



HAL
open science

Research on data: Legal and ethical aspects through the experience of the Foch Hospital

Elisabeth Hulier-Ammar, Amélie Chioccarello, Pauline Touche, Achille Ivasilevitch, Henri Corto Stoeklé, Christian Hervé

► To cite this version:

Elisabeth Hulier-Ammar, Amélie Chioccarello, Pauline Touche, Achille Ivasilevitch, Henri Corto Stoeklé, et al.. Research on data: Legal and ethical aspects through the experience of the Foch Hospital. *Médecine & Droit*, 2022, 2022 (172), pp.8-14. 10.1016/j.meddro.2021.06.003 . hal-03604117

HAL Id: hal-03604117

<https://hal.science/hal-03604117>

Submitted on 16 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License



Disponible en ligne sur

ScienceDirect
www.sciencedirect.com

Elsevier Masson France

EM|consulte
www.em-consulte.com



Protection de la personne – Exercice Professionnel

Recherche sur données : aspects juridiques et éthiques à travers l'expérience de l'hôpital Foch



Research on data: Legal and ethical aspects through the experience of the Foch Hospital

Elisabeth Hulier-Ammar^{a,*}, Amélie Chioccarello^a, Pauline Touche^a,
Achille Ivasilevitch^{b,c,d}, Henri-Corto Stoeklé^{b,c}, Christian Hervé^{b,c,e,f,g}

^a Délégation à la Recherche Clinique et à l'Innovation (DRCI), Hôpital Foch, Suresnes, France

^b Département d'Éthique et Intégrité Scientifique, Hôpital Foch, Suresnes, France

^c Comité d'éthique pour la recherche de l'hôpital Foch (CERF), IRB 00012437, Hôpital Foch, Suresnes, France

^d Laboratoire Dante (EA4498), Université Paris-Saclay (UVSQ), Montigny-Le-Bretonneux, France

^e Université de Paris, Paris, France

^f Académie internationale d'Éthique, Médecine et Politique Publique, Université de Paris, Paris, France

^g Académie vétérinaire de France, Paris, France

ARTICLE INFO

Mots clés:

Données médicales
RGPD
Recherche (données personnelles)
Protection des données: Entrepôt de données

Keywords:

Health data
Personal data
Data studies
GDPR

RÉSUMÉ

Les données de santé font l'objet de convoitise par de nombreux acteurs, bien entendu par les industriels de la santé, notamment du médicament et du dispositif médical, par les hôpitaux et les instituts de recherche, mais aussi par tout type d'entreprises marchandes qui souhaiteraient en retirer des bénéfices conséquents. Face à ce phénomène, les instances de l'Union Européenne, dans le cadre du règlement européen de 2016 (RGPD) remplaçant la directive européenne sur les données de santé de 1995, ont renforcé la protection des données de santé qui sont des données particulièrement sensibles pour tout un chacun et, en conséquence, la réalisation des études sur les données de santé. Les recherches n'impliquant pas la personne humaine, improprement appelées « Études sur données », sont très encadrées par le RGPD et, pour la France, par la Loi Informatique et Libertés (LIL) qui a été modifiée en conséquence. Cet article expose les étapes à réaliser pour la mise en place d'études sur données et les droits des participants/patients dans le cadre de ces recherches. Une vigilance éthique demanderait à ce que ces recherches soient examinées par un comité ad hoc.

© 2021 The Authors. Published by Elsevier Masson SAS. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

ABSTRACT

Health data is the object of covetousness by many actors, of course by the healthcare industry, in particular the drug and medical device industry, by hospitals and research institutes, but also by all types of merchant companies which would like to derive substantial benefits from it. Faced with this phenomenon, the European Commission, within the framework of the replacement of the European Directive on health data of 1995, by the General Data Protection Regulation of 2016 (GDPR) has strengthened the protection of health data which is particularly sensitive data for everyone and, consequently, carrying out studies

* Auteur correspondant.

E-mail address: e.hulier-ammarr@hopital-foch.com (E. Hulier-Ammar).

on health data. Researches that does not involve human beings, improperly called “Data studies”, are closely regulated by the GDPR and, for France, by the Data Protection Act, which has been amended accordingly. This article describes the steps to be taken for the implementation of data studies and what are the rights of participants/patients in the context of these researchs. Ethical vigilance would require that such research be reviewed by an ad hoc committee.

