impliquant la personne humaine, qui en assure la gestion, qui vérifie que son financement est prévu et qui détermine les finalités et les moyens des traitements au sens de l'article 3 de la loi informatique et libertés. Il s'agit du promoteur de la recherche ;

– responsable scientifique de la recherche : la personne désignée par le responsable de traitement, et agissant sous sa responsabilité, veillant à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci. Il peut s'agir de l'investigateur coordonnateur ;

– professionnel(s) de santé intervenant dans la recherche : la (ou les) personne(s) physique(s) qui collecte(nt) les données, dirige(nt) ou surveille(nt) la réalisation de la recherche dans un centre participant. Il s'agit notamment des investigateurs, des professionnels de santé, du personnel médical et des personnes qualifiées, au sens des dispositions de l'article L. 1121-3 du code de la sante publique ;
– centre participant : le lieu dans lequel la recherche est réalisée ;
– 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.

1.2. **Traitement 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 dans lesquelles l'inclusion d'une personne suppose qu'elle et/ou ses représentants légaux ne se soit pas opposée(s) à sa participation à la recherche après avoir été dûment informée(és) dans les conditions prévues par l'article 57 de la loi informatique et libertés.

Les recherches concernées par l'application de la présente méthodologie appartiennent aux catégories suivantes :

– les essais cliniques pour lesquels la personne ne s'oppose pas à sa participation, dans le respect des conditions prévues par l'article 30 du règlement UE n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE (essais cliniques par grappes) ;
– les recherches visant à évaluer les soins courants ;
– les recherches non interventionnelles organisées et pratiquées sur/avec l'être humain en vue du développement des connaissances biologiques, médicales ou en santé dans lesquelles tous les actes sont pratiqués et les produits utilisés de manière habituelle, sans procédure supplémentaire ou inhabituelle de diagnostic, de traitement ou de surveillance pouvant porter sur des bases de données et/ou des collections d'échantillons biologiques préexistantes, légalement constituées et ayant fait l'objet des formalités de déclaration et/ou d'autorisation nécessaires auprès des autorités compétentes.

Cependant, la présente méthodologie de référence ne s'applique pas :

– aux traitements de données à caractère personnel relatifs à la gestion de données de santé recueillies dans le cadre de la vigilance (notamment pharmacovigilance, matériovigilance, cosmétovigilance, vigilance alimentaire, hémovigilance, biovigilance) ;
– aux recherches en génétique dont l'objet, principal ou secondaire, est l'identification ou la réidentification des personnes par leurs caractéristiques génétiques ;
– aux recherches nécessitant un appariement avec des données issues des bases médico-administratives ;
– aux recherches pour lesquelles il est envisagé de déroger à l'obligation d'information individuelle des personnes impliquées dans la recherche telle que prévue par l'article 57 de la loi informatique et libertés ;
– aux recherches nécessitant le traitement de données à caractère personnel directement identifiantes, notamment les études prévoyant un suivi longitudinal nécessitant le traitement de telles données.

TITRE II

TRAITEMENTS DE DONNÉES DES PERSONNES SE PRÊTANT À DES RECHERCHES

2.1. **Finalité des traitements**

Les traitements de données à caractère personnel des personnes se prêtant à des recherches doivent avoir pour seule finalité la réalisation des recherches décrites à l'article 1.2 ci-dessus.

Ces traitements incluent la gestion des données relatives aux personnes se prêtant à des recherches, en vue de permettre le recueil, la saisie des cahiers d'observation, le contrôle de validité et de cohérence et l'analyse statistique des données recueillies au cours de la recherche.

2.2. **Origine et nature des données**

2.2.1. *Nécessité du recours à des données à caractère personnel*

L'identification des personnes se prêtant à des recherches ne peut être réalisée, dans un traitement visé par les présentes dispositions, 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.

Ce mode d'identification est nécessaire pour :

– certifier que, pour chaque personne se prêtant à des recherches, les informations recueillies successivement au cours de la recherche et susceptibles de provenir de plusieurs sources la concernent ;

– permettre au responsable de traitement d'identifier les personnes concernées par une modification ou une interruption du traitement en cours de recherche, en vue de la confrontation d'informations provenant de plusieurs professionnels de santé intervenant dans la recherche, des progrès ou des résultats de recherches parallèles et d'en informer le ou les professionnels de santé intervenant dans la recherche, qui sont les seuls à pouvoir contacter rapidement et sans erreur les personnes concernées ;
– 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 auxquels seul le professionnel de santé intervenant dans la recherche peut accéder ;
– satisfaire aux obligations réglementaires en tenant à jour un registre des événements ou effets indésirables qui peuvent survenir en cours de recherche.

