Université de Lille
Faculté D'Ingénierie et Management de la Santé (ILIS)
Master Management Sectoriel
Spécialité Management de la qualité et des risques.

**Louise CALMELET**

# EXIGENCES ET APPLICATION DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN CRO EN FRANCE.

*Sous la direction de Monsieur Hervé HUBERT*

*Mémoire de fin d'étude de deuxième année de Master - 2019*
*Master Management Sectoriel – Management de la qualité et des risques.*

**Composition du jury :**

Monsieur Laurent CASTRA – Président de jury
Monsieur Hervé HUBERT – Directeur de mémoire
Monsieur Olivier D'HONDT – Professionnel invité

*Faculté d'Ingénierie et Management de la Santé - ILIS*
*42 rue Ambroise Paré*
*59120 LOOS*

# REMERCIEMENTS.

Au terme de la rédaction de ce mémoire, je souhaite remercier Monsieur **Hervé HUBERT**, pour son suivi et ses conseils.

Je souhaite également remercier Monsieur **Olivier D'HONDT** pour son accompagnement durant mon stage de Master 1 et mon année d'alternance de Master 2. Ces expériences et son tutorat m'ont permis d'acquérir les connaissances indispensables à ce mémoire.

J'adresse à **l'ensemble de l'équipe pédagogique et administrative de l'Institut Lillois d'Ingénierie de la Santé** et particulièrement à Madame **Marjorie FEMERY** ainsi qu'à **Monsieur Hervé HUBERT,** mes remerciements pour leur soutien et leur accompagnement durant cette année de Master 2.

Enfin, je remercie **Monsieur Laurent CASTRA, Monsieur Hervé HUBERT et Monsieur Olivier D'HONDT** pour leur participation au jury de soutenance de ce mémoire.

# TABLE DES MATIERES.

# TABLE DES FIGURES ET TABLEAUX.

**Figures** :



**Tableaux** :

# GLOSSAIRE.

*Les informations présentes dans ce glossaire sont signalées par un astérisque (*) dans le présent document.*

| | |
|---|---|
| AIPD | Analyse d'Impact relative à la Protection des Données |
| ANSM | Agence Nationale de Sécurité du Médicament et des produits de santé |
| CNIL | Commission Nationale de l'Informatique et des Libertés |
| (e)CRF | (electronic) Case Report Form<br>*Document (électronique) support de recueil des informations* |
| CRO | Contract Research Organisation<br>*Organisation de recherche par contrat* |
| DPO | Data Protection Officer<br>*Délégué à la Protection des Données* |
| BPC | Bonnes Pratiques Cliniques |
| ICH | The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use<br>*Conseil International d'Harmonisation des Exigences Techniques pour l'enregistrement des médicaments à usages humains* |
| MR | Méthodologie(s) de Référence |
| PMSI | Programme de Médicalisation des Systèmes Informatisés |
| RGPD | Règlement Général sur la Protection des Données |
| RIPH | Recherche Impliquant la Personne Humaine |

| | |
|---|---|
| Promoteur | Individu/entreprise à l'origine de la recherche. Met en place, gère ou finance la recherche – Client de la CRO*. |
| Investigateur | Médecin ou autre personnel médical responsable de la conduite des recherches. Est à l'origine de la collecte des données utilisées pour l'étude. |
| Site/centre d'investigation | Lieu (hôpital, structure médicale) d'intervention des investigateurs. |

# INTRODUCTION.

Durant le demi-siècle passé, le monde a connu une émergence technologique à l'origine de grands bouleversements. Bien que les évolutions aient été multiples et progressives avant cette date, le Centre National de Recherche Scientifique (CNRS) a retenu quelques repères significatifs balisant une fulgurante évolution. Il attribue l'arrivée du premier ordinateur à Claude Shannon en 1949. Les prémices de la démocratisation de l'informatique ont été marquées en France par son arrivée dans les administrations au cours des années 1970. Elle se poursuit ensuite par la démocratisation d'Internet dans les années 1990. Puis, dans les années 2000, l'émergence du numérique, principalement symbolisée par les smartphones, s'est accompagnée de celle des nanotechnologies et biotechnologies. Nous parlons alors d'une révolution numérique. (1) (2) (3)

Par son impact mondial, la révolution numérique a radicalement modifié l'organisation des échanges internationaux (échanges d'informations, commerciaux ou encore financiers). Internet, versus mondialisation ; a créé l'instantanéisation de l'offre et de la demande, l'accès quasi illimitées à « *l'information* » en direct. Ce schéma bouleverse évidemment la vie citoyenne plus vite et au-delà des systèmes (géo)politiques en place. (4)

La démocratisation des outils numériques et des réseaux a entraîné des possibilités grandissantes en matière d'exploitation des données personnelles, tant par la quantité d'informations accessibles que par les outils d'analyses de plus en plus performants. Ainsi, la problématique de la protection des données et, en conséquence, la protection de chacun des citoyens qu'elles caractérisent, a très rapidement constitué le talon d'Achille de la généralisation des échanges de toute nature.

Plus rapide que les évolutions politiques, ce développement fulgurant a conduit à créer quelques tensions juridiquement mal cernées qui ont interpellé les politiques en place. Des pares-feux législatifs sont donc apparus.

Les premiers pouvoirs politiques sensibles à cette révolution, furent les régimes totalitaires qui ont très vite censuré voire empêché la diffusion d'internet pour protéger leur mainmise sur le système d'information à la base de leur organisation politique (système d'information descendant mais aussi ascendant afin d'assurer le contrôle de la

communication entre les individus). Sous d'autres régimes des scandales de traitement et récupération excessives de données ont éclaboussé des états réputés les plus emblématiques de la liberté individuelle. Parmi les scandales récents, « *Cambridge Analytica* » découvert en avril 2018, révèle l'utilisation illégale de données impliquant 87 millions d'utilisateurs Facebook par les gouvernements britannique et états-unien.(5) La Chine peut également être citée dans les récents faits de reconnaissance faciale de masse, source de polémique internationale.(6)

Si le droit existant permet de repérer ce type d'infraction, son champ d'application national est un obstacle majeur dans un contexte de mondialisation des échanges. C'est cette difficulté, partagée par la plupart des états, qui a conduit les membres de l'Union Européenne à élaborer un texte commun applicable par tous : le RGPD* (7) (Règlement Général sur la Protection des Données).

Le RGPD*, appliqué depuis le 25 mai 2018, permet d'offrir une réponse locale à un problème international. Il donne une uniformité européenne à la protection des données à caractère personnel. Ces principes ont été envisagés en France, à l'échelle nationale, par la Loi Informatique et Liberté créée en 1978 en même temps que la CNIL* (Commission Nationale d'Informatique et des Libertés). La CNIL* constitue l'autorité française de référence chargée du contrôle en matière de protection des données personnelles.

Parmi les données considérées comme personnelles, dont l'utilisation est encadrée par le RGPD* et la loi Informatique et Liberté, se trouvent les données de santé. La collecte et le traitement de données de santé sont considérés au regard de la CNIL* comme particulièrement sensibles. La recherche clinique, principal vecteur d'utilisation de données de santé, est donc directement impactée par l'évolution de la réglementation.

Les perspectives historiques de l'évolution de la réglementation en matière de recherche médicale, de son contrôle et de ses limites peuvent retenir une date repère : 1947 et le procès de Nuremberg. Parmi les conséquences de ce procès des barbares du nazisme, une réflexion mondiale s'est poursuivie sous l'égide de l'Association Médicale Mondiale, à l'origine de la déclaration d'HELSINKI de 1964. Cette dernière, définit un cadre éthique à la médecine moderne et sera également précurseur de la distinction entre l'expérimentation thérapeutique et l'acte médical.(8) Par la suite, en France, la loi HURIET (9) de 1988, suivie et mise à jour en 2012 par la loi JARDE (10) donneront un socle à la

protection des participants à des recherches biomédicales, s'incluant dans le Code de la santé publique. (11) Aujourd'hui, en France, la loi JARDE fait référence, pour l'encadrement des recherches impliquant la personne humaine. (12)

C'est suite à ces évolutions réglementaires que l'externalisation de certaines étapes d'un essai clinique par les entreprises promotrices (à l'origine des recherches cliniques) a émergé. C'est ainsi que les CRO* (Contrat Research Organization – Organisation de Recherche par Contrat) ont fait leur apparition.

Les CRO* sont des sociétés fournissant un ensemble de services supports autour de la recherche biomédicale. Ces services sont principalement liés à des activités de traitement de données de santé. Elles sont donc concernées d'une part par la loi JARDE, d'autre part, par des obligations strictes en matière de protection des données.

C'est ainsi un contexte réglementaire très rigoureux dans lequel évoluent les CRO*. D'après l'Association Française des CRO* (AFCRO), les difficultés d'application de l'ensemble de ces contraintes semblent être communes aux CRO* françaises. Or, la bonne pratique des traitements de données a un impact important, d'une part, sur la croissance commerciale de ces entreprises, d'autre part, sur la qualité des pratiques de traitement des données, enfin, sur la gestion des informations concernant les personnes participant à ces études ; ce dernier aspect est particulièrement sensible.

Dans le cadre de la recherche clinique, les CRO* sont particulièrement concernées par cette problématique étant donné qu'elles traitent de données de santé. L'évolution des outils technologiques utilisés dans le cadre de la collecte et du traitement des données, présente un atout majeur pour ces entreprises mais elle conduit également à multiplier les risques pour les personnes dont les données sont étudiées.
Pour chaque entreprise, il s'agit d'identifier et de clarifier le foisonnement d'obligations réglementaires qui s'imposent à chaque CRO*.

L'objectif de ce mémoire est de rassembler l'ensemble des obligations en matière de protection des données à caractère personnel s'imposant aux CRO* en France. Par la suite, seront envisagés leurs impacts et leurs mises en application tout au long du processus de réalisation d'une étude clinique.

La problématique est donc la suivante :

***Comment les CRO* françaises peuvent-elles appliquer les exigences réglementaires actuelles de protection des données à caractère personnel ?***

Les données personnelles concernent un grand nombre de domaines d'activités et services d'une entreprise : la gestion des ressources humaines (formation du personnel, données financières du personnel, dossiers de compétences etc.) ou encore la gestion des fichiers client et les relations contractuelles avec chacun.
Certaines situations accroissent les contraintes et dispositifs de sécurité. Les recueils, traitements et archivages de données de santé ne sont possibles que dans des conditions légales bien spécifiques dès lors qu'ils concernent la personne humaine. Aussi, je souhaite ici m'intéresser uniquement aux données personnelles de patients dans le cadre de recherches impliquant la personne humaine.

Afin de répondre à la problématique précitée, je définirai dans un premier lieu le contexte de ce mémoire : qu'est-ce qu'une recherche clinique et plus particulièrement, qu'est-ce qu'une recherche impliquant la personne humaine ? Dans ce cadre, les pratiques réalisées par les CRO* seront détaillées.

Dans une seconde partie, le cadre réglementaire s'imposant à ces pratiques et à la recherche clinique sera décrit dans le contexte de la protection des données à ccaractère personnel.

Cette partie est réalisée par analyse de nombreuses références bibliographiques. Elle permettra de présenter dans une troisième section, les exigences s'imposant aux CRO* lors de recherches impliquant la personne humaine.

Enfin, je tenterai de présenter un outil support d'application de ces exigences pour les CRO*.

# I. DEFINITIONS : RECHERCHE CLINIQUE ET CRO*.

## A. La recherche clinique.

D'après l'ANSM* (Agence Nationale de Sécurité du Médicament et des produits de santé), une recherche ou un essai clinique est « *une recherche biomédicale* [qui concerne la biologie et la médecine] [(13)] *organisée et pratiquée sur l'homme en vue du développement des connaissances biologiques et médicales.* » [(14)]

Afin de définir le cadre de ce mémoire, il est important de faire le point sur les catégories et sous-catégories retenues dans la législation française.

Les essais cliniques peuvent impliquer ou non, la personne humaine. Une étude clinique est considérée comme n'impliquant pas la personne humaine lorsqu'elle réutilise des données de santé préalablement collectées. La recherche est alors considérée comme non interventionnelle puisqu'aucune intervention n'aura lieu sur une personne humaine.

La loi JARDE, mise en place en 2012 (se référer à la partie **II. HISTORIQUE REGLEMENTAIRE**) a redéfini le cadre de la RIPH* (Recherche Impliquant la Personne Humaine).

Il existe désormais trois catégories de RIPH* :

**RIPH* de catégorie 1**

Elles englobent les recherches dites « *interventionnelles* », il s'agit ici de recherches impliquant une intervention hors du parcours de santé habituel défini pour la prise en charge du patient. Une intervention « *non justifiée* » représente toute modification des pratiques courantes de prise en charge d'un patient au regard de son état de santé.