© 2021 The Authors. Published by Elsevier Masson SAS. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Depuis des années, les données personnelles de santé sont convoitées par de nombreux acteurs et c'est encore plus aigu avec le développement des entrepôts de données de santé (EDS) et de l'intelligence artificielle [1–5]. Tout le monde veut utiliser des données de santé pour des finalités diverses [6,7] : les médecins, les hôpitaux, les industriels de la santé (médicament, dispositifs médicaux), les autres industriels, les *start-up*, etc.

La notion de « données à caractère personnel » est précisément définie aux articles 4 du règlement européen n°2016-679 du 27 avril 2016, dit RGPD pour « règlement général sur la protection des données » et article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL) : « 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 ». Par cette définition, il est essentiel de savoir, pour mener à bien des recherches n'impliquant pas la personne humaine, que des données dites codées (expression utilisée en pratique pour signifier qu'un numéro de référence est en lien avec une personne identifiable par ce dernier) ou, selon la terminologie de la réglementation, pseudonymisées (art 4. RGPD), sont juridiquement qualifiées de données personnelles et, par conséquent, doivent respecter la réglementation relative au données personnelles. Or dans le domaine des recherches en santé, il n'est pas une donnée qui ne puisse être rattachée à une personne. Une vigilance toute particulière doit alors être observée sur les données concernant la santé. Cette notion, « données concernant la santé », est également définie à l'article 4 du RGPD. Ce sont « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

Par le RGPD, remplaçant de la directive européenne sur les données personnelles de 1995, la protection des données de santé, qui sont des données particulièrement sensibles pour tout un chacun, a été renforcée et en conséquence, la réalisation des études sur les données de santé [8,9].

Dès lors, en particulier à partir de différents textes de loi et réglementaires, cet article essaiera d'apporter de nouveaux éléments de réponses aux questions suivantes : Comment ces recherches sont-elles régulées ? Par qui sont-elles régulées ? Quels sont les droits des patients/participants à ces recherches ?

1. - Définition d'une recherche sur données

Depuis 2018, dans le monde de la recherche en santé, il existe deux types de recherche décrits dans l'article L.1121-1 du code de

la santé publique¹ : les recherches impliquant la personne humaine et les recherches sur données.

Les recherches impliquant la personne humaine (RIPH) correspondent aux recherches interventionnelles ou observationnelles, en vue du développement des connaissances biologiques ou médicales, qui nécessitent une participation active des participants ; voici quelques exemples de types de recherches RIPH : l'évaluation d'un nouveau médicament ou d'un nouveau dispositif médical, le recueil d'un échantillon de sang spécifique à la recherche, la réalisation d'un scanner ou d'une IRM spécifique à la recherche, ou la réponse à un questionnaire de qualité de vie.

Les recherches n'impliquant pas la personne humaine (RNIPH), improprement appelées « recherches sur données », peuvent être de deux ordres : des recherches qui ne nécessitent pas la participation active des personnes puisqu'il s'agit de réutiliser des « données », générées dans le cadre du soin, pour des finalités de recherche ; et/ou des recherches qui ne permettent pas le développement des connaissances biologiques ou médicales.

Il est donc possible de trouver différentes types de recherches sur « données » dans les articles R.1121-1 du code de la Santé Publique, et 72 de la LIL² : des enquêtes de satisfaction auprès des patients ; des expérimentations en sciences humaines et sociales dans le domaine de la santé ; des évaluations des modalités d'exercice des professionnels de santé ou des pratiques d'enseignement dans le domaine de la santé. Certaines recherches consistent seulement à réutiliser des données issues des dossiers médicaux : traitements, antécédents, imageries (scanner, IRM), échantillons biologiques, photos, télésurveillance des participants, compte-rendu de consultation ou d'hospitalisation, bilans biologiques etc.

Dans le cadre de cet article, nous ne parlerons que de ce second type de recherche, les RNIPH.