2.2.2. *Origine des données*

Les données relatives aux personnes se prêtant à des recherches proviennent des intéressés eux-mêmes et des professionnels de santé intervenant dans la recherche.

2.2.3. *Nature des données*

En application de l'article 6 (3°) de la loi informatique et libertés, les données traitées doivent être pertinentes, adéquates et non excessives 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.** Dès lors, chacune des catégories de données ne peut être collectée que si leur traitement est justifié scientifiquement dans le protocole de recherche.

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

– identification : 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 se prêtant à 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 ;
– 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, suivi et traitement des données relatives aux effets et événements indésirables survenant au cours de la recherche, antécédents personnels ou familiaux, maladies ou événements associés ;
– informations signalétiques : 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 ;
– images : photographie et/ou vidéo ne permettant pas l'identification des personnes se prêtant à la recherche (par exemple avec masquage du visage, 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) ;
– origine ethnique ;
– données génétiques strictement nécessaires pour répondre aux objectifs ou finalités de la recherche, ne permettant pas par elles-mêmes une identification directe ou indirecte de la personne. Ces données ne pourront en aucun cas être utilisées aux fins d'identification ou de réidentification des personnes ;
– situation familiale ;
– niveau de formation (par exemple, primaire, secondaire, supérieur) ;
– catégorie socioprofessionnelle (par exemple, les catégories INSEE) ;
– vie professionnelle : profession actuelle, historique, chômage, trajets et déplacements professionnels ;
– 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 (oui ou non) ;
– déplacements (vers le lieu de soin : 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 ;
– 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 ;
– montant annuel des indemnités perçues ;
– échelle de qualité de vie.

Seul le professionnel de santé qui dirige la réalisation de la recherche dans un centre peut conserver le lien entre l'identité codée des personnes se prêtant à la recherche et leurs nom(s) et prénom(s).

2.3. **Destinataires des données à caractère personnel traitées**

Sous la responsabilité du responsable de traitement ou en application de 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 réglementation, les catégories de personnes suivantes :

– le responsable de traitement et les personnes agissant pour son compte ;
– le responsable scientifique de la recherche ;
– les professionnels de santé intervenant dans la recherche et les personnels agissant sous leur responsabilité ;
– les personnes, au sein des centres participant à la recherche, responsables de l'assurance de qualité, c'est-à-dire 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.

S'agissant des contrôles menés pour s'assurer de la qualité de la recherche et notamment de l'accès des attachés de recherche clinique (ARC) et techniciens d'étude clinique (TEC) aux dossiers médicaux des patients, ils doivent répondre aux règles suivantes en matière de confidentialité :

• être réalisés sous la direction et la surveillance d'un professionnel de santé intervenant dans la recherche ;
• les personnes doivent être habilitées par le responsable de traitement ;
• les personnes concernées doivent en être informées et donner leur accord ;
• la personne chargée du contrôle qualité ne peut avoir accès qu'aux données individuelles nécessaires à ce contrôle, préalablement identifiées par le responsable scientifique de la recherche ;
• les données consultées servent à vérifier l'authenticité et la cohérence des informations recueillies dans le cahier d'observation et si nécessaire à les corriger, compléter, pour autant que les règles de confidentialité soient respectées ;
– les personnes chargées des affaires réglementaires et de l'enregistrement de la recherche auprès des autorités compétentes ;
– les personnels d'autorités sanitaires et d'autorités publiques de contrôle légalement habilités, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ;
– les personnes chargées des analyses statistiques ;
– les personnels habilités agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du promoteur, notamment en application de l'article L. 1121-10 du code de la santé publique.

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 participants à la recherche ou de structures agissant pour le compte du responsable de traitement.

Les données peuvent être transmises aux sociétés du groupe auquel appartient le responsable de traitement et à ses partenaires contractuels, sous une forme qui ne doit pas permettre l'identification directe ou indirecte des personnes se prêtant à la recherche.