**RIPH* de catégorie 2**

Il s'agit ici de recherches dites « *interventionnelles à risques et contraintes minimes* ». Il peut alors y avoir une intervention non justifiée dans le cadre de la prise en charge du patient mais estimée comme peu invasive. La liste des interventions considérées comme « *peu invasives* » est définie dans le Code de la santé publique.

**RIPH* de catégorie 3**

Il s'agit de recherches dites non interventionnelles ou observationnelles. Ces essais ne comportent ni intervention, ni contrainte pour le patient. (15) (16)

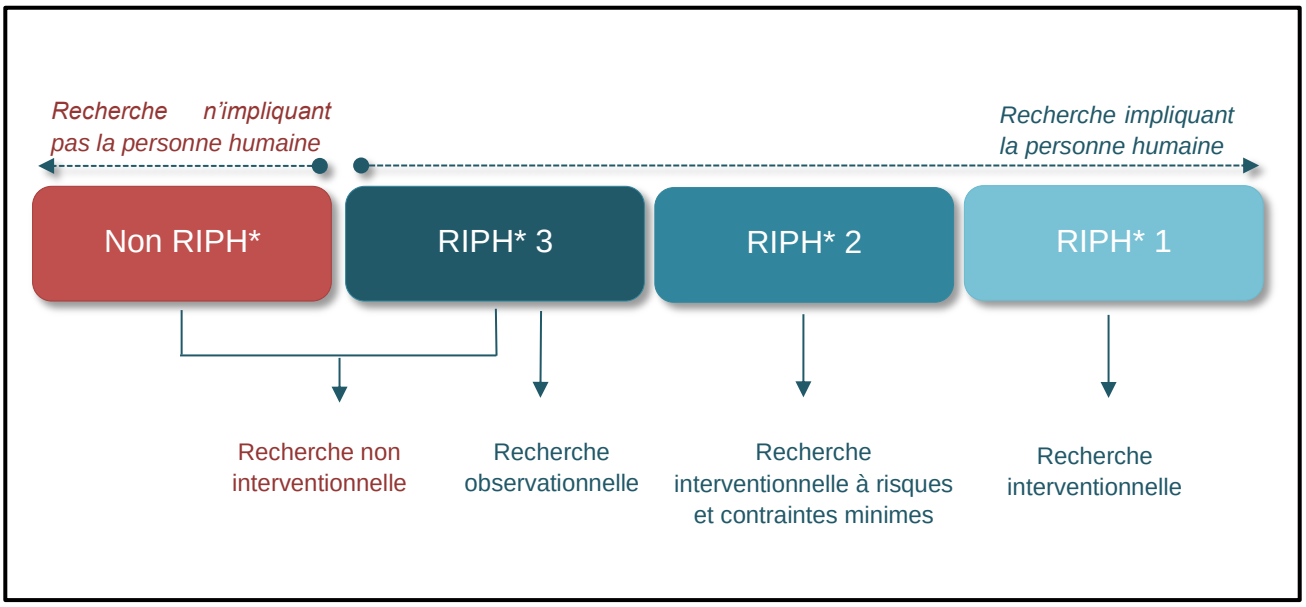


*Figure n°1 – Les différents types de recherches cliniques.*

Les essais cliniques impliquant la personne humaine sont également répartis en quatre phases : [17]

**Etudes de phase 1**

Elles correspondent à la première administration d'un médicament ou d'un dispositif sur l'Homme, en général sur un petit nombre d'individus. Ces études permettent entre autres de vérifier la tolérance du médicament, la dose maximale tolérée, pour vérifier la sécurité de l'emploi, observer la pharmacocinétique chez l'Homme sain et adapter le mode d'administration.

**Etudes de phase 2**

Elles sont considérées comme des études pilotes à petite échelle mais sur un nombre de personnes plus important que pour la phase I. Elles ont pour objectif d'étudier la relation dose-effet, la pharmacocinétique, de trouver la dose minimale efficace, d'évaluer l'effet du médicament sur la maladie. Pour cette phase, les études incluent généralement des personnes porteuses de la maladie concernée.

**Etudes de phase 3**

Il s'agit d'études pivots (thérapeutiques). Elles ont pour objectif d'analyser l'efficacité et la sécurité de l'emploi, le rapport bénéfice/risque, les interactions potentielles. Elles sont généralement menées à plus grande échelle afin de valider l'efficacité (notamment au regard de traitements ou dispositifs déjà existants) ou encore d'ajuster la posologie.

**Etudes de phase 4**

Elles correspondent à une d'étude post-commercialisation. Il s'agit alors du suivi des populations traitées afin de vérifier la sécurité de son usage réel, détecter les effets indésirables à plus long terme, analyser le rapport coût / efficacité, optimiser l'utilisation, la durée du traitement.

## B. La CRO*. (18) (19) (20)

Jusqu'à la deuxième moitié du XX$^{ème}$ siècle, les études cliniques étaient généralement gérées et organisées par les hôpitaux, principalement dans un objectif de compréhension scientifique. C'est en 1940 que les premières entreprises fournissant des services dans le cadre de recherche voient le jour. Par la suite, dans les années 1960, les diverses évolutions (réglementaires, pharmaceutiques, commerciales et technologiques), rendent la mise sur le marché de produits pharmaceutiques de plus en plus complexes incitant donc les laboratoires à réaliser des études sur leurs produits en pré commercialisation.

Dans les années 1980, l'accroissement du nombre d'études réalisées et les évolutions réglementaires ouvrent un potentiel commercial majeur donnant naissance à des entreprises proposant l'externalisation de certaines parties d'une étude clinique. Elles se multiplient alors et s'inscrivent dans une catégorie spécifique : les CRO*.

Les CRO* sont des entreprises de services qui, sur une base contractuelle, engagent des processus de recherches médicales, biomédicales pour des groupes privés (l'industrie pharmaceutique en particulier) ou en réponse à des organismes d'intérêts publics. Les CRO* proposent aux promoteurs* d'études, l'externalisation de l'ensemble ou d'une partie des étapes d'une étude clinique (aspects détaillés dans la partie **C. Intervention des CRO* dans une étude clinique**). Une CRO* capable de réaliser l'ensemble de ces services est considérée comme « *full services* ».

En 2002, après un accroissement important du nombre de CRO*, l'Association Française des CRO* a été créée, puis la Fédération Européenne des CRO* (EUCROF) a suivi en 2005. Ces groupes permettent d'obtenir une collaboration entre les différentes CRO* membres et d'harmoniser quelques modalités. Le 31 janvier 2019, l'Association Française des CRO* a organisé la 8$^{ème}$ journée de la recherche clinique à PARIS. Durant cette journée, elle a présenté un état des lieux de la recherche clinique en France. Il démontre que la France est actuellement le premier pays de la recherche clinique en Europe avec plus 6 730 études supplémentaires enregistrées entre 2017 et 2018, contre 1 148 au Royaume-Uni, 932 en Allemagne ou encore 904 en Espagne.

## C. Intervention des CRO* dans une étude clinique.

Une étude clinique est initiée à la demande d'un promoteur* (client, en général un laboratoire pharmaceutique) qui soumet son projet d'étude à la CRO*. La CRO* va ensuite prendre en charge une partie ou la totalité de l'étude. Les données des patients sont collectées dans des structures médicales appelées centres (ou site) d'investigations*, par des médecins dits investigateurs*. Elles sont ensuite transmises et traitées par la CRO*.

Différents professionnels de la CRO* interviennent dans la réalisation d'une étude :

| ETAPE | INTERVENTION | PROFESSIONNEL(S) |
|---|---|---|
| **Rédaction scientifique et médicale** | Après avoir pris connaissance de la littérature scientifique sur le sujet, la CRO* proposera un synopsis (un résumé du déroulement de l'étude clinique).<br><br>Une fois le synopsis validé par le promoteur*, un protocole détaillant la réalisation de l'étude lui sera soumis puis une étude de faisabilité sera réalisée. | *Rédacteur scientifique* |
| **Soumission réglementaire** | Lorsque l'étude est enclenchée et le protocole validé par le promoteur*, la CRO* doit attester de la licéité de l'étude en soumettant l'ensemble du projet à différentes organisations en fonction du type de RIPH* :<br><br>o **CNIL*** : Selon le type d'étude, la CNIL* a créé des méthodologies de référence précisant les obligations spécifiques à chaque étude. La CRO* doit attester de sa | *Chef de projets* |

| | | |
|---|---|---|
| **Soumission réglementaire (suite)** | conformité à l'ensemble des méthodologies de référence (voir précision dans la partie **III. OBLIGATIONS DE LA CRO***) correspondant aux études qu'elle réalise en interne. Certaines études n'entrent pas dans le cadre des méthodologies de référence. Dans ce cas une autorisation doit être demandée à la CNIL*.<br>○ **Comité de protection des personnes** : il donne un avis sur les conditions dans lesquelles le promoteur* assure la protection des participants à une RIPH*. [21] L'avis du comité est valable 2 ans.<br>○ **ANSM*** : l'ANSM* est sollicité pour les RIPH* 1 (interventionnelles) et délivrera une autorisation ou non sur l'étude à venir. Pour les RIPH*2 et 3, une information à l'ANSM suffit et son autorisation n'est pas nécessaire. L'autorisation est valable 2 ans | *Chef de projets* |
| **Chefferie de projet** | La chefferie de projet assure la supervision de l'ensemble de l'étude clinique. Les chefs de projet sont le point de contact entre les différentes parties prenantes (entre autres les sites d'investigations* et promoteurs*), ils sont également responsables de la soumission réglementaire de l'étude, de la sélection et du suivi des sites d'investigation* ou encore de la supervision des visites de monitoring.<br>Le chef de projet s'occupe de la gestion des TMF (Trial Master Files - dossier contenant l'archivage des documents liés à l'étude). Des recommandations ont été publiées par la Commission Européenne quant au contenu du TMF*. [22] Parmi ses fonctions, le chef de projet gère aussi la sélection des sites d'investigations* et investigateurs*. | *Chef de projets* |

| | | |
|---|---|---|
| **Gestion administrative et financière** | Hormis la gestion des ressources internes, indispensable à toute entreprise, ce service doit également gérer les contrats avec les investigateurs*/Directions hospitalières, financés pour réaliser l'étude, ou la logistique liée à l'étude (envoie des kits avec le matériel nécessaire pour la réalisation de l'étude). | *Chef de projets, assistant Chef de projets* |
| **Saisie** | Les opérateurs de saisie ont pour mission de réceptionner des documents liés à l'étude, en particulier lorsque l'étude est réalisée sur CRF* (Case Report Form).papier et de saisir les données dans la base.<br><br>Afin de limiter les erreurs lors de la copie des données du papier vers le numérique, il est fréquent d'utiliser une méthode de double saisie (saisie par deux personnes). | *Opérateur de saisie* |
| **Monitoring** | Le monitoring est un audit réalisé sur les sites d'investigation* afin d'assurer le bon déroulement de l'étude (respect du protocole et des procédures) et de vérifier la conformité des données collectées.<br><br>Les visites de monitoring sont réalisées par un attaché de recherche clinique (souvent nommé ARC). Le nombre de visites de monitoring à réaliser au cours d'une étude est déterminé en amont avec le promoteur*.<br><br>Durant ses visites, l'attaché de recherche clinique peut, entre autres, vérifier la présence des consentements des participants, la cohérence des dates de rencontre entre investigateurs* et participants ou encore la cohérence des données incluses dans les CRF*. | *Attaché de recherche clinique* |

| | | |
|---|---|---|
| **Data-management** | Les Data-manager ont la charge de préparer la base de données et vérifier la cohérence des données récupérées des CRF* en fonction du protocole de l'étude.<br>Ils vérifient par exemple que tous les champs ont bien été complétés, que chaque patient entre précisément dans le cadrage retenu pour le panel de la population étudiée ou encore que la date de consentement du patient a bien été documentée. | *Data-manager* |
| **Statistique** | A la fin des opérations de data management, la base est gelée. Cela signifie que les données ne peuvent plus être modifiées. C'est alors le début de l'analyse statistique qui validera ou invalidera (en fonction d'indicateurs significatifs) l'hypothèse scientifique émise dans la phase initiale. | *(Bio)statisticien* |
| **Rédaction du rapport** | Lorsque l'analyse statistique est terminée, un rapport est rédigé et transmis au promoteur* de l'étude. Ce rapport apporte la conclusion s'appuyant sur les résultats de l'essai. | *Rédacteur scientifique* |
| **Publication** | En fonction de la demande du promoteur*, les résultats peuvent également être publiés. | *Rédacteur scientifique* |

*Tableau n°1 – Intervention d'une CRO* dans une étude clinique.*

# II. HISTORIQUE RÉGLEMENTAIRE.

## A. Cadre réglementaire de la recherche clinique. [23] [24]

L'existence de règles contraignantes, déterminant un cadre strict à la recherche clinique, n'a pas toujours été une évidence. La médecine expérimentale sur la personne humaine a conduit à de nombreuses tentations diaboliques. Malgré les horribles dérives dont le troisième Reich s'est rendu coupable ultérieurement, c'est paradoxalement en Allemagne que furent promulguées, au cours de la période allant de 1931 à 1933, les premières lois déterminant les conditions dans lesquelles pouvait être envisagée la recherche médicale.