2. - Réglementation d'une recherche sur données

Pour rappel, les réglementations européennes et françaises posent un principe d'interdiction de traitement des données sensibles qui forment une catégorie particulière des données personnelles (article 9 du RGPD)³ ; les données de santé et les données de génétique en font partie (Annexe 1). Ce principe est assorti d'exceptions : il est possible de traiter des données sensibles si la personne a donné son consentement (article 9-2 a) RGPD) ou si le traitement des données à des fins de recherche scientifique est proportionné à l'objectif poursuivi et présente des garanties appropriées pour les droits et libertés de la personne concernée (article 9-2 j RGPD) ou encore si le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique comme garantir des normes élevées de qualité et de sécurité des soins de

¹ Code de la Santé Publique (CSP) : <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072665&dateTexte=20200723>.

² Loi Informatique et Libertés (LIL) : <https://www.cnil.fr/la-loi-informatique-et-libertes>.

³ Plateforme des données de santé du Health Data Hub (HDH) : <https://www.health-data-hub.fr/>.

santé et des médicaments ou des dispositifs médicaux. En France, les traitements de données dans la recherche ne peuvent être mis en œuvre qu'en considération de l'intérêt public qu'ils présentent (article 66 LIL). Le respect de ces mesures prend la forme soit d'une autorisation de la Commission Nationale informatique et libertés (CNIL)⁴ soit d'un engagement de conformité à l'une des méthodologies de référence⁵ homologuées par la CNIL tel que décrit dans l'article 73 de la LIL.

Bien que la Loi Informatique et Libertés (LIL) soit en application depuis 1978, c'est depuis les années 2000 et l'apparition de la notion de « données à caractère personnel », que toute recherche en santé, utilisant des données à caractère personnel (Annexe 1) doit obligatoirement obtenir une autorisation ou s'engager à se conformer à une méthodologie de référence homologuée par la CNIL.

Depuis le 25 mai 2018, date de l'entrée en application du RGPD, les recherches sur données sont encadrées par le RGPD⁶, par le Code de la Santé Publique et par loi n° 78-17 du 6 janvier 1978, dite « loi Informatique et Libertés ».

Les réglementations ont pour but de protéger les personnes en protégeant les données personnelles des participants/patients et notamment d'éviter que ceux-ci soient identifiés directement ou indirectement par le biais de leurs données personnelles. Pour les recherches RNIPH, trois préalables⁷ relatifs à la protection des personnes sont à retenir : tout d'abord, les participants/patients doivent être informés de toute recherche réutilisant leurs données à caractère personnel et ne pas s'y être opposés ; puis les données réutilisées doivent être limitées aux stricts besoins de la recherche (pas de recueil de données inutiles) ; enfin les données réutilisées doivent être codées et sécurisées, c'est-à-dire pseudonymisées ou anonymisées (Annexe 1), de façon à ne pas pouvoir facilement identifier les participants/patients.

Ensuite, en fonction du lieu de réalisation de la recherche, du type de données réutilisées, de la faculté d'informer facilement ou pas les participants, comme définit dans la section 3 de la LIL, le responsable de traitement devra : soit obtenir une autorisation de la CNIL ; soit se conformer à une méthodologie de référence et le documenter en interne ; soit n'avoir aucune démarche à faire. Il est alors permis de constater que si le RGPD a instauré le principe d'*accountability* ou autrement dit de responsabilisation des personnes responsables des traitements de données personnelles en ce qu'il limite les formalités administratives de déclaration ou d'autorisation auprès de la Commission nationale de l'informatique et des libertés, il en va différemment des recherches dans le domaine de la santé dans la mesure où il s'agit de traitement et de données personnelles particulièrement sensibles et *in extenso* présentant des risques élevés pour les personnes concernées.

3. - Démarches à entreprendre pour réaliser une recherche sur données

En fonction du type de recherche sur données réalisées, des démarches auprès de la CNIL sont nécessaires ou pas (Annexe 2).

⁴ <https://www.cnil.fr/>.

⁵ Les méthodologies de référence de la CNIL (MR) : <https://www.cnil.fr/fr/les-referentiels-et-methodologies-de-referance-sante>.

⁶ Règlement (UE) 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 (règlement général sur la protection des données = RGPD) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>.

⁷ Méthodologie de Référence 004 (MR-004) : 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) : <https://www.cnil.fr/fr/declaration/mr-004-recherches-nimpliquant-pas-la-personne-humaine-etudes-et-evaluations-dans-le>.