Conformément au troisième alinéa de l'article 55 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 se prêtant à la recherche.

2.4. **Information et droits des personnes se prêtant à la recherche**

2.4.1. *Information des personnes*

Outre une information générale sur l'éventualité que leurs données puissent être utilisées à des fins de recherche, en application de l'article 59 de la loi informatique et libertés, les personnes se prêtant à la recherche et/ou leurs représentants légaux sont, en application de l'article 57 de cette même loi, préalablement et individuellement informés du traitement de leurs données à caractère personnel, notamment :

– de la nature des informations transmises ;
– de la finalité du traitement de données ;
– des personnes physiques ou morales destinataires des données ;
– du droit d'accès et de rectification institués aux articles 39 et 40 de la loi informatique et libertés ;
– du droit d'opposition institué aux premier et troisième alinéas de l'article 56 de la loi informatique et libertés.

Les personnes se prêtant à la recherche et/ou leurs représentants légaux sont également préalablement informés du caractère facultatif de leur participation et des modalités d'exercice des droits d'accès, de rectification et d'opposition.

Dans l'hypothèse de recueil d'informations par questionnaire remis à la personne se prêtant à la recherche et/ou à ses représentants légaux, les mêmes informations sont mentionnées sur le questionnaire ou la lettre jointe.

2.4.2. *Modalités d'exercice des droits des personnes se prêtant à la recherche*

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

Le droit de rectification prévu par l'article 40 de la loi informatique et libertés vise la correction de données inexactes, incomplètes ou équivoques au moment de leur collecte. La rectification de ces données pourra être effectuée à tout moment auprès du professionnel de santé intervenant dans la recherche.

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, son opposition par tout moyen auprès soit du responsable de la recherche, soit de l'établissement ou du professionnel de santé détenteur de ces données.

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 de deux mois.

2.5. **Durée de conservation**

Les données à caractère personnel relatives aux personnes se prêtant à 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 de santé intervenant dans la recherche que jusqu'à la mise sur le marché du produit étudié ou jusqu'au rapport final de la recherche ou jusqu'à la publication des résultats de la recherche.

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 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 6 de la loi informatique et libertés et font l'objet des formalités préalables distinctes auprès de la commission.

TITRE III

LES TRAITEMENTS DE DONNÉES DES PROFESSIONNELS DE SANTÉ INTERVENANT DANS LA RECHERCHE

3.1. **Finalité des traitements**

Les traitements de données des professionnels de santé 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 de santé 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 de santé intervenant dans la recherche ne peut s'opérer qu'au moyen de données personnelles comportant leur identité complète.

3.2.2. *Origine des données*

Les données relatives aux professionnels de santé 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 de la loi informatique et libertés.

3.2.3. *Nature des données*

En application de l'article 6 (3°) de la loi informatique et libertés, les données traitées doivent être pertinentes, adéquates et non excessives 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 de santé intervenant dans la recherche pouvant faire l'objet du traitement sont les suivantes :

- identité : nom, prénom(s), sexe, adresse, adresse électronique, téléphone ;
- 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 ;
- participation à d'autres études.

3.3. **Destinataires des données à caractère personnel traitées**

Sous la responsabilité du responsable de traitement ou en application de 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 réglementation, les catégories de personnes suivantes :

- le responsable de traitement et les personnes agissant pour son compte ;
- le responsable scientifique de la recherche ;
- les professionnels de santé intervenant dans la recherche, et les personnels agissant sous leur responsabilité ;
- les personnes chargées des affaires réglementaires et de l'enregistrement de la recherche auprès des autorités compétentes ;
- les personnels d'autorités sanitaires et d'autorités publiques de contrôle légalement habilités, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ;
- les personnels habilités agissant sous la responsabilité de l'organisme d'assurance garantissant la responsabilité civile du promoteur, notamment en application de l'article L. 1121-10 du code de la santé publique.

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 de santé intervenant dans la recherche**

3.4.1. *Information des professionnels de santé 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 de santé intervenant dans la recherche. Cette information reprend les mentions prévues à l'article 32-I de la loi informatique et libertés, notamment les modalités d'exercice des droits d'accès, de rectification et d'opposition.

3.4.2. *Personnes auprès desquelles s'exercent les droits d'accès, de rectification et d'opposition*

Les droits d'accès, de rectification et d'opposition s'exercent à tout moment auprès du responsable de traitement.