Au terme de la Seconde Guerre mondiale, furent découvertes les barbaries conduites par les médecins nazis au sein des camps de concentration, sous le prétexte d'expérimentations prétendument scientifiques. Une prise de conscience des enjeux liés à la recherche clinique suivit. Le procès de ces crimes de guerre, appelé « *Procès des médecins* » a lieu de 1946 à 1947, suite au procès de Nuremberg. Ces étapes sont marquées par l'élaboration de repères internationaux qui engagent un tournant dans l'histoire de l'éthique médicale.

C'est ainsi qu'en 1964, l'Association Médicale Mondiale rédige le premier texte d'ampleur internationale, consacrant les principes fondamentaux de la recherche biomédicale, « ***la déclaration d'HELSINKI*** ». [25] Deux années plus tard, en 1966 le « *Pacte International Relatif aux Droits Civils et Politiques* » est signé. Il stipule dans son article 7 que « *Nul ne sera soumis à la torture ou à des peines de traitement cruel, inhumain ou dégradant. En particulier, il est interdit de soumettre une personne, sans son libre consentement, à une expérience médicale et scientifique* ».

Par la suite la **déclaration de TOKYO** [26] introduira, en 1975, le principe de comité d'éthique (Comité de Protection des Personnes) puis la **déclaration de MANILLE** [27] (sous le couvert de l'Organisation Mondial de la Santé) en 1981 précisera quant à elle, les directives internationales concernant toutes recherches impliquant la personne humaine.

C'est dans une logique d'appui des principes de ces déclarations (HELSINKI, TOKYO et MANILLE) que deviennent explicites les **BPC*** [28] (*Bonnes Pratiques Cliniques*) en 1990, promues par l'ICH* (*International Council for Harmonization – Conseil international d'Harmonisation des Exigences Techniques pour l'enregistrement des médicaments à usage humain*). Les BPC* décrivent alors des normes internationales pour la recherche impliquant la personne humaine applicables aux Etats-Unis, Japon et Europe. Bien que n'étant pas définies comme entrant dans un cadre légal/réglementaire, les BPC* constituent néanmoins une base importante lors de mise en place d'une recherche impliquant la personne humaine. Les pays non-membres de l'ICH* ont le droit d'assister à certaines de ses sessions et de ses conférences, mais ne prennent pas part aux prises de décision. On estime donc que les intérêts d'environ 85 % de la population mondiale ne sont pas directement représentés dans le processus d'harmonisation.

Concernant la France, c'est sous la double influence des différentes dérives éthiques mais également d'un besoin de l'industrie pharmaceutique d'obtenir une législation lui permettant de réaliser ses essais médicamenteux que fut adoptée la première loi traitant de « *la protection des personnes qui se prêtent à des recherches biomédicales* » – dite **loi HURIET-SERUSCLAT (1988)**, offrant l'autorisation et l'encadrement nécessaires aux « *expérimentations* » sur l'homme.

Par la suite en 2001, le parlement européen promulgue une première directive - **directive 2001/20/CE.** [29] Elle permet alors d'harmoniser les règles en matière de sécurité et de vigilance des essais cliniques entre les états membres de l'Union Européenne. Suite à cette publication, la loi HURIET doit être actualisée. Le premier à dénoncer alors l'incomplétude et l'insécurité du nouveau dispositif législatif fut Claude HURIET lui-même qualifiant de « *sabotage de la loi* » les nouvelles dispositions retenues.

En 2004 **la loi Santé Publique** [30] est promulguée en France afin de compléter la loi HURIET. Elle permettra une transposition de la directive européenne 2001/20/CE : l'avis du Comité de Protection des Personnes devient obligatoire et prend une place majeure après le rôle consultatif auquel il était limité jusqu'alors. Ainsi, l'ANSM* voit son rôle renforcé. Parallèlement, une **Loi bioéthique** [31] s'ajoute en 2004 à une première loi du même nom de 1994, pour contrôler l'utilisation de matériel d'origine humaine. Suite à plusieurs dénonciations d'incomplétude de la loi HURIET, Olivier JARDE, sous le ministère de Roselyne BACHELOT, entame un travail ambitieux de rédaction d'un texte

légal de simplification et d'harmonisation des procédures réglementaires dans ce domaine. C'est ainsi que le 5 mars 2012 est promulguée la **loi JARDE** unifiant les différentes catégories dans un ensemble unique « *la recherche impliquant la personne humaine* » et offrant un socle réglementaire commun à toutes les recherches portant sur l'être humain. La loi JARDE est à l'origine de la distinction entre trois types de recherches impliquant la personne humaine : (RIPH* 1), interventionnelle à risque minime (RIPH* 2) et non interventionnelle (RIPH* 3).

En 2014, le **règlement (UE) n°536/2014** [32] relatif aux essais cliniques de médicaments à usage humain vient abroger la directive de 2001.

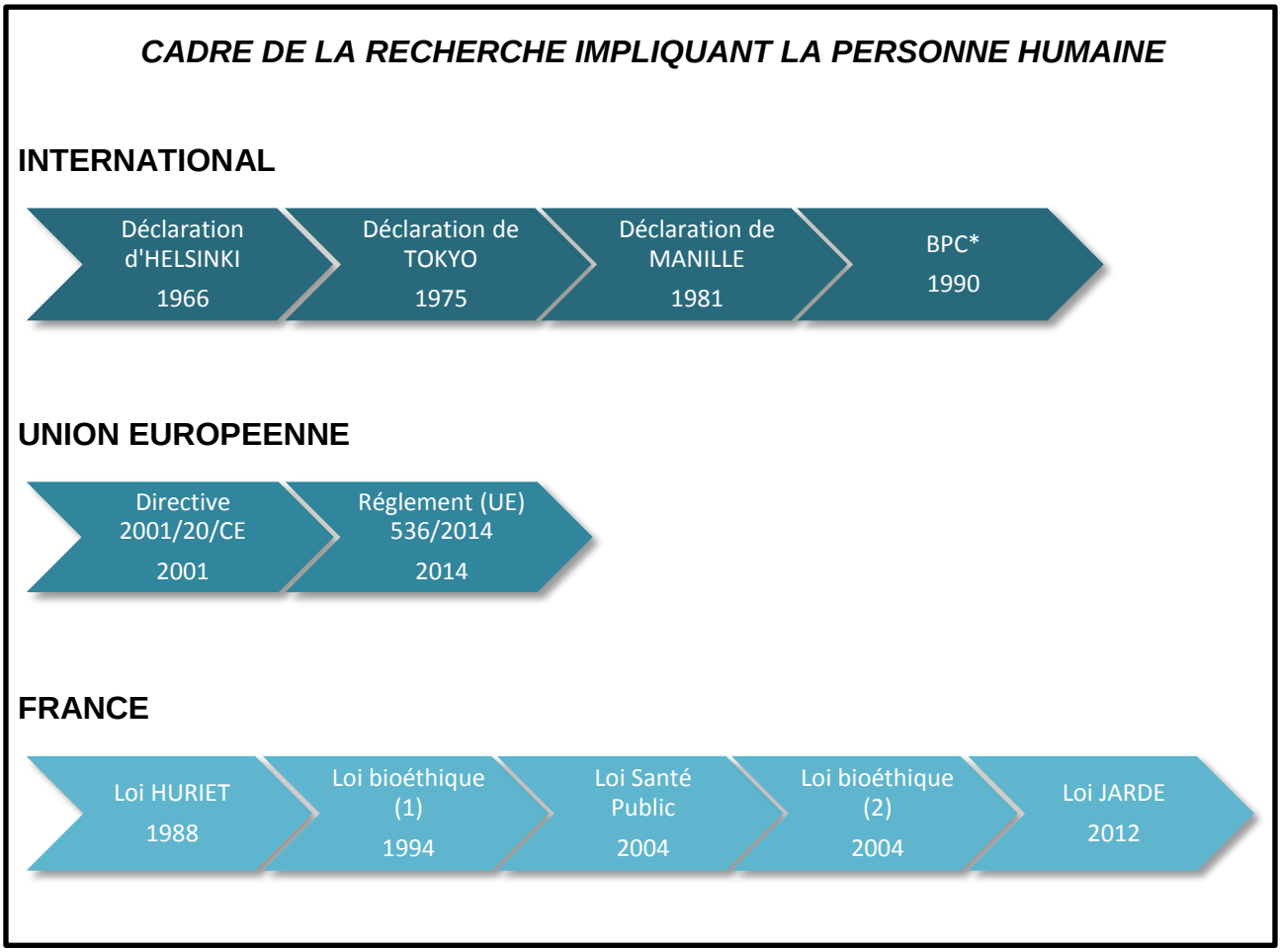


*Figure n°2 – Historique de l'encadrement des essais cliniques.*

## B. Cadre réglementaire de la protection des données personnelles.

Avant de décrire le cadre réglementaire, il est important de définir ce que recouvrent les termes de « *données à caractère personnel* ».

En France, la CNIL* (référente en la matière) définit une donnée personnelle en accord avec le RGPD* comme « *toute information identifiante directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...)* ». [(33)] Dans cette mention, apparaît une notion peu définie et pourtant primordiale : la(les) donnée(s) indirectement identifiante(s). Le choix de cette formule permet d'offrir aux citoyens européens, une protection de toutes les informations qui pourraient potentiellement les identifier.

Il existe deux cas de figure :

- Les données cryptées (pseudonymisation, codage des données par un logiciel etc.) qui bien qu'illisibles en accès direct peuvent être décryptées assez aisément.
- Les données qui, recoupées, identifient une personne. Par exemple : si une entreprise ne dispose pas du nom d'un patient mais possède sa pathologie, son âge, son lieu de naissance et sa ville de résidence, elle peut potentiellement identifier cette personne.

Cette nuance n'est pas reconnue dans tous les pays. Les Etats-Unis par exemple, ne protègent globalement que les données directement identifiantes. D'autres nuances différencient la France d'autres pays, parmi elles, la considération de sensibilité ou de confidentialité.

On doit donc faire le constat que la notion de « *sensibilité* » des données varie d'un pays à l'autre. Les conséquences retentissent sur l'ensemble du domaine étudié, de la recherche à l'entreprenariat industriel ou commercial, dès lors que la culture des citoyens et les législations des différents pays induisent des comportements et pratiques relativement nuancés.

La CNIL* décrit certaines données personnelles comme classiques (nom, prénom ou encore adresse personnelle) et d'autres comme sensibles : les données de santé font partie de cette dernière catégorie. Cette notion est primordiale au regard des obligations légales. En effet, le cadre réglementaire entraîne des astreintes croissantes lors d'utilisation des données dites sensibles.

En France, la question de l'utilisation des données à caractère personnel émerge en 1973, lorsque le Ministère de l'Intérieur et l'Institut National de la Statistique et des Etudes Economiques décident d'utiliser l'informatique pour créer un fichier nommé « *SAFARI* » (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus). Le projet SAFARI a pour but de créer une base de données centralisées de la population fondée sur le fichier de la sécurité sociale. Cette initiative est alors attaquée et présentée comme une entrave grave à la liberté, notamment par un article du journal « *Le Monde* », « *« Safari » ou la chasse aux Français* ». [(34)] C'est le début d'une campagne d'opposition retentissante contre le pouvoir en place : pour répondre à la critique et témoigner de la probité de ses intentions, le gouvernement fait promulguer **la loi Informatique et Liberté**. Elle est appliquée en 1978 sous la présidence de Valery GISCARD D'ESTAING ; la CNIL* sera parallèlement créée comme instance de contrôle de l'application de ce texte. La loi informatique et liberté sera ensuite régulièrement mise à jour, notamment en 2004 et en 2018.

En 1995, peu de temps après la signature du traité de MAASTRICHT, la première directive européenne voit le jour. La **directive 96/46/CE** crée ainsi un socle commun à tous les pays adhérents en matière de protection des données personnelles. Facilitant les échanges intra-européens, la directive marque très vite son obsolescence face à la révolution numérique à l'origine du bouleversement des échanges.