Si la recherche reste dans l'équipe de soin en charge du patient à des fins de recherche interne, conformément à l'article 65.2 de la loi Informatique et Libertés², aucune démarche CNIL n'est nécessaire. L'information aux patients dans cette hypothèse s'effectue au moyen du document d'information générique de l'établissement, l'affichage, le site internet, le livret d'accueil. Et il n'y a pas de nécessité d'information spécifique par recherche. S'il y a « opposition », les données des patients qui s'opposent à la réutilisation de leurs données ne peuvent pas être utilisées⁸.

Si la recherche est multiservice ou multicentrique, il faudra qu'elle se conforme à l'une des méthodologies de référence de la CNIL attestant notamment de l'intérêt public de la recherche (MR004 ou MR005) ou, si nécessaire, qu'elle soit soumise à demande d'autorisation auprès de la CNIL⁹ notamment pour les demandes de dérogation à l'information des personnes.

Pour l'information aux participants, une information individuelle et spécifique par recherche est obligatoire, comme défini dans les articles 69, 70 et 74 de la LIL.

S'il est possible et facile d'informer les participants/patients et que le nom, prénom et/ou date de naissance complète ne sont pas recueillis, il n'y a pas de demande d'autorisation à faire, seulement l'engagement de suivre la méthodologie de référence 004 à condition de se conformer en tous points à l'ensemble de cette méthodologie de référence.

S'il n'est pas possible d'informer les participants/patients (décès, perdus de vue) ou s'il y a de nombreux participants/patients à informer et/ou si la recherche nécessite le recueil du NIR et/ou des nom, prénom et/ou date de naissance complète des participants/patients notamment, une demande d'autorisation auprès de la CNIL est obligatoire, d'après l'article 66 III de la LIL.

Soulignons aussi que, quel que soit le type de recherche, un participant/patient peut s'opposer à n'importe quel moment à l'utilisation de ses données même s'il ne s'est pas opposé en début de recherche ; et que dans chacune des situations présentées, une inscription au registre du responsable de traitement est impérative, de même que la réalisation d'une analyse d'impact (PIA) relative à la protection des personnes.

3.1. Les méthodologies de référence de la CNIL

Il en existe 6 à ce jour (Annexe 3). Celle qui intéresse les RNIPH est la MR 004, 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), qui est disponible intégralement sur le site de la CNIL.

La MR004 définit parfaitement le périmètre des RNIPH et des données qu'il est possible de recueillir pour ces recherches, elle précise également les recherches qui ne font pas partie de son périmètre (Annexe 3).

Chaque RNIPH doit pouvoir répondre aux critères et conditions de la MR004 notamment sur le type de données utilisées, sur les modalités d'information des participants, sur le destinataire des données.

L'analyse d'impact (PIA), selon les articles 62 et 63 de la LIL est nécessaire pour chaque recherche sur données. C'est une analyse permettant de vérifier que la recherche n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés des participants/patients concernées. Si un risque élevé est détecté, une autorisation devra être demandée à la CNIL.

L'analyse d'impact doit notamment vérifier, le système de pseudo-anonymisation utilisé, la localisation de la base de données

⁸ Article 74 de la Loi Informatique et Libertés.

⁹ Section 3 de la Loi Informatique et Libertés, chapitre 3, Titre 2 LIL.

où sont stockées les données de la recherche, les accès à la base de données (qui et comment) et la sécurité informatique mise en place par le responsable de traitement.

Cette analyse est sous la responsabilité du responsable de traitement. En pratique, il s'agit du Responsable de la sécurité des systèmes d'information (RSSI) de la Direction des Systèmes d'Information (DSI) et de la Direction de l'Information Médicale ou de la Direction de la Recherche Clinique de l'établissement de santé. Le Délégué à la Protection des Données doit émettre, de manière indépendante, un avis et des recommandations.

3.2. Demande d'autorisation auprès de la CNIL

Quand une demande d'autorisation est requise, elle est réalisée en deux temps par l'intermédiaire de la Plateforme des Données de Santé, le « Health data Hub » (HDH)^[10], anciennement l'Institut des Données de santé (INDS), qui assure successivement les deux étapes.

Premièrement, intervient le Comité d'Expertise pour les Recherches, les Études et les Évaluations dans le domaine de la Santé (CESREES)¹⁰ (Annexe 4), comité scientifique de la CNIL, dont la mission est de rendre un avis sur les projets d'études nécessitant le recours à des données personnelles de santé.