3.5. **Durée de conservation**

Les données à caractère personnel des professionnels de santé intervenant dans la recherche ne peuvent être conservées au-delà d'un délai de cinq 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 SÉCURITÉ

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 les conditions suivantes :

- saisie des données :
  - 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 de santé 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 ;
  - cette saisie peut également être réalisée par les professionnels de santé, les laboratoires d'analyses biologiques 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 ;
- contrôle de validité et de cohérence : si la finalité ou la typologie de la recherche le nécessitent, les données font l'objet d'un contrôle de cohérence ou d'un contrôle qualité réalisé selon des modalités conformes aux articles 2.3 et 3.3 de la présente méthodologie ;

– analyse statistique : les données peuvent faire l'objet de traitements statistiques et donner lieu à l'édition de résultats.

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 est déterminée au regard des risques identifiés à la suite d'une étude des risques présentés par le traitement, qui doit couvrir en particulier les risques sur les libertés et la vie privée des personnes concernées.

Elle doit notamment décrire :

– 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.

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.

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

– 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 de santé intervenant dans la recherche ou chez un prestataire, 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 ayant trait aux données de la recherche (demandes de précisions, etc.) doivent intervenir au moyen d'une messagerie sécurisée ou une plate-forme dédiée appliquant des droits d'accès spécifiques (le courriel simple étant proscrit) ;
– 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.

De plus, la relation contractuelle avec les éventuels prestataires de saisie doit intégrer la conformité à l'exigence de sécurité prévue par l'article 34 de cette même loi.

Pour tout projet commencé avec un nouveau prestataire, un audit est effectué. Il couvre notamment la vérification des plans qualité et sécurité de l'entreprise, 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.

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, présentes dans les locaux du responsable de traitement.

TITRE V

TRANSFERTS DE DONNÉES

Seules des données anonymes ou indirectement identifiantes des personnes se prêtant à la recherche peuvent faire l'objet d'un transfert hors de l'Union européenne.

Les données à caractère personnel des professionnels de santé intervenant dans la recherche peuvent faire l'objet d'un transfert hors de l'Union européenne, lorsque ce transfert est strictement nécessaire à la mise en œuvre de la recherche ou à l'exploitation de ses résultats dans un pays qui le requiert, dans les conditions d'encadrement rappelées ci-après.

Tout transfert des données vers un pays non membre de l'Union européenne doit s'opérer conformément aux dispositions spécifiques de la loi précitée relatives aux transferts internationaux de données, notamment en son article 69.

Il est satisfait à ces dispositions lorsque l'une des conditions suivantes est réunie :

– le transfert s'effectue à destination d'un pays reconnu par la Commission européenne comme assurant un niveau de protection suffisant ou d'un organisme appliquant les modalités et utilisant les outils approuvés par la Commission européenne pour la finalité du traitement concerné ;
– le traitement garantit un niveau suffisant de protection de la vie privée ainsi que des droits et libertés fondamentaux des personnes par la mise en œuvre des clauses contractuelles types adoptées par la Commission européenne ou par l'adoption de règles internes d'entreprise (dénommées « BCR »), dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant ;
– il correspond à l'une des exceptions prévues à l'article 69 de la loi informatique et libertés, dont le champ d'application est limité à des cas de transferts ponctuels et exceptionnels. Ainsi, les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (BCR, clauses contractuelles types ou modalités et outils approuvés par la Commission européenne).

Le responsable de traitement doit avoir préalablement informé les personnes concernées de l'existence de transferts de données vers des pays tiers et des droits qui leurs sont reconnus par la loi informatique et libertés ainsi que de leurs modalités d'exercice.

S'il est satisfait à ces conditions et si le traitement dont le transfert est envisagé est par ailleurs conforme à l'ensemble des autres dispositions de la présente méthodologie de référence, l'engagement de conformité à celle-ci porte également autorisation du transfert envisagé en application de l'article 69 de la loi informatique et libertés.

TITRE VI

FORMALITÉS

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 dans le cadre des recherches dès lors qu'ils sont réalisés en conformité avec l'ensemble des dispositions de la méthodologie.

TITRE VII

ENTRÉE EN VIGUEUR

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

Le vice-président,
M.-F. Mazars