Les données de chaque consommateur d'internet (données volontairement ou indirectement partagées) se trouvent rapidement au centre d'un important et juteux marché parallèle : la collecte des données personnelles de leurs clients conduit la plupart des prestataires à revendre les fichiers constitués à des tiers.

## **RGPD*** :

Le transfert de données est rapidement devenu une forme de spéculation sur laquelle reposent les fonds de commerce de toutes les entreprises du net. Les enjeux commerciaux de facilitation des échanges, mais également de protection des individus, conduit l'Union Européenne à créer une réglementation commune partagée par l'ensemble de ses pays membres. Elle abroge la directive de 1996 pour instaurer le **RGPD***. En tant que règlement, il vient alors imposer ses principes contrairement à la directive qui se limitait à recommander une orientation des pratiques. Créé en 2016, le RGPD* a été mis en application le 25 mai 2018 : les entreprises des pays membres ont deux années pour se mettre en conformité. Le RGPD* laisse également la possibilité aux états membres d'adapter plus de 50 critères à leurs propres lois.

Le RGPD* s'applique à toutes les entreprises ou associations présentes sur le territoire de l'Union Européenne et traitant de données à caractère personnel. Le traitement de données comprend toute action ayant lieu sur les données, de la collecte à l'archivage, de l'analyse en passant par une simple consultation ou lecture. Il s'applique également à toute entreprise ou association traitant de données à caractère personnel de citoyens de l'Union Européenne, même si elle n'est pas située en France. En bref, toute entreprise *présente sur le sol de l'Union Européenne* ou *traitant de données de citoyens de l'Union Européenne* est soumise au RGPD*.

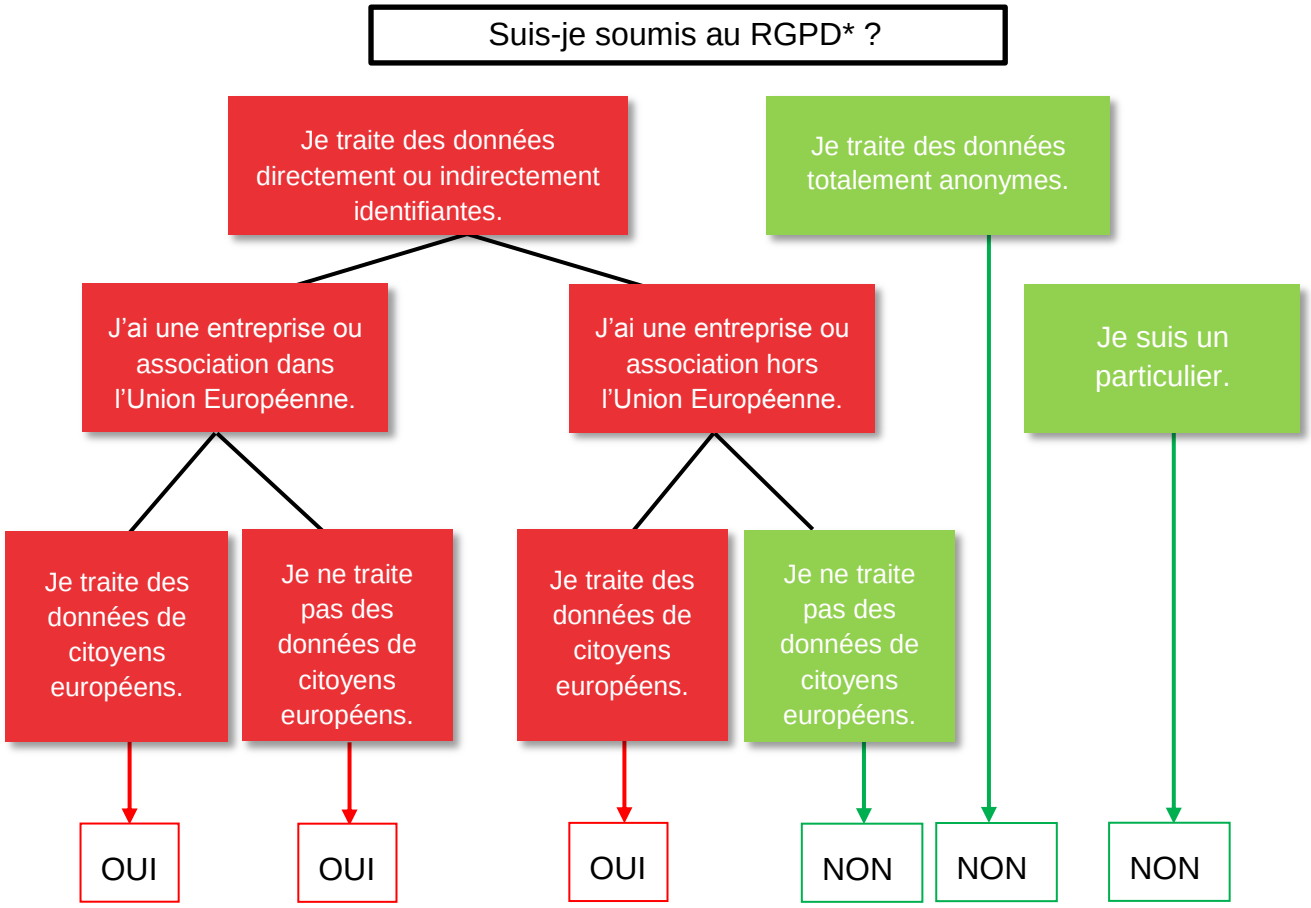


*Figure n°3 – Soumission au Règlement Général sur la Protection des Données.*

Supervisé par le G29, groupe de travail regroupant les autorités de contrôle de l'ensemble des pays de l'Union Européenne, le RGPD* vient introduire de nombreux principes fondamentaux. Il oblige l'ensemble des parties traitant les données personnelles, à mettre en place toutes les mesures afin d'assurer la protection de ces dernières. Le RGPD* a été promulgué dans une optique de responsabilisation des entreprises, en utilisant une approche par le risque. Il permet ainsi de faciliter les échanges intra-européens, mais également de protéger les individus lors des multiples traitements subis par leurs données. Mais le point de vue nouveau qu'il instaure repose sur le principe de la protection de chaque citoyen et impose donc les nouvelles dispositions à toute entreprise utilisant ou traitant des données personnelles quel que soit le pays de son siège.

Alors qu'auparavant les entreprises françaises étaient étroitement supervisées par la CNIL* dans la mise en place des traitements de données, elles sont davantage

autonomes aujourd'hui. En contrepartie, elles doivent assurer (prouver) le respect des obligations imposées par le RGPD* en cas d'audit de la CNIL* risquant une sanction financière allant jusqu'à 4% du chiffre d'affaire mondial. L'Europe choisit ainsi un verrouillage dédoublé : les entreprises sont responsabilisées et bénéficient d'un gain d'indépendance mais elles s'exposent, en cas de défaillance, à de très lourdes sanctions.

En plus de modifier l'encadrement des pratiques, le RGPD* crée certains principes dont la création d'un registre de traitement, la nomination d'un référent en protection des données ou encore le droit à l'effacement qui n'existaient pas auparavant (ces principes sont détaillés dans la partie **IV. OBLIGATIONS DE LA CRO***). Le RGPD* est également à l'origine, durant l'année écoulée, d'une adaptation du cadre national, amenant à des modifications des méthodologies de référence ainsi que de la loi Informatique et Liberté ou encore du Code de la santé publique.

## MÉTHODOLOGIES DE RÉFÉRENCE :

Précurseur de cette responsabilisation, en 2014, parallèlement à la promulgation de la loi JARDE, la CNIL* avait décrit des méthodologies de référence offrant aux entreprises des modalités de référence. Ces méthodologies de référence permettent aux CRO* d'une part d'assurer leur conformité aux multiples obligations légales, d'autre part de faire une unique déclaration de conformité de leurs méthodologies auprès de la CNIL*. Cette pratique supprime ainsi la nécessité de déclaration de chaque étude à la CNIL*.

A chaque type d'essai décrit dans la loi JARDE correspond une méthodologie de référence. Chacune permet de déterminer les modalités de traitement des données personnelles mais également de consentement et d'information des personnes en fonction du type d'étude. Elles regroupent l'ensemble des informations et dispositions à mettre en place dans le cadre d'une collecte de données en fonction du contexte. Les méthodologies de référence précisent pour chacune le niveau d'exigence attendu (quelques exemples : la définition des responsabilités des partis, les types de données concernées, la durée de conservation des données, l'encadrement des transferts de données, les modalités d'information et consentement ou les transferts hors Union Européenne…).

Il existe actuellement 6 méthodologies de référence appelé MR* :

| | |
|---|---|
| MR*-001 | *« Recherche dans le domaine de la santé avec recueil du consentement ».* [35] |
| MR*-002 | *« Etudes non-interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro ».* [36] |
| MR*-003 | *« Recherche dans le domaine de la santé sans recueil du consentement ».* [37] |
| MR*-004 | *« Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé ».* [38] |
| MR*-005 | *« Études nécessitant l'accès aux données du PMSI* (Programme de Médicalisation des Systèmes Informatisés) et/ou des RPU (Résumés de Passage aux Urgences) par les établissements de santé et les fédérations hospitalières ».* [39] |
| MR*-006 | *« Études nécessitant l'accès aux données du PMSI* (Programme de Médicalisation des Systèmes Informatisés) par les industriels de santé ».* [40] |

La **MR*-001** s'applique aux **RIPH* 1** et **RIPH* 2**. Elle vise notamment les traitements de données ayant pour objet une recherche interventionnelle, un essai clinique de médicament et une recherche nécessitant la réalisation d'un examen génétique.

La **MR*-003** s'applique aux **RIPH* 3**. Elle peut également s'appliquer aux **RIPH* 2** dans le cas d'une information donnée collectivement. La MR*-003 vise notamment les traitements de données ayant pour objet une recherche non interventionnelle, interventionnelle à risques et contraintes minimes (lorsque l'information est collective uniquement) et les essais de médicaments par grappes.

Dans certains cas les RIPH* peuvent ne pas entrer dans le cadre des méthodologies de référence. C'est le cas par exemple si des données ne figurant pas dans la liste des données autorisées des méthodologies de référence sont collectées.

