



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

Légifrance

Le service public de la diffusion du droit

Délégation 2015-256 du 16 juillet 2015

Commission Nationale de l'Informatique et des Libertés

Nature de la délégation : Référentiel/rglement type/ norme Date de publication sur Légifrance : Mardi 15 septembre 2015
Etat juridique : En vigueur NOR : CNIL1519965X

Délégation n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro (MR-002)

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 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, notamment ses articles L. 1121-1 (1er), L. 1211-2, L. 1241-1, L. 5221-1 et suivants, R. 5211-26 et R. 5221-1 et suivants ;

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 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 les études de performances effectuées en matière de dispositifs médicaux de diagnostic in vitro sont conduites selon des méthodologies standardisées, la commission estime nécessaire de simplifier la procédure ainsi prévue en adoptant une méthodologie de référence dédiée à ces études non interventionnelles après qu'une concertation ait été engagée avec le CCTIRS, le Syndicat de l'industrie du diagnostic in vitro (le SIDIV) et l'Agence nationale de sécurité du médicament et des produits de santé (l'ANSM).

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 :

Article 1

Définitions et champ d'application.

1. Définitions

Le responsable de traitement correspond à toute personne physique ou morale qui détermine les finalités et les moyens de l'étude et ainsi assume la responsabilité de sa mise en œuvre, en application de l'article 3 de la loi du 6 janvier 1978 modifiée dite Informatique et libertés .

Le chargé de mise en œuvre correspond à l'organisme désigné par le responsable de traitement pour mettre en œuvre l'étude concernée.

L'investigateur correspond à la personne physique qui dirige et surveille la réalisation de l'étude non interventionnelle de performances.

2. Traitements concernés

Seuls peuvent faire l'objet d'un engagement de conformité par référence à la présente méthodologie de référence les traitements ayant pour finalités la réalisation d'études non interventionnelles de performances soumises aux dispositions des articles L. 1121-1 (1er), L. 1211-2 et L. 1241-1 du code de la santé publique relatives aux dispositifs de diagnostic in vitro et produits visés au livre II, titre II, de la cinquième partie du code de la santé publique, mis en œuvre par les entreprises ou organismes.

Ces traitements de données à caractère personnel sont ceux mis en œuvre dans le cadre des études non interventionnelles de performances portant sur les dispositifs médicaux de diagnostic in vitro (ci-après, DM DIV) réalisées dans des conditions conformes aux articles L. 5221-1 et suivants du code de la santé publique. Sont exclus du champ d'application de la présente méthodologie de référence, les traitements de données à caractère personnel ne répondant pas à la finalité précitée, notamment, les traitements réalisés dans le cadre des études suivantes :

- les recherches mentionnées aux articles R. 1121-1 et R. 1121-3 du code de la santé publique qui entrent dans le champ d'application des dispositions des articles L. 1121-1 et suivants dudit code relatifs aux recherches biomédicales ;
- les études qui mettent en œuvre un traitement de données à caractère personnel faisant apparaître l'identité complète des personnes se prêtant à l'étude ;
- les études épidémiologiques, les études médico-économiques et notamment celles relevant des dispositions du chapitre X de la loi Informatique et libertés ;
- les études dont l'objet principal est l'étude des comportements ;
- les études en génétique qui ont pour objet d'identifier les personnes par leurs caractéristiques génétiques ou les investigations génétiques portant sur des données sensibles pour lesquelles une rupture de confidentialité pourrait porter atteinte au statut ou à l'état psychologique, familial, social, économique de la personne qui s'est prêtée à la recherche.

Article 2

Finalités des traitements.

Les traitements de données à caractère personnel ont pour seule finalité la réalisation des études non interventionnelles de performances énumérées dans le champ d'application ci-dessus.

Ces traitements incluent la gestion des données relatives aux personnes se prêtant à des études non interventionnelles de performances, 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 l'étude.

Article 3

Nature des données traitées.