Deuxièmement, après avis du CESREES, le dossier est soumis à la CNIL qui vérifie tous les aspects de la recherche dont la sécurité juridique et informatique de la recherche. Elle rend une autorisation en deux mois, renouvelable une fois.

La plateforme des données de Santé du Health Data Hub (HDH), remplace l'Institut National des Données de Santé (INDS) et les modalités de soumission sont actuellement en cours de mise en place.

4. Rôle des entrepôts de données

Depuis quelques années, les établissements de soins mettent en place des EDS¹¹. Un entrepôt de données de santé permet de faire converger toutes les données administratives et médicales (compte rendus de consultation, d'hospitalisation, d'imagerie, résultats de biologie, d'anatomopathologie, etc.) issues des différents logiciels utilisés par les professionnels de santé dans une seule et même base de données. Il permet de multiplier les usages des données massives de santé en vue d'améliorer la prise en charge des patients et d'accélérer la recherche clinique.

Ces EDS, disposant de l'ensemble des données sensibles des patients d'un établissement, doivent actuellement faire la plupart du temps l'objet d'une autorisation de la CNIL avec rédaction d'une analyse d'impact.

Dans ce cadre, les EDS doivent avoir une gouvernance qui va assurer la gestion des accès et des données intégrées dans l'EDS. En effet, différents profils d'accès doivent être prévus avec des accès nominatifs, pour les équipes de soins en charge du patient, et les accès pseudonymisés pour les autres intervenants ; il faut déterminer en amont qui peut avoir accès à quoi.

De la même façon, les projets utilisant les données d'un EDS doivent être autorisés soit par un conseil scientifique incluant un membre qualifié en éthique, soit par un comité d'éthique local.

Quant aux patients, ils doivent être informés de l'intégration de leurs données dans un EDS et pouvoir s'y opposer à tout moment ou y avoir consenti. Ensuite, pour chaque projet, une information doit à nouveau être communiquée à chaque patient qui a la possibilité de s'y opposer.

¹⁰ Article 76 2° de la Loi Informatique et Liberté.

¹¹ <https://www.hopital-foch.com/professionnels/recherche/lentrepot-de-donnees-de-sante/>.

Ces dossiers sont longs et complexes à monter, la CNIL envisage de mettre à disposition des utilisateurs un référentiel, sur le modèle des méthodologies de référence, permettant d'éviter les demandes d'autorisation. Ce référentiel est attendu courant 2021.

5. Le transfert de données personnelles vers un pays tiers¹²

Le transfert de données personnelles consiste à toute communication, copie ou déplacement de données ayant vocation à être traitées dans un pays tiers ou par une organisation internationale.

Le responsable de traitement doit impérativement sécuriser les transferts de données personnelles vers des pays tiers en choisissant l'outil juridique le plus adapté à la situation¹³.

Tout d'abord, le responsable de traitement doit dissocier¹⁴ si le transfert à lieu vers un pays dit « adéquat »¹⁵ ou un pays dit « non-adéquat »¹⁶.

La décision d'adéquation de la Commission européenne pour transférer des données personnelles vers un pays tiers est la plus simple pour les responsables de traitement¹⁷ dans la mesure où le responsable de traitement peut transférer des données personnelles vers un pays tiers adéquat. Il existe également des décisions d'adéquation sectorielle c'est-à-dire pour certains secteurs du pays tiers¹⁸.

En l'absence d'adéquation, un transfert peut avoir lieu en mettant en place des garanties de protection des données personnelles suffisantes¹⁹ soit en se fondant sur des règles d'entreprise contraignante ou autrement appelées « *binding corporate rules* (BCR) »²⁰, soit en utilisant des clauses contractuelles types²¹ soit en appliquant des codes de conduite ou des mécanismes de certification approuvés soit en s'appuyant sur des accords internationaux ou arrangements administratifs entre autorités ou organismes publics. Enfin, si un transfert de données personnelles est envisagé vers un pays tiers « non-adéquat » et sans l'une des garanties appropriées ci-dessus, il existe des dérogations strictement encadrées par le RGPD²² qui sont néanmoins peu appliquées en matière de recherche.