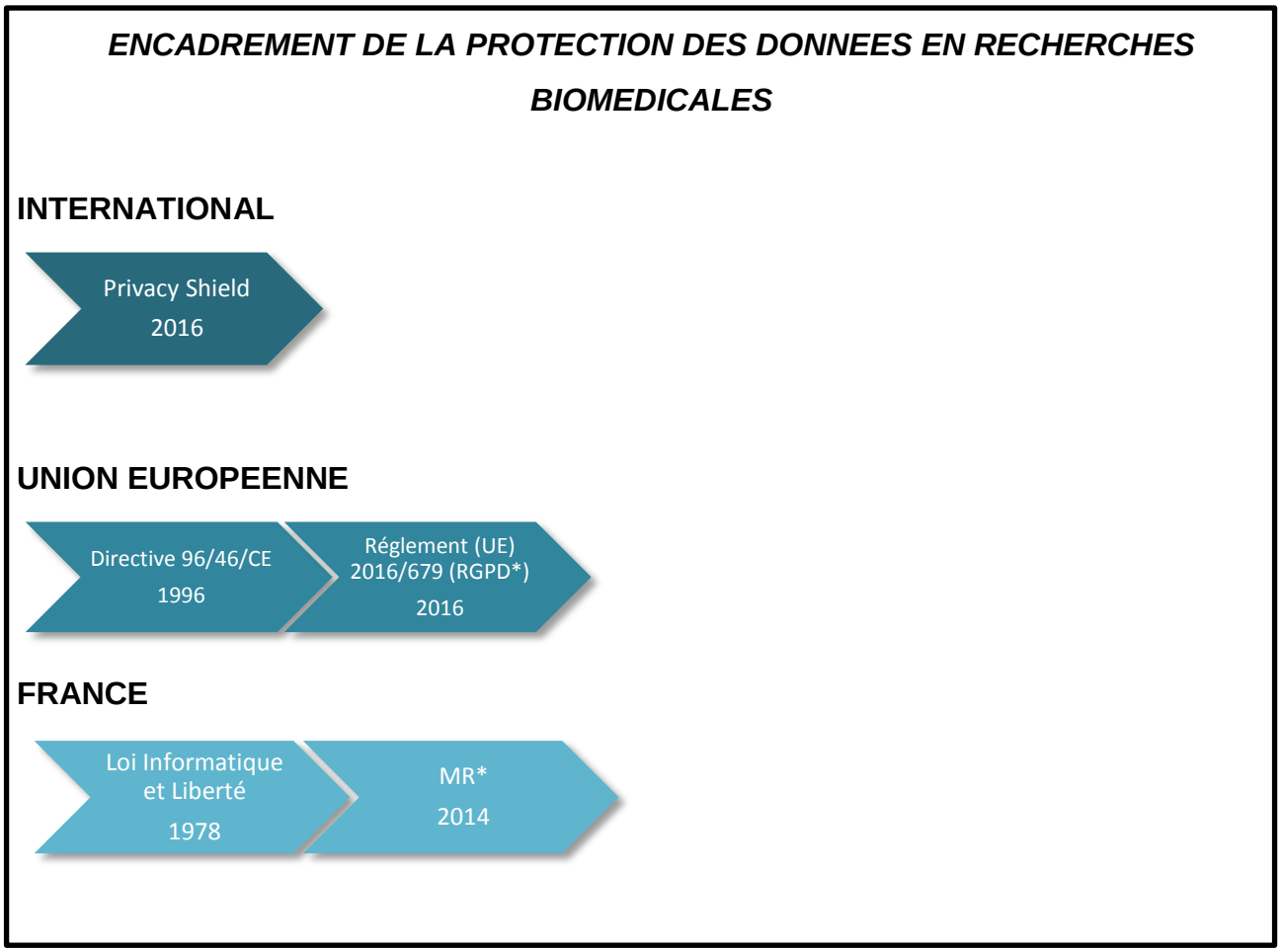


*Figure n°4 – Historique de l'encadrement de la protection des données.*

## C. Encadrement général.

Les recherches cliniques sont donc réglementées par deux bases légales : le consentement lié à la participation à l'étude et le consentement lié à la protection des données. En effet, il est notable que la loi JARDE s'accorde à orienter la protection des données dans le cadre des RIPH*. On observe également que la loi JARDE et le RGPD* s'entendent sur un souhait de s'orienter vers une documentation de conformité et une réduction des contraintes déclaratives, tout en maintenant une protection optimale des participants.

Le RGPD* présente certes de nombreux avantages, mais n'est, à ce jour, pas adapté au domaine de la santé, ce qui amène à de nombreuses questions autour de sa mise en pratique. De plus, le RGPD* a laissé aux pays membres la possibilité d'adapter plus de 50 articles. Cette liberté rend les échanges complexes créant des diversités réglementaires entre les différents pays de l'Union Européenne.

# III. OBLIGATIONS DE LA CRO*.

Il résulte de cette analyse que les évolutions historiques des réglementations, tant en matière d'essais cliniques que de protection des données personnelles, amènent les CRO* à être confrontées à des exigences strictes et denses. Plus récemment, la mise en œuvre du RGPD* a été à l'origine de grands changements en matière de protection des données personnelles mais a également soulevé de multiples questions quant à son application.

En raison de leurs pratiques et de l'enjeu commercial, les CRO* doivent impérativement attester que la démarche qu'ils mettent en place assure un respect strict de la protection des données. Il s'agit du principe de « *Privacy by Design* » (*RGPD* Chapitre IV, section 2, Article 25 – Protection des données dès la conception)* défini par le RGPD* comme la mise en place de toutes les protections nécessaires dès l'initiation de la collecte. Ces dispositions privilégient deux axes :

- Atteindre un niveau de risque négligeable de violation des données personnelles (accès, destruction, perte, altération, divulgation non autorisée, accidentelle ou illicite, de données à caractère personnel. (41)
- Assurer le respect des droits des patients (RGPD*).

La CRO* doit donc assurer la mise en place de nouvelles procédures afin de rendre licite le traitement de données, base de son activité.

## A. Sécurité.

*(RGPD* section 2)*

L'infaillibilité réglementaire est à la base de toute pratique de protection des données. Aucun traitement de données n'est possible sans un système de sécurité, principalement informatique, (mais cela englobe également l'ensemble des locaux, des archives… Tout s'inscrit dans la même logique de performance au regard de la protection des données de chaque personne). Assurer le respect de ce volet permet d'une part d'être conforme aux

recommandations de la CNIL* (réglementaires), d'autre part de se positionner dans le marché concurrentiel où la sécurité est devenue un enjeu majeur.

D'après le RGPD*, des moyens doivent être mis en place afin d'assurer « *la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement* » (*RGPD* Chapitre IV, Section 2, Article 32*). Cette attente, bien que succinctement décrite dans le RGPD* représente néanmoins un nombre non négligeable d'actions à mettre en place. La norme ISO 27 000 (Sécurité informatique) peut être utilisée comme référence dans le cadre de la sécurité informatique.

Voici une liste (non exhaustive) de certaines de ces dispositions :

- Assurer la sécurité de ses locaux par le moyen d'alarmes-incendies et d'alarmes anti-intrusion, notamment dans les lieux de stockage de données sous leurs différents supports (serveurs, papiers etc.).
- Garantir sa « *compliance* » (mise en conformité) technique et organisationnelle aux mesures de sécurité liées à la protection des données, entre autres :
    - Gestion des violations (*RGPD* Chapitre IV, section 2, Article 33 et 34*)
    - Gestion des incidents
    - Contrôle des accès
    - Contrôle de disponibilité des données
    - Contrôle des transferts
    - Récupération des données

Ces différents points de sécurité doivent être démontrés en cas d'audit (de la CNIL* ou du client par exemple). En d'autres termes, le niveau de sécurité attendu implique que chaque CRO* dispose des outils actualisés permettant d'assurer le verrouillage attendu et de documents écrits et à jour conformes aux recommandations de gestion documentaire de l'ISO 9001, décrivant l'ensemble des processus mis en place.

Afin d'assurer une logique dans la mise en place de l'ensemble des mesures de sécurité, la CRO* doit former ses collaborateurs à la protection des données au sens large mais également aux spécificités des études sur lesquelles ils interviennent (modalités de transferts, analyses statistiques autorisées etc.). Ces formations doivent également être tracées. La sensibilisation/formation aux pratiques de protection des données est un point

clé de la mise en place de bonnes pratiques en ce sens. Les prestataires et sous-traitants des CRO* ont un rôle tout aussi indispensable dans la sécurisation et la gestion des traitements de données. Néanmoins les CRO* ne peuvent pas assurer la formation de toutes des parties prenantes. Il arrive ainsi que des violations soient constatées en raison d'un manquement d'information ou de vigilance.

Les CRO* n'ont théoriquement aucun accès aux données nominatives de patients, il arrive pourtant fréquemment qu'elles soient confrontées à des réceptions de ce type de données (copie des consentements, dossiers médicaux, e-mail provenant d'un investigateur* contenant une information nominative). La CRO* doit théoriquement déclarer toute action sortant du cadre de la réglementation à la CNIL*. Bien que le nombre de déclarations de violation à la CNIL* ait été démultiplié depuis la mise en application du RGPD*, la totalité des violations ne peut pas être déclarée ; toutes les violations ne sont pas connues, certaines sont minimes (aucun risque n'est encouru). La difficulté résulte donc dans la prise de décision de notifier ou non une violation à la CNIL*.

## B. Data Protection Officer.

*(RGPD* Chapitre IV, Section 4, Article 37)*

Le RGPD* impose désormais à toutes les CRO* de nommer un DPO* (Data Protection Officer – Délégué à la Protection des Données). Le RGPD* définit le rôle du DPO* en trois fonctions :

- Informer et conseiller les entreprises et leurs employés afin d'assurer le respect du RGPD*.
- Conseiller et vérifier l'exécution des AIPD* (Analyse d'Impact Relative à la Protection des Données).
- Coopérer et être le point de contact avec l'autorité de contrôle (en France, la CNIL*). L'entreprise a une obligation de coopération avec l'autorité de contrôle (*RGPD* Chapitre IV, section 2, Article 31)*.

Chaque CRO* doit déclarer un DPO* auprès de la CNIL*. Celui-ci sera considéré comme un référent dans la mise en place du RGPD* ; dans l'entreprise, son positionnement est transversal. De par ses fonctions, le DPO* ne peut être totalement dépendant du système

hiérarchique mis en place par sa direction : il doit et peut déterminer de manière autonome ses actions en fonction des besoins réglementaires dont il est le garant. Pour autant, en cas d'infraction, c'est bien l'entreprise qui assumera la responsabilité pénale des failles de son dispositif, proportionnellement à son rôle (responsable de traitement/sous-traitant). Le DPO* n'encourt aucune poursuite ni personnelle ni professionnelle en cas de non-respect de la réglementation par son entreprise. Bien que le ressenti de l'entreprise soit subjectif et propre à chacune concernant l'imputation de la responsabilité d'une faute, l'entreprise n'est pas en droit de sanctionner le DPO*.

Le DPO* est également le point de contact dans les cas de signalement d'une violation ou de demande d'exercice d'un droit.

La complexité réside ici dans le profil du DPO*. La personne DPO* doit avoir de très solides connaissances dans différents domaines (droit, informatique, recherche clinique, fonctionnement interne, gestion des ressources humaines). Il est pourtant rare, voire impossible, de trouver une personne disposant de l'ensemble de ces connaissances. C'est pourquoi, bien que le DPO* soit nommé auprès de la CNIL* comme une personne unique, cette fonction peut être confiée à une équipe polyvalente, intégrant des représentants des différents domaines de compétences impliqués dans la gestion à sécuriser. Le DPO* peut également être externalisé. Il existe aujourd'hui de plus en plus d'entreprises proposant ce type de prestation.

### C. Contrat CRO*/Client.

Afin de définir un cadre strict en matière de protection des données, un contrat doit être signé entre la CRO* et le client (le promoteur*). Ce contrat, ou à défaut, cet avenant, devra préciser les obligations des deux parties en matière de protection des données, dans le respect du cadre réglementaire (RGPD* et autres lois applicables) et des exigences des parties. L'Association Française des CRO* travaille en ce moment même sur la rédaction d'un avenant type reprenant le contenu de la partie protection des données du contrat.

Dans le cadre de ce mémoire, j'ai souhaité rédiger une check-list présentée dans la partie **IV. CHECK-LIST.**

## D. Définition des rôles.

*(RGPD* Chapitre IV, Section1)*

Le RGPD* inclut deux acteurs dans les traitements de données : le responsable de traitement et les sous-traitants. Ces rôles sont ainsi définis :

- Le responsable de traitement est la personne ou l'organisme qui détermine les finalités et les moyens de traitement des données.
- Le sous-traitant est une personne qui assure le traitement et met en œuvre les outils d'analyse des données personnelles pour le compte du responsable de traitement.

La différenciation de ces acteurs est indispensable. En effet, les responsabilités légales sont bien plus importantes pour un responsable de traitement. Il doit répondre des mesures prises pour garantir que l'ensemble des personnes ayant accès aux données ne les traitent que dans le cadre de ses instructions. Il est donc important de définir les rôles avant tout contrat.

Dans le cas des recherches cliniques menées par une CRO*, le responsable de traitement est le promoteur* de l'étude, tandis que la CRO*, comme le centre d'investigation*, est considérée comme sous-traitante.

La distinction de ces acteurs reste néanmoins ambivalente pour d'autres pays. Par exemple : l'Espagne désigne le promoteur* et le centre d'investigation* comme co-responsable de traitement. Cette distinction a un impact important sur la répartition des responsabilités. De plus, les distinctions d'un pays ne sont pas toujours connues par les autres ce qui crée des difficultés dans le cas d'études réalisées sur plusieurs pays.

## E. Sous-traitants.

*(RGPD* Chapitre IV, section 2, Article 28)*

Bien que la CRO* soit sous-traitante dans le cadre d'une recherche clinique, elle reste responsable des sous-traitants qu'elle-même emploie. Parmi eux, la CRO* peut, selon ses besoins, sous-traiter avec des sociétés d'hébergement, utiliser des logiciels divers, des sites d'investigation*, recourir à des prestataires informatiques mais également sous-traiter des pratiques comme le monitoring (par un attaché de recherche clinique freelance) ou

engager un prestataire en pharmacovigilance. En premier lieu le responsable de traitement doit connaître la liste des sous-traitants avec lesquels la CRO* travaille. Il pourra alors s'il le souhaite, exprimer des réserves au regard de prestataires proposés. Ensuite, la CRO* doit s'assurer du respect des principes du RGPD* par ses sous-traitants par différents moyens (signature d'un contrat de conformité à la réglementation, audit du sous-traitant) en fonction des prestations réalisées.