S'agissant des données relatives aux personnes faisant l'objet de l'étude :

Les seules catégories de données à caractère personnel relatives aux personnes participant à une étude non

interventionnelle de performances des DM DIV pouvant faire l'objet du traitement sont les suivantes :

- identification : code alphanumérique à l'exclusion des nom(s), prénom(s) et du numéro d'inscription au répertoire national d'identification des personnes physiques. Le code alphanumérique peut correspondre aux deux premières lettres du nom et à la première 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 dès lors qu'un numéro est également attribué à l'inclusion de la personne ;
- santé : thérapie suivie, résultats d'examens, événements indésirables, antécédents personnels ou familiaux, maladies ou événements associés ;
- informations signalétiques : âge ou date de naissance (mois/année), sexe, poids, taille ;
- date d'inclusion dans l'étude ;
- origine ethnique, dès lors que sa collecte est scientifiquement justifiée dans le protocole de l'étude ;
- variations génétiques incluant les polymorphismes génétiques et/ou variations de l'expression des gènes, en relation à la réponse à un médicament ou à un produit ou avec la thérapeutique ;
- consommation de tabac, alcool, drogues ;
- habitudes de vie et comportements : exercice physique (intensité, fréquence, durée), régime et comportement alimentaire ;
- vie sexuelle.

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. Dès lors, chacune des catégories de données précitées ne peut être collectée que si elle est justifiée scientifiquement et strictement nécessaire à la réalisation de l'étude menée en application de la présente méthodologie.

Seul l'investigateur conserve le lien entre l'identité codée des personnes faisant l'objet de l'étude et leur nom(s) et prénom(s).

Les données relatives aux personnes participant à l'étude proviennent des intéressés eux-mêmes et des investigateurs.

S'agissant des données relatives aux investigateurs et autres professionnels intervenant pour la mise en œuvre de l'étude :

Les seules catégories de données à caractère personnel pouvant faire l'objet d'un traitement sont les suivantes :

- identité : nom(s) prénom(s), sexe, adresse, adresse électronique, téléphone ;
- formation - diplôme(s) ;
- montant des indemnités et rémunérations perçues ;
- participation à d'autres études ;
- vie professionnelle : cursus professionnel.

Les données relatives aux investigateurs et aux autres professionnels intervenant dans la mise en œuvre de l'étude non interventionnelle de performances des DM DIV proviennent des intéressés eux-mêmes, des autres intervenants ou de listes publiques.

Article 4

Sur les destinataires.

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 :

- les personnes, désignées par le responsable de traitement chargées de contrôler et d'évaluer la qualité et l'authenticité des données contenues dans les études réalisées, et notamment par la comparaison des données enregistrées avec le contenu des documents sources ;

S'agissant des contrôles menés pour s'assurer de la qualité de l'étude 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 :

- ils doivent être réalisés sous la direction et la surveillance d'un médecin ;
 - les personnes doivent être mandatées par le promoteur et être soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal ;
 - 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 l'investigateur ;
 - les données collectées 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 analyses statistiques ;
 - les membres des services en charge des affaires réglementaires et de l'enregistrement auprès des autorités compétentes des DM DIV ;
 - les inspecteurs 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.

Article 5

Les droits des personnes.

Sur l'information des personnes faisant l'objet de l'étude

Outre une information générale sur l'éventualité que leurs données puissent être utilisées à des fins de recherche, en application de l'article 37 du décret n° 2005-1309 du 20 octobre 2005 modifié, les participants à l'étude sont, en application de l'article 57 de la loi Informatique et libertés, préalablement et individuellement informés du traitement de leurs données à caractère personnel, notamment de :

- la nature des données transmises ;
- la finalité du traitement des données ;
- les personnes physiques ou morales destinataires des données ;
- l'existence de droits d'accès de rectification, d'opposition et de retrait discrétionnaire ainsi que des modalités d'exercice de ces droits.

Cette information individuelle doit s'opérer dans des conditions conformes à l'article 36 du décret précité.

Dès lors que l'étude relèverait des dispositions prévues aux L. 1211-2, alinéa 2, et L. 1241-1 du code de la santé publique, ainsi que par l'article 56 de la loi Informatique et libertés, le consentement des personnes est requis. Les modalités d'expression du consentement précité doivent s'opérer dans des conditions conformes à celles requises par ces dispositions.

Dans l'hypothèse où la réglementation n'impose pas le recueil du consentement des personnes concernées, celles-ci doivent être informées de leur droit de pouvoir s'opposer préalablement ou pendant leur participation à l'étude.

Le droit d'accès peut être exercé à tout moment, soit directement auprès de l'investigateur, soit auprès de l'investigateur par l'intermédiaire d'un médecin désigné à cet effet par l'intéressé.

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 pendant la durée de l'étude auprès de l'investigateur qui doit y donner suite dans un délai maximum de deux mois.

Sur l'information des investigateurs et des professionnels intervenant dans la mise en œuvre de l'étude

L'information est délivrée par une mention figurant sur des documents remis aux personnes concernées ou sur les

conventions signées par les intervenants. 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 et de rectification. Le droit d'accès s'exerce à tout moment auprès du responsable de traitement.