Notons qu'une difficulté existe pour les recherches en santé nécessitant des transferts de données personnelles aux États-Unis. Depuis un arrêt majeur de la CJUE (*CJUE, Grande Chambre, 16 juillet 2020, Aff. Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems, Affaire C-311/18*) invalidant le régime de transfert de données personnelles entre l'Union européenne et les États-Unis dit « Privacy Shield », il n'est plus possible de se fonder sur une décision d'adéquation. Dans l'attente de recommandation de la CNIL et du Comité européen de la protection des données, les clauses contractuelles types et les BCR peuvent être utilisées sous réserve de préserver le niveau de protection de la vie privée requis par le RGPD.

¹² Sont considérés comme des pays tiers les pays non membres de l'Union européenne sauf le Liechtenstein et la Norvège (membres de l'Espace Economique Européen).

¹³ Article 44 RGPD.

¹⁴ Article 45 RGPD.

¹⁵ Pays dont la législation en matière de protection des données est considérée comme étant adéquate à la législation de l'Union européenne.

¹⁶ Pays dont le niveau de protection des données est considéré comme insuffisant par l'Union européenne.

¹⁷ La CNIL a produit une carte interactive pour visualiser rapidement les pays « adéquats » et « non-adéquats » : <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>.

¹⁸ Exemple : Anciennement, pour les États-Unis, le Safe Harbor et le Privacy Shield.

¹⁹ Article 46 RGPD.

²⁰ Article 47 RGPD.

²¹ Article 46§2 RGPD - <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries>.

²² Article 49§1 RGPD.

6. Exemple de l'Hôpital Foch

Au vue de ces éléments de réflexion, en 2019, l'Hôpital Foch a décidé de créer le Comité d'Éthique pour la Recherche de Foch (CERF)²³, présidé par le Pr. Christian Hervé, afin de soumettre l'ensemble des recherches sur données de l'hôpital. Le CERF est notamment composé de personnalités extérieures à l'hôpital : un historien, un psychologue, une pédiatre et anesthésiste réanimatrice, un médecin légiste et deux internistes, un juriste en thèse de droit et un biologiste. Cinquante pour cent des membres de ce comité ont suivi un master en éthique et pour le quart des membres un doctorat d'université en éthique. Il donne des avis répertoriés.

Le CERF veille à ce que les recherches respectent les droits et la sécurité de tous les patients/participants en s'assurant de la validité scientifique de chaque projet et de leur conformité aux règles éthiques et réglementaires en vigueur en France et en Europe.

Le CERF est également habilité à donner un accès étendu à l'entrepôt de données de santé de Foch à un investigateur dans le cadre d'une recherche donnée, si celle-ci le justifie.

Le CERF est, depuis le 10 février 2020, enregistré par l'Office for Human Research Protections (OHRP) du ministère de la santé des États-Unis comme *Internal Review Board* (IRB) et à ce titre, les avis rendus sur les recherches sont acceptés pour des appels d'offres internationaux comprenant des fonds américains [11].

Le CERF s'inscrit plus largement dans la démarche éthique de l'Hôpital Foch où la question de l'intégrité scientifique²⁴ est discutée avec l'ensemble des acteurs médicaux et soignants dans le cadre du Groupe de réflexion éthique de l'Hôpital Foch (GREF).

7. Vers une vigilance éthique et prospective

Les recherches n'impliquant pas la personne humaine ne sont pas légalement soumises à évaluation par un comité d'éthique. Elles peuvent néanmoins réutiliser tout type de données des patients si ceux-ci ne s'y sont pas opposés [12]. Mais est-il normal ou pas que chaque responsable de traitement puisse décider seul de la réutilisation des données des patients ?

En principe, l'engagement de conformité à la méthodologie de référence 004 et l'analyse d'impact réalisées pour chaque recherche doivent permettre une régulation de la réutilisation des données des patients. Est-ce suffisant ? Ces actions restent internes au responsable de traitement compte tenu du principe d'*accountability* c'est-à-dire de responsabilisation du responsable de traitement. Un œil extérieur est souvent utile pour discuter sur les projets et éventuellement y apporter des clarifications. C'est pourquoi, l'Hôpital Foch considère ce comité indépendant comme indispensable dans l'élaboration et le déroulement des projets de recherche sur données.