En outre, le contrat signé entre la CRO* et son sous-traitant doit préciser les responsabilités de chacun dans le cadre de la gestion des violations de données personnelles, de la gestion des réclamations des patients ou encore de la gestion des incidents. Les obligations en termes de sécurité de stockage ou de transferts doivent être précisées et respectées. En cas de transfert de données hors de l'Union Européenne, la CRO* doit obtenir l'accord du promoteur* de l'étude. Elle devra assurer que toutes les mesures assurant la conformité au RGPD* sont mises en place lors du traitement des données concernées.

Cette étape est importante car en cas de dysfonctionnement chez un sous-traitant, la responsabilité de la CRO* serait également engagée.

## F. Attestation de conformité.

La création des méthodologies de référence par la CNIL* en 2016, « *vise à créer un cadre protecteur des personnes concernées favorable à la recherche, à l'innovation et la compétitivité* ». [(42)] En effet, elles permettent aux CRO* de se déclarer conformes à des méthodologies auprès de la CNIL*. Ainsi, lorsqu'une étude est réalisée conformément à ces méthodologies, la demande d'autorisation auprès de la CNIL* n'est plus nécessaire. L'objectif est d'une part de simplifier les démarches de déclaration de conformité, d'autre part, en lien avec les valeurs du RGPD*, de responsabiliser les acteurs.

Dans le cas de RIPH*, les CRO* doivent se déclarer conformes aux MR*-001 et MR*-003.

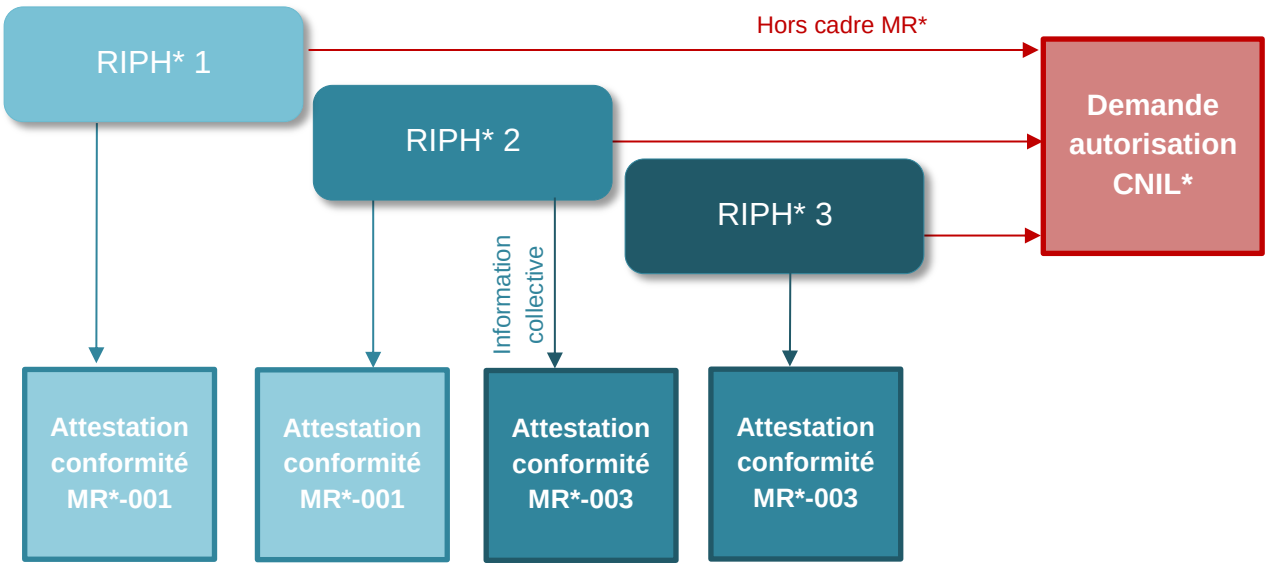


*Figure n°5 – Conformité des recherches impliquant la personne humaine.*

Lorsqu'une étude est préparée, la CRO* doit s'assurer de sa conformité avec l'une ou l'autre des méthodologies de référence, au regard de la finalité de l'étude et des moyens mis en œuvre pour y arriver. Si l'étude présente des spécificités, ne la rendant pas conforme à une méthodologie de référence, une demande d'autorisation doit être déposée à la CNIL* : on parle alors de coopération avec l'autorité de contrôle.

## G. Pseudonymisation.

Aujourd'hui, l'anonymisation totale des données est quasi inexistante en raison de la prise en considération des données dites indirectement identifiables. La pseudonymisation est un concept d'anonymisation partielle des données. Afin de protéger les participants aux études cliniques un processus de pseudonymisation doit être mis en place. Les patients inclus dans une étude, se voient attribuer un pseudonyme (en général un numéro). Lorsque les médecins investigateurs* renseignent les données des patients sur papier (CRF*) ou via un logiciel informatique (eCRF* - Electronic CRF*), seul leur numéro est indiqué. Ainsi, le médecin dispose d'un document de correspondance entre les noms et

numéros des participants : il est le seul, avec l'attaché de recherche clinique de la CRO*, à avoir accès aux données nominatives des patients de l'étude.

Aux yeux du RGPD* la pseudonymisation n'est pas considérée comme une anonymisation, elle n'exempte donc pas les CRO* des obligations liées aux données sensibles. Néanmoins, elle leur permet, d'une part, d'attester de la mise en place de dispositifs de sécurité, d'autre part, de stocker les données sur des hébergeurs n'ayant pas forcément la certification « *Hébergeur De Santé* ».

## H. Analyse d'Impact relative à la Protection des Données.

*(RGPD* Chapitre IV, Section 3, Article 35)*

Les Analyses d'Impact relative à la Protection des Données ou AIPD* doivent être réalisées dans le cas de traitement de données personnelles présentant un risque élevé pour la personne. Les données traitées par les CRO* sont des données de santé et donc sensibles par définition. Ainsi, une AIPD* est systématiquement réalisée dans le cadre d'une RIPH*.

Afin de déterminer la nécessité ou non de réaliser une analyse d'impact, la CNIL* a créé l'outil qui suit.

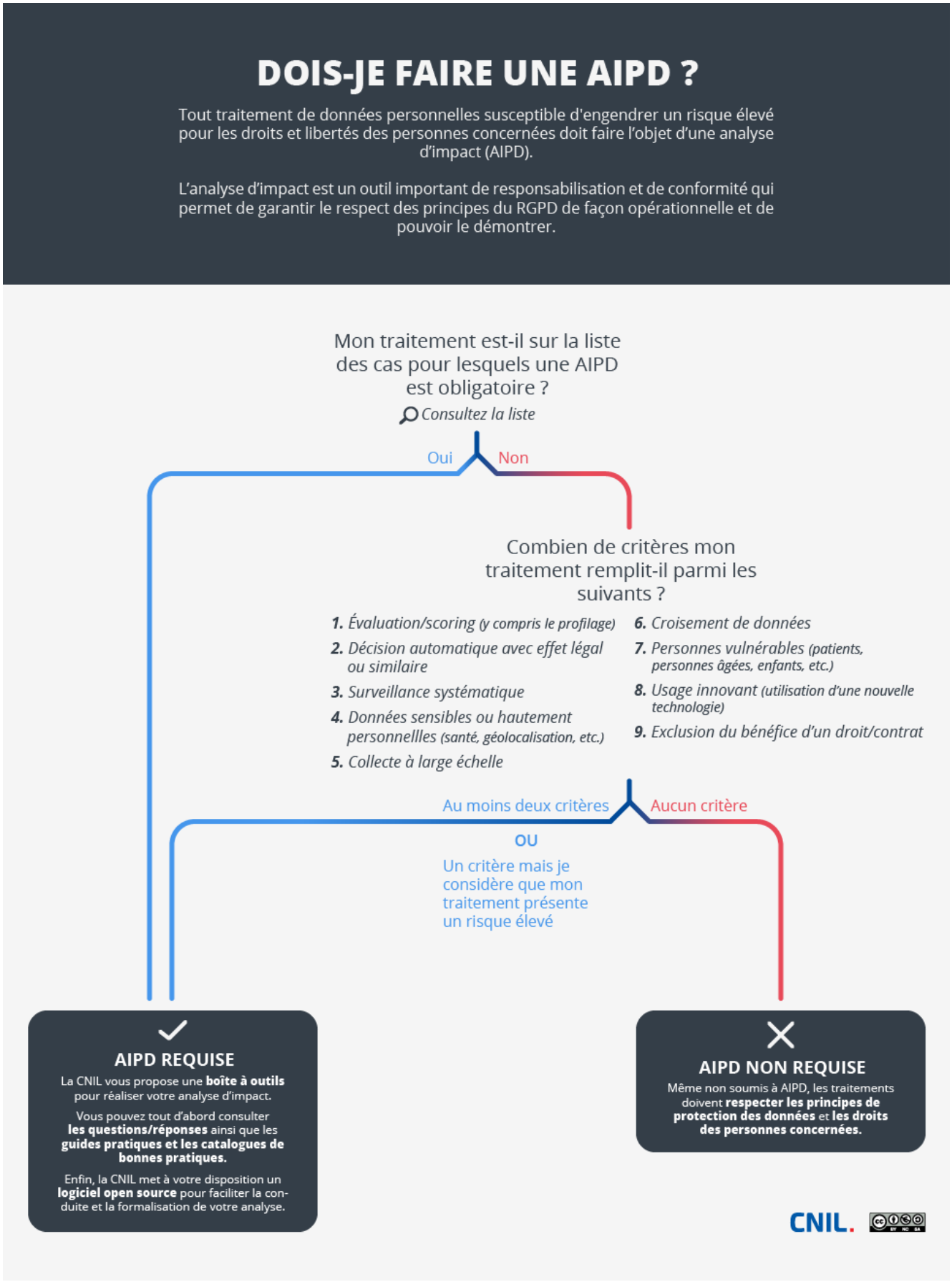


*Figure n°6 – Analyse d'Impact relative à la Protection des Données* [43]

Les CRO* exploitent quasi-systématiquement au moins deux des critères cités dans le cadre de leurs essais cliniques : « 4. *Données sensibles (…) / 5. Collecte à large échelle* ».

Le but des AIPD* est le veiller à ce que, d'une part, le traitement de données soit conforme à la réglementation, d'autre part, que l'ensemble des risques potentiels ait été pris en compte et traité. Les AIPD* permettent ainsi d'assurer la sécurité des données collectées. La CNIL* a mis en place un outil informatique gratuit appelé « *PIA : Privacy Impact Assesment* » permettant la réalisation des AIPD*.

Il appartient au DPO* de proposer une personne identifiable qui aura la charge de cette analyse d'impact.

Le cas des CRO* présente une particularité. Les AIPD* sont théoriquement menées par le responsable de traitement, néanmoins, le cas de la recherche clinique diffère des pratiques courantes. Le responsable de traitement, le promoteur* de l'étude, n'est pas, dans ce cas, le collecteur des données, il n'en a d'ailleurs, a priori, pas de copie. Ainsi, les analyses d'impact sont réalisées par les CRO*. Les CRO* transmettent ensuite leur AIPD*. au responsable de traitement, elle pourra ainsi servir de base à leur propre AIPD*.


*Figure n°7 – Capture d'écran du logiciel « PIA : Privacy Impact Assesment »*

## I. Registre.

*(RGPD* Chapitre IV, section 2, Article 30)*

Chaque traitement de données, réalisé par une entreprise, doit être renseigné dans un registre. Le registre comprend un ensemble d'informations permettant d'assurer un suivi des traitements internes et d'offrir une vision globale sur ces derniers. Bien que relativement libre dans sa forme, ce « *registre* » a donné lieu à une publication de la CNIL* qui a proposé un modèle de référence reprenant l'ensemble des informations nécessaires (Annexe n°1).

Le registre participe à la documentation de conformité. Il réunit ainsi toutes les informations relatives au traitement. C'est également un outil indispensable de pilotage, il permet ainsi de s'assurer que l'ensemble des facteurs a bien été pris en compte. De plus, le registre permet d'assurer le respect du cycle de vie des données (délai d'archivage, délai de suppression).

Le registre peut être tenu par le DPO* ou par un collaborateur qui en est chargé en interne, sous sa responsabilité.

## J. Respect des droits.

*(RGPD* Chapitre III, Section 2, 3 et 5)*

Les patients inclus dans une étude disposent de différents droits concernant leurs données :

### DROIT À LA TRANSPARENCE ET À L'INFORMATION

Le patient doit avoir connaissance de l'ensemble des informations le concernant dans l'étude à laquelle il accepte de participer. La note d'information diffère selon le type de RIPH* concerné (les détails sont précisés dans la partie **L. Information et consentement : RIPH* 1, 2 et 3** de ce document).

## DROIT D'ACCÈS

Toute personne peut demander l'accès aux informations le concernant et en demander une copie.