Article 6

Sur les durées de conservation.

Les données à caractère personnel des participants à l'étude non interventionnelle de performances ne peuvent être conservées dans les systèmes d'information de l'organisme que jusqu'au rapport final de l'étude ou jusqu'à l'enregistrement du DM DIV auprès des autorités compétentes.

Elles font ensuite l'objet d'un archivage sur support papier ou informatique.

Les personnes énumérées à l'article 4 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 dispositifs visés dès lors que les traitements ainsi mis en œuvre le seraient pour une finalité compatible avec la finalité initiale conformément à l'article 6 de la loi Informatique et libertés.

Les données à caractère personnel des investigateurs et professionnels intervenant dans la mise en œuvre de l'étude non interventionnelle de performances ne peuvent être conservées au-delà d'un délai de cinq ans après la fin de la dernière étude à laquelle a participé la personne en application de l'article R. 5211-26 du code de la santé publique.

Elles font ensuite l'objet d'un archivage sur support papier ou informatique.

Les personnes énumérées à l'article 4 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 dispositifs ou pour solliciter la personne pour participer à de nouveaux travaux d'étude.

Article 7

Sur les transferts des données.

Seules des données anonymes ou codées des participants à l'étude non interventionnelle de performances des DM DIV peuvent être transmises hors de l'Union européenne.

Les données à caractère personnel des investigateurs et professionnels intervenant dans la mise en œuvre de l'étude non interventionnelle de performances peuvent être transférées hors de l'Union européenne, lorsque ce transfert est strictement nécessaire à la mise en œuvre de l'étude non interventionnelle de performances ou à l'enregistrement du DM DIV 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'une entreprise américaine ayant adhéré aux principes du Safe Harbor 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 (dénommée 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 Safe Harbor).

Le responsable de traitement doit avoir préalablement informé les personnes concernées de l'existence de transfert de données vers des pays tiers, dans les conditions prévues par les dispositions de l'article 91 du décret

du 20 octobre 2005 modifié.

S'il est satisfait à ces conditions et si le traitement, dont le transfert est issu, 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.

Article 8

Mise en œuvre et sécurité des traitements.

La mise en œuvre de traitements de données à caractère personnel intervenant dans le cadre de l'étude s'effectue chez le 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 supports papier renseignés par les investigateurs.

Les résultats des mesures et les données rassemblées tout au long d'une étude sont consignés par les investigateurs ou sous leur responsabilité.

Lors de la saisie, les données sont identifiées par un code alphanumérique, tel que défini à l'article 3 et enregistré dans un cahier d'observation papier ou électronique.

L'ensemble des données est saisi, soit au fur et à mesure de l'avancement de l'étude, soit globalement lorsque l'étude est terminée.

Contrôle de validité et de cohérence :

Si la finalité de l'étude le nécessite, les données peuvent faire l'objet d'un contrôle de cohérence ou d'un contrôle qualité réalisé selon des modalités conformes à l'article 4 de la présente méthodologie.

Analyse statistique :

L'ensemble des données saisies fait l'objet de traitements statistiques et donne 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 ;
- 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 justifier de sa mise en œuvre, le responsable de traitement est invité à procéder comme suit :

- réalisation d'un schéma fonctionnel avec les flux de données personnelles et leurs supports ;
- identification des mesures de sécurité mises en œuvre ;
- 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 étude 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 investigateurs 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 exclusivement remis en main propre aux personnes habilitées pour la saisie des données ;
- dans le cas de cahiers d'observation numériques installés sur des dispositifs nomades (tablettes...), 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 ;
- dans l'hypothèse d'une alimentation directe du traitement par des automates d'analyse, ces derniers doivent disposer d'une connexion sécurisée avec le traitement (authentification et chiffrement) et faire l'objet de mesures de surveillance particulières ;
- tous les échanges électroniques de messages ayant trait aux données de l'étude (demandes de précisions, etc.) doivent se faire sur 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 ré-identification 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 la loi Informatique et libertés.

Pour tout projet commencé avec un nouveau prestataire, un audit est effectué qui 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 l'étude 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 l'étude.

Article 9

Sur les formalités.

Les traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances des dispositifs médicaux de diagnostic in vitro conformes aux présentes dispositions font l'objet d'un engagement de conformité adressé à la Commission nationale de l'informatique et des libertés.

Article 10

Publication.

La présente délibération sera publiée au Journal officiel de la République française.

La présidente,

I. Falque-Pierrotin