La nécessité d'une évaluation éthique des recherches sur données peut être questionnée. Toutefois, de nombreuses sociétés savantes et de nombreux hôpitaux ont désormais créé un comité d'éthique mutualisé permettant de valider leurs recherches sur données. L'Hôpital Foch, quant à lui, a opté pour un comité rattaché à la Direction Générale tout en garantissant son indépendance dans une charte constitutive. Ce rattachement est un atout dans la mesure où le comité connaissant la structure, peut garantir au mieux les procédures relatives aux protocoles de recherche au sein de l'hôpital. De plus, de nombreux pays européens et outre-Atlantique exigent une telle validation éthique pour tout type de recherches, incluant les RNIPH, depuis des années.

D'ailleurs, ces recherches ont vocation à être publiées et il ne faut pas oublier que la plupart des revues anglo-saxonnes exigent un avis éthique pour autoriser la publication d'une étude sur données. Ne serait-il pas temps de faire la même chose en France [11] ?

Déclaration de liens d'intérêts

Les auteurs déclarent ne pas avoir de liens d'intérêts.

Annexe 1. Quelques définitions issues de la méthodologie de référence 004 de la CNIL

Données à caractère personnel(CNIL) : C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement. Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Données anonymisées : L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. Lorsque l'anonymisation est effective, le RGPD ne s'applique plus aux données ainsi anonymisées, celles-ci n'étant dès lors plus à caractère personnel.

Données pseudonymisées(CNIL) : La pseudonymisation est un traitement de données personnelles réalisée de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires. En pratique la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro dans un classement, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces. C'est pourquoi des données pseudonymisées demeurent des données personnelles. L'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Données sensibles: Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Responsable de traitement (# Promoteur) : la personne physique ou morale qui, seule ou conjointement avec d'autres, est responsable d'une recherche, recherche 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.

Professionnel(s) intervenant dans la recherche(# Investigateur) : 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.

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,

²³ <https://www.hopital-foch.com/patients-familles/recherche/lentrepot-de-donnees-de-sante-eds/>.

²⁴ <https://www.inserm.fr/recherche-inserm/integrite-scientifique>.

la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR-001) ≥ utilisée pour les RIPH interventionnelles de catégories 1 et 2.

Annexe 2. - Quelle(s) démarche(s) pour quelle recherche RNIPH

Localisation de la recherche	Protection des données des participants/patients	Démarches à réaliser				
		Information individuelle	Information Générique	Engagement Méthodologie de Référence	Demande Autorisation CNIL	Rien
Equipe de soins	Anonymisées					
	Pseudonymisées (codées)		X	X ^a		X
Multiservice ou Multisites (multi établissements)	Directement identifiantes (nom, prénom, date de naissance, NIR)	X			X	
	Impossibilité de contact (décès, perdus de vues)				X (dérogation à l'information)	
Multiservice ou Multisites (multi établissements)	Anonymisées					
	Pseudonymisées (codées)	X		X ^a		X
Multiservice ou Multisites (multi établissements)	Directement identifiantes (nom, prénom, date de naissance, NIR)	X			X	
	Impossibilité de contact (décès, perdus de vues)				X (dérogation à l'information)	

^a Pour toute recherche sur données suivant l'une des MR de la CNIL, il faudra réaliser un PIA. Si le PIA montre un risque élevé pour la protection des données, il faudra demander une autorisation à la CNIL.

Mentions obligatoires à intégrer dans la lettre d'information [4] :

- l'identité et les coordonnées du responsable de traitement ;
- les coordonnées du délégué à la protection des données du responsable de traitement ;
- la finalité du traitement de données (présentation du projet de recherche) ;
- la base juridique du traitement (article 6 du RGPD) ;
- la nature des informations qui seront utilisées dans la recherche ;
- les destinataires ou les catégories de destinataires des données ;
- les droits d'accès, de rectification, d'opposition, à l'effacement, à la limitation du traitement ;
- les modalités d'exercice de ces droits ;
- le caractère facultatif de la participation ;
- le cas échéant, le transfert de données à caractère personnel hors de l'Union européenne et la référence aux garanties appropriées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou les critères utilisés pour déterminer cette durée.

Annexe 3. - Les méthodologies de référence de la CNIL. Disponibles sur le site de la CNIL

MR001 : méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des

MR002 : 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).

MR003 : méthodologie de référence relative au traitement des 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 de la personne concernée (MR-003) ≥ utilisée pour les RIPH non interventionnelles de catégorie 3.

MR004 : 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) ≥ utilisée pour les RNIPH.