## DROIT DE PORTABILITÉ

Toute personne peut demander que ses données soient transférées à une autre entreprise. C'est un droit qui présente quelques risques commerciaux pour une entreprise, puisque toute personne, y compris un patient, peut transmettre ses données à qui il le souhaite, y compris à un concurrent.

## DROIT DE RECTIFICATION

Toute personne peut demander à rectifier ses données si elle les estime erronées.

## DROIT DE LIMITATION

Toute personne doit avoir l'assurance que seules les données nécessaires à la finalité déterminées sont collectées. Aucune donnée non-indispensable ne doit être collectée.

## DROIT D'OPPOSITION

Toute personne peut s'opposer au traitement de ses données ou demander l'arrêt d'un traitement (de données) en cours (retrait de consentement).

## DROIT A L'EFFACEMENT

Toute personne peut demander l'effacement de toutes les données la concernant.

## DROIT DE DÉPOSER UNE RÉCLAMATION AUPRÈS DE LA CNIL*

Toute personne dispose du droit de déposer une réclamation auprès de son autorité de contrôle (en France, la CNIL*). Chaque citoyen doit déposer sa réclamation auprès de l'autorité de contrôle de son propre pays. En cas de traitement ayant lieu dans un autre pays de l'Union Européenne, c'est le G29 (Groupe d'autorités de contrôle) qui sera en charge de la gestion de la réclamation.

Les demandes de droits doivent être exercées auprès du responsable de traitement. Celui-ci dispose d'un délai d'un mois pour y répondre. La CRO* peut être confrontée à des demandes d'exercice de droit par les patients, elle doit donc disposer d'une procédure de gestion de ces réclamations.

Le RGPD* laisse la possibilité aux responsables de traitement de refuser l'exercice d'un droit si ce refus est justifié et motivé.

*Quelques restrictions concernent la spécificité des recherches médicales.*

Le droit à l'effacement n'est pas applicable dans le cas d'un essai clinique « *si son application est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de la recherche* » (35). En effet, les études ont parfois des durées conséquentes et des rapports peuvent être rédigés de manière intermédiaire. L'effacement des données d'un patient pourrait mettre en péril le bon déroulement de l'étude. Néanmoins, le RGPD* impose aux entreprises d'indiquer l'ensemble des droits des personnes concernées. Elles devront par la suite justifier directement le refus d'exercice d'un droit auprès de la personne concernée directement.

Il appartient au responsable de traitement de procéder à l'exercice de ces droits. Le cas des études cliniques diffère des cas classiques de protection des données. En effet, dans la majorité des cas, le responsable de traitement est la personne/l'entreprise, à l'origine de la collecte des données et donc en possession de la base d'origine. Ainsi, en cas de réclamation, le responsable de traitement doit agir en conséquence et s'assurer du respect de la demande par ses sous-traitants. Néanmoins, dans le cas des études cliniques, le responsable de traitement n'est pas en possession des données.

Le RGPD*, ainsi que l'ensemble des organisations décisionnelles dans le cadre d'un essai clinique (CNIL*, Comité de Protection des Personnes) imposent au responsable de traitement d'indiquer le contact de son DPO* dans la note d'information adressée au patient. Or, la loi indique également que le responsable de traitement ne doit pas avoir connaissance de l'identité des sujets participant à l'étude.

Ainsi deux questions apparaissent (la CNIL* a répondu - appel téléphonique) :

*En cas de demande d'exercice de droit(s) provenant d'un patient, comment le responsable de traitement doit-il la gérer, étant donné qu'il ne connaît pas la correspondance de pseudonymisation ?*

> **Réponse de la CNIL*** : Lorsqu'une personne demande à exercer un droit auprès du DPO* du responsable de traitement, celui-ci doit orienter la personne vers son médecin investigateur* qui pourra alors agir en fonction de la demande. On note ici l'importance donc d'inclure un paragraphe de gestion des violations dans les contrats avec les investigateurs*.

*N'y a-t-il pas un conflit d'intérêt si le DPO* du responsable de traitement est en possession d'une information nominative ?*

> **Réponse de la CNIL* :** Le DPO* a un rôle particulier, son titre lui donne la possibilité d'avoir connaissance de données sensibles. Ainsi le DPO*, y compris dans le cas d'un promoteur* d'étude clinique, peut être en possession d'une donnée nominative. Il doit néanmoins s'assurer de détruire cette donnée (par exemple l'e-mail si la demande a eu lieu par e-mail) directement après avoir orienté la personne dans le cadre de sa demande comme précisé ci-dessus.

En cas de réclamation, la demande doit être gérée dans un délai d'un mois. Ce délai peut être allongé à deux mois à condition que le prolongement soit justifié. Une fois la demande gérée, la personne doit en être informée.

## K. Cycle de vie des données.

Les différentes étapes d'utilisation des données à caractère personnel peuvent être nommées « *cycle de vie* » de la donnée.


*Figure n°8 – Cycle de vie des données*

La phase active des données ne comprend pas de durée limite fixée par la réglementation. Des données sont considérées comme actives durant l'ensemble de la phase de traitement : une donnée est active jusqu'à atteinte de la finalité (l'objectif) faisant l'objet de la collecte.

Par la suite, une fois la finalité atteinte, les données ne sont pas immédiatement supprimées. La CNIL* a défini une durée d'archivage intermédiaire déterminée selon le type de données collectées, permettant aux entreprises de conserver les données après leur phase active. Durant l'étape d'archivage intermédiaire, les données sont conservées mais avec un accès restreint. L'archivage intermédiaire est, entre autres, nécessaire en cas de plainte déposée dans le cadre de la collecte ; il permet par ailleurs, de revenir à l'étude en cas de contestation scientifique des conclusions.

Enfin, une fois le délai d'archivage intermédiaire atteint, les données doivent être supprimées. Le RGPD* définit l'archivage définitif comme la suppression/destruction irrémédiable des données.

Dans le cas des études cliniques, la question de durée de conservation des données est complexe. La CNIL* a déterminé de manière précise les durées de conservation de données pour différents cas :

- Les Curriculum Vitae peuvent être conservés jusqu'à deux ans après le dernier contact avec la personne concernée
- Les données de ressources humaines peuvent être conservées jusqu'à cinq ans après le départ de l'entreprise avec la personne concernée.

Pourtant, pour la recherche clinique, le référentiel établi par la CNIL* spécifie que les données doivent être supprimées par la CRO* immédiatement après l'atteinte de la finalité de l'étude. Les CRO* doivent donc renvoyer leurs données au responsable de traitement et les supprimer définitivement de leur côté. Cette pratique est actuellement problématique car les CRO* sont confrontées à des pratiques récurrentes : il arrive régulièrement que les promoteurs* se retournent vers la CRO* afin d'obtenir une copie des données bien que le traitement soit terminé.

Aussi, afin d'assurer la conformité de la CRO* sur ce sujet, les spécificités d'archivage et la suppression des données doivent être déterminées en amont dans le contrat entre les parties.

## L. Information et consentement : RIPH* 1, 2 et 3.

Le RGPD* précise que toute collecte de données, hormis les collectes d'intérêt public ou judiciaire, doit faire l'objet préalable d'une note d'information et d'un consentement exprès. Pourtant, la loi française indique des spécificités selon les RIPH*. Les essais cliniques sont soumis à deux verrous légaux : le consentement à la recherche, qui doit suivre la prise de connaissance des informations liées à la recherche (l'article L. 1122-1 du Code de la santé publique précise les informations à fournir concernant l'étude), et le consentement au traitement des données, qui doit suivre la prise de connaissance des informations spécifiques du traitement des données. **Ici la description est faite uniquement dans le cadre de la protection des données.**

### a. Information des personnes :

L'information doit être fournie à la personne directement. Dans le cas d'un patient mineur, chacun des titulaires de l'autorité parentale devra en prendre connaissance. Dans le cas d'un patient majeur inapte (protégé ou hors d'état de recevoir ces informations, elles seront fournies au représentant légal ou à défaut, à la personne de confiance.

**Pour les RIPH* 1, 2 et 3 :**
Les informations doivent être données **individuellement** et par **écrit**.
Dans certains cas de RIPH* de catégorie 2, les informations et le consentement ne peuvent pas être donnés individuellement. Les informations sont donc données collectivement et les personnes concernées peuvent faire valoir leur droit d'opposition.

Quel que soit le cas, les informations suivantes doivent être fournies :

- Une information générale sur les activités de recherche de l'établissement d'investigation*.
- Une information sur l'étude auquel le patient participe.

*A ces informations s'ajoutent l'ensemble des obligations de l'article 13 du RGPD* :*

- Base réglementaire (légitimité)
- Identité et coordonnées du responsable de traitement
- Coordonnées du DPO* du responsable de traitement
- Identité et coordonnées de l'investigateur* principal
- Catégories de données à caractère personnel concernées
- Finalité de traitement (objectif de l'étude)
- Destinataires ou catégories de destinataires des données à caractère personnel
- Si applicable : transfert de données vers un pays tiers (non inclus dans l'Union Européenne)
- Durée de conservation ou critères utilisés pour déterminer cette durée
- Existence des droits (accès, portabilité, rectification, limitation, opposition, effacement et droit d'introduire une réclamation à une autorité de contrôle)
- Modalités d'exercices de ces droits

- Si applicable, la personne doit être informée de son inscription au fichier national des personnes qui se prêtent à des recherches.
- Dans le cas où les données ne seraient pas collectées directement auprès de la personne concernée, la source d'où proviennent les données (article 14 RGPD*)

Il est à noter que dans le cadre d'un questionnaire remis à la personne se prêtant à la recherche, ces informations doivent également être présentes.

### b. Consentement :

**RIPH* 1 et RIPH* 2 :** Le consentement doit être écrit, libre et éclairé.

**RIPH* 3 :** Le consentement dans le cadre de la MR*-003 n'est pas demandé. On parle ici de non-opposition du patient. Néanmoins, certaines CRO* tendent à faire signer un document de non-opposition afin de pouvoir attester de la licéité de leur traitement.

**RIPH* 2** avec information collective : la non opposition suffit.

## M. Bilan des obligations.

- ✓ **Assurer la sécurité technique et organisationnelle**
- ✓ **Désigner un DPO***
- ✓ Adaptation du contrat avec le promoteur*
- ✓ Faire une AIPD*
- ✓ Définir les rôles (responsable de traitement / sous-traitants)
- ✓ Créer une fiche de registre
- ✓ Assurer la conformité des sous-traitants
- ✓ Attester et/ou vérifier sa conformité à la méthodologie de référence concernée / déclaration CNIL*
- ✓ Assurer la pseudonymisation des données
- ✓ Assurer le respect des droits des patients
- ✓ Assurer le respect du cycle de vie de la donnée
- ✓ Information et consentement
  - Conformité du type de consentement
  - Conformité de la note d'information

*Tableau n°2 – Liste des vérifications à effectuer pour la mise en place d'une étude clinique.*

# IV. CHECK-LIST.

Dans le cadre de ce mémoire l'objectif est de présenter une synthèse des mesures de protection des données attendues de la part des CRO*. Deux outils ont été retenus pour éclairer les pratiques :

- La check-list n°1 présente l'ensemble des points à définir dans les contrats signés entre les promoteurs* d'études cliniques et les CRO* en matière de protection des données.

- La check-list n°2 présente quant à elle, la sécurité et les obligations dont la présence doit être assurée par les CRO* pour chaque RIPH*.

## CHECK-LIST n°1 – CONTRAT CRO/PROMOTEUR

☐ Définition des responsabilités (promoteur responsable de traitement / CRO sous-traitante).

☐ Nature des opérations de traitement.

☐ Finalité(s) de traitement.

☐ Types de données traitées.

☐ Catégories de personnes concernées.

**Engagement de la CRO**

☐ Respecter des seules finalités faisant l'objet de la sous-traitance.

Respecter :

- ☐ Le règlement (UE) 2016/679 (RGPD)
- ☐ Les lois françaises en vigueur
- ☐ Les exigences du responsable de traitement

☐ Garantir la confidentialité des données à caractère personnel.

☐ Former les personnes autorisées à traiter les données au respect de la confidentialité et aux modalités de traitement.

☐ Assurer la limitation d'accès et de traitement des données par les seules personnes autorisées.

Aider le responsable de traitement.

- ☐ À réaliser les analyses d'impact liées à la protection des données.
- ☐ À échanger avec l'autorité de contrôle.
- ☐ À répondre aux réclamations (exercice de droits).

☐ Prévenir le responsable de traitement en cas d'audit de la CRO par une autorité de contrôle.

☐ Assurer le respect des exigences de protection des données par ses sous-traitants et la présence de garanties suffisantes (par contrat).