MR005 : méthodologie de référence relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du PMSI et des résumés de passage aux urgences (RPU) centralisées et mises à disposition sur la plateforme sécurisée de l'ATIH (MR 005).

MR006 : méthodologie de référence relative aux traitements de données nécessitant l'accès pour le compte des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique aux données du PMSI centralisées et mises à disposition par l'ATIH par l'intermédiaire d'une solution sécurisée (MR 006).

FOCUS sur la MR004

Périmètre de la MR004 :

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.

Hors périmètre MR004 :

- les recherches impliquant la personne humaine ;
- 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 demandé une dérogation à l'information
- les recherches pour lesquelles l'analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel, indique que le traitement présenterait 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).

**Annexe 4. - Le comité scientifique de la CNIL (CESREES).
(Informations du site du Health Data Hub visité le 12 juillet 2021)**

Le CESREES (Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé) est chargé de rendre, avant l'autorisation de la CNIL, des avis sur les projets d'études nécessitant le recours à des données personnelles de santé.

Missions.

Le CESREES (Comité d'Expertise pour les Recherches, les Études et les Évaluations dans le domaine de la Santé) se substitue au CEREES. Il se prononce sur :

- La finalité et la méthodologie de la recherche
- La nécessité du recours à des données de santé à caractère personnel

- La pertinence éthique
- La qualité scientifique du projet
- Le cas échéant sur le caractère d'intérêt public que présente le projet.

Fonctionnement

Le CESREES a été créé à la parution du décret d'application de la loi informatique et libertés le 15 mai 2020 et de l'arrêté de nomination de ses membres le 9 juin 2020.

Le secrétariat du comité est assuré par le Health Data Hub.

Composition

Présidé par Bernard Nordlinger, le CESREES est composé d'une vingtaine de membres (nommés par arrêté) et d'un réseau d'experts extérieurs en matière de recherche dans les domaines de la santé, de l'épidémiologie, de la génétique, de la biostatistique, des sciences humaines et sociales, de l'éthique, du juridique et en matière de traitements algorithmiques et de traitement des données à caractère personnel dans le domaine de la santé.

References

- [1] Biclet P. Où en est t'on du Big Data en médecine ? *Médecine & Droit* 2018;2018(150):62–7.
- [2] Zins M, Cuggia M, Goldberg M. Les données de santé en France. *Med Sci (Paris)* 2021;37(2):179–84.
- [3] Polton D. Les données de santé. *Med Sci (Paris)* 2018;34(5):449–55.
- [4] Hervé C, Stanton Jean M. Les systèmes informatisés complexes en santé ; banque de données, télémédecine : normes et enjeux éthiques. Dalloz ed; 2013.
- [5] Hervé C, Stanton Jean M. Les nouveaux paradigmes de la médecine personnalisée : enjeux juridiques, médicaux et éthiques. Dalloz ed; 2014.
- [6] Lucas J. Le partage des données personnelles de santé dans les usages du numérique en santé à l'épreuve du consentement exprès de la personne. *Ethics, Medicine and Public Health* 2017;3(1):10–8.
- [7] Peugeot V. Données de santé : contours d'une controverse. *L'Économie politique* 2018;80(4):30–41.
- [8] Lesaulnier F. Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données. *Médecine & Droit* 2019;2019(158):103–11.
- [9] Siranyan V. La protection des données personnelles des patients face à la modernisation de notre système de santé. *Médecine & Droit* 2019;2019(158):112–7.
- [10] Moore N, Blin P, Lassalle R, Thurin N, Bosco-Levy P, Droz C. National Health Insurance Claims Database in France (SNIRAM), Système Nationale des Données de Santé (SNDS) and Health Data Hub (HDH). In: Sturkenboom M, Schink T, editors. *Databases for Pharmacoepidemiological Research*. Cham: Springer International Publishing; 2021. p. 131–40.
- [11] Stoeklé H-C, Ivasilevitch A, Hulier-Ammar E, Reynaert D, Hervé C. COVID-19 : quel rôle pour les comités d'éthique ? *Médecine & Droit* 2021;2021(167):17–8.
- [12] Griffier R, Jouhet V, Thiessard F, Cossin S. Identification des verrous et des leviers à la réutilisation secondaire des données dans un établissement de santé. *Revue d'Épidémiologie et de Santé Publique* 2020;68:S49–50.