☐ Engager sa responsabilité en cas de défaillance d'un sous-traitant.

☐ Informer le responsable de traitement dans les 24h en cas de violation et définir les modalités d'intervention.

☐ Renvoyer tous les documents liés à l'étude au responsable de traitement à l'aboutissement de celle-ci.

☐ Archiver et supprimer les données conformément au cadre légal sauf spécificité contractuelle.

☐ Documenter le cadre de protection des données personnelles et mettre sa documentation à disposition du responsable de traitement et des autorités de contrôle.

☐ Garantir sa compliance technique et organisationnelle aux mesures de sécurité liées à la protection des données (violations, contrôle d'accès, contrôle de disponibilité des données, surveillance des lectures, contrôle des transferts etc.).

☐ Assurer les garanties de protection des données nécessaires en cas de transfert hors de l'UE prédéfinies avec le responsable de traitement.

**Engagement du responsable de traitement**

☐ Documenter de façon explicite les exigences liées à la protection des données personnelles.

☐ Désigner un Délégué à la Protection des Données.

☐ Donner suite aux demandes d'exercice de droits.

☐ Informer les autorités nationales et les personnes concernées en cas de violation si applicable *(le signalement des violations aux personnes concernées est fonction de la gravité de la violation)*

☐ Réaliser un audit chez le sous-traitant si nécessaire.

***Glossaire*** *:*

***CRO*** *: Contract Research Organization*
***RGPD*** *: Règlement Général sur la Protection des Données*

2/2

## CHECK-LIST n°2 – OBLIGATIONS DE LA CRO

*Dans le cadre d'une RIPH 1, RIPH 2 ou RIPH 3*

### Généralités sur la CRO.

☐ La sécurité des locaux est assurée (alarme anti-intrusion / anti-incendie).

*La sécurité informatique est assurée :*

- ☐ Si applicable, la CRO a assuré le respect du RGPD par son/ses prestataire(s) Informatique(s) (maintenance, hébergement etc.).
- ☐ La CRO dispose d'une procédure de sécurité informatique.
- ☐ La CRO a documenté l'ensemble des moyens informatiques mis en place pour assurer le respect de protection des données personnelles.
- ☐ Le personnel est formé à la documentation des mesures précitées.

☐ La CRO dispose d'un DPO.

☐ Le personnel a été formé aux obligations de confidentialité au regard des données personnelles traitées.

☐ La CRO s'assure de la pseudonymisation des données / aucune donnée nominative ne sera en sa possession.

☐ Une déclaration de conformité à la méthodologie de référence correspondante a été effectuée auprès de la CNIL.
- ☐ A défaut, une demande d'autorisation a été déposée à la CNIL

☐ La conformité à la méthodologie de référence concernée est documentée et à jour.

☐ Une AIPD a été réalisée et ne présente pas de risques pour le patient.
- ☐ A défaut l'accord de la CNIL a été obtenu.

☐ La CRO dispose de procédure(s) attestant sa conformité (gestion des réclamations, gestion des violations, sécurité informatique).

### Gestion des contrats et des sous-traitants

☐ Le contrat entre la CRO et le promoteur est conforme à la Check-list n°1.

☐ Les contrats avec les sous-traitants comprennent un paragraphe RGPD imposant les obligations de chaque partie.

☐ La CRO s'est assurée de la conformité de ses sous-traitants au RGPD.

☐ Le responsable de traitement a été informé de la liste des sous-traitants dans le cadre de l'étude et ne s'y est pas opposé.

**Information et consentement**

☐ La note d'information est conforme aux recommandations de la MR applicable

A défaut, la note d'information contient les recommandations :

- ☐ De l'article L. 1122-1 du code de la santé publique
- ☐ De l'article 13 du RGPD* (ou 14 si les données ne sont pas collectées directement auprès de la personne).

☐ Dans le cadre d'une étude conforme à la MR-001, les modalités de recueil de consentement exprès ou écrite ont été mises en place.

**Après la première inclusion**

☐ Une fiche de registre a été créée.

☐ La CRO gère l'archivage et la suppression des données en fonction des durées de conservation prédéterminées pour l'étude.

***Glossaire*** *:*

***AIPD :*** *Analyse d'Impact relative à la Protection des données*
***CRO*** *: Contract Research Organization*
***RGPD*** *: Règlement Général sur la Protection des Données*
***DPO*** *: Data Protection Officer / Délégué à la Protection des Données*
***CNIL*** *: Commission Nationale de l'Informatique et des libertés*
***MR*** *: Méthodologie(s) de référence*
***RIPH*** *: Recherche Impliquant la Personne Humaine*
***UE*** *: Union Européenne*

# CONCLUSION.

Interférant dans les rouages complexes que constitue la recherche clinique, les évolutions réglementaires pèsent sur la vie des entreprises. Le RGPD*, s'ajoutant aux méthodologies de référence et aux lois nationales déjà rigoureuses, a imposé de multiples contraintes à la réalisation des études cliniques. On peut observer leur évolution permanente : lorsqu'une étude clinique débute, plusieurs années, quelquefois, seront nécessaires avant de parvenir à des conclusions significatives. Ainsi, les ressorts vitaux des intérêts commerciaux propres à la survie de toute entreprise peuvent être contrariés par l'apparition de conditions nouvelles.

Du RGPD* émane diverses problématiques dont les conséquences peuvent être lourdes : la CNIL* peut venir auditer toutes les entreprises quand elle le souhaite et les conséquences financières en cas de non-conformité peuvent être désastreuses (jusqu'à 4% du chiffre d'affaire ou 20 millions d'euros de sanction). La conformité des CRO* est capitale pour leur existence même. Le principe du « *Privacy By Design* » (protection dès la conception) doit donc être respecté et appliqué, au plus proche du cadre réglementaire.

Ben qu'étant un pilier de l'harmonisation des pratiques au sein de l'Union Européenne, le RGPD*, depuis sa récente application, génère quelques interprétations encore divergentes au sein des pays membres. Un travail d'harmonisation des pratiques semble donc à poursuivre.

Ce mémoire présente un inventaire non exhaustif des exigences imposées aux CRO* dans un cadre défini. Deux outils sous forme de check-list synthétisant les obligations des CRO* dans l'environnement réglementé des recherches impliquant la personne humaine y sont proposés. Ces check-lists restent pourtant bornées aux obligations liées aux données de patients. Les CRO* mènent de nombreuses recherches impliquant ou non la personne humaine, incluant entre autres des données personnelles de patients mais aussi de médecins investigateurs*, de personnel administratif des différents clients et sous-traitants. Ce travail ne présente donc qu'une partie des obligations encadrant la protection des données mais soulève déjà de nombreuses questions sur sa mise en application.

Depuis peu L'Association Française des CRO* et l'Association Européenne des CRO* travaillent sur un projet de « *code of conduct* » (code de conduite) en matière de protection des données en recherche clinique. Ce travail fait suite aux nombreux questionnements dus à la mise en application du RGPD* et permettra d'offrir un référentiel commun à l'ensemble des CRO* européennes.

Enfin, tout au long de ce travail, l'inventaire des recommandations relatives aux citoyens, la qualification du niveau de « sensibilité » des informations qui sont recueillies, demandées, traitées, conduit, au-delà de la perspective du dossier limité à la recherche clinique, à s'interroger sur ce citoyen que l'Union Européenne met au centre de sa législation : la question globale de la protection de nos données de santé fait écho aux risques potentiels encourus.

PMSI* (Projet de Médicalisation du Système Informatique), Dossier Médical Partagé, e-Santé, les données de santé représentent aujourd'hui un outil politique mais également commercial de plus en plus privatisé et convoité. De nombreux secteurs s'intéressent aux données de santé, considérées comme le nouvel eldorado du secteur de la donnée. (44) Mais l'utilisation commerciale croissante des données de santé crée également un marché noir grandissant dans ce domaine : elles représentent aujourd'hui le type de données le plus vendu et le plus cher sur le « *Darknet* » (marché noir). (45)

Alors peut-on raisonnablement faire rimer informatisation des données et sécurité ? La ville de BALTIMORE (Etats-Unis) est depuis quelques semaines, le théâtre d'un piratage de masse paralysant toute utilisation des services informatiques de la mégalopole. (46) Les hackers, pour le moment incoercibles, semblent utiliser un outil créé par la NSA (National Security Agency – *Agence de sécurité Nationale*) elle-même. Si les outils créés et contrôlés par l'agence sensée la plus experte en matière de sécurité informatique, peuvent être détournés, dans quelle mesure les évolutions réglementaires, les obligations et le niveau de la sécurité informatique seront-ils capables de protéger les citoyens en résistant aux actes de malveillance dans notre univers du « *tout informatisé* » ?

# BIBLIOGRAPHIE.


**1. K. DOUPLITZKY.** *Guide pratique de l'internet: pratiquer et comprendre* - pp. 20 - 29. Edition ODILE JACOB, 2001.

**2.** M. **LEINER et al.** *Un bref historique de l'internet.* InternetSociety. [En ligne] 1997. [Consulté : 05/03/2019.] https://www.internetsociety.org/fr/internet/history-internet/brief-history-internet/.

**3. D. GENELOT.** *Manager dans la complexité.* Edition BROCHE, 2017.

**4**. **RIEFFEL, R.** *Révolution numérique, révolution culturelle ? .* s.l. : GALLIMARD, 2014.

**5.** *Cambridge Analytica : 87 millions de comptes Facebook concernés.* **LeMonde.** 2018.

**6.** *Comment la reconnaissance faciale s'immisce dans la vie des chinois ?* **LesEchos.** 2018.

**7. Parlement Européen.** *Règlement (UE) 2016/679 (RGPD)***.** 2016**.**

**8. P. JAILLON et J.P. DEMAREZ.** *L'histoire de la genèse de la loi Huriet-Sérusclat de décembre 1988*. Med SCI (Paris), Volume 24, Number 3. 15 mars 2008, pp. 323 - 317.

**9. Ministère de la santé, France.** *Loi 88-1138 HURIET, 1988.*

**10. Ministère de la santé, France.** *Loi 2012-300 JARDE,* 2012.

**11. Ministère de la santé, France.** *Code de la Santé Publique,* 1953.

**12. F. LEMAIRE et M. MATEI, M.** *De la loi Huriet à la loi Jardé.* SRLF et Springer-Verlag France, 17 mai 2012. pp. 4 - 5.

**13.***Définition biomédical(e).* **Larousse**. [En ligne] 2018. [Consulté : 16/01/2019.] https://www.larousse.fr/dictionnaires/francais/biom%C3%A9dical_biom%C3%A9dicale_biom%C3%A9dicaux/9444.

**14.** *Qu-est ce qu'un essai clinique ?* **ANSMSanté.** [En ligne] 2017. [Consulté : 16/01/2019.] https://www.ansm.sante.fr/Activites/Essais-cliniques/Qu-est-ce-qu-un-essai-clinique/(offset)/1.

**15.** *Comprendre la recherche clinique.* **Inserm.** [En ligne] 2016. [Consulté : 16/01/2019.] https://www.inserm.fr/recherche-inserm/recherche-clinique/comprendre-recherche-clinique.

**16. A. YAVCHITZ et C. DAOUI.** *Réglementation des études cliniques*. 2018.

**17.** *Développement et suivi des médicalements.* **Pharmacomedicale**. [En ligne] 2019. [Consulté : 27/05/2019.] https://pharmacomedicale.org/pharmacologie/developpement-et-suivi-des-medicaments/28-essais-cliniques-chez-l-homme.

**18. *EUCROF.*** [En ligne] 2005. [Consulté : 31/05/2019.] https://www.eucrof.eu.

**19. *AFCRO***. [En ligne] 2002. [Consulté : 31/05/2019.] https://www.afcros.com.

**20.** *A history of: Contract Research Organisations (CROs)*. **Pharmaphonun**. [En ligne] 2010. [Consulté : 31/05/2019.] https://pharmaphorum.com/views-and-analysis/a_history_of_contract_research_organisations_cros/.

**21.** *Comité de protection des personnes.* **ARS.santé.** [En ligne] 2017. [Consulté : 31/05/2019.] https://www.ars.sante.fr/comite-de-protection-des-personnes-1.

**22. Parlement Européen,** *Recommandation on the content of the Trial Master File and archiving,* 2016.

**23. A. CAROL.** *La recherche biomédicale - Droit, Histoire, Médecine.* 2005. p. 20 à 35.

**24. B. PITCHO et V. DESPAT-SEBAG.** *Médecine et droits de l'homme : Pratiques soignantes et recherche biomédicale-Textes fondamentaux depuis 1948.* Edition VUIBERT, 2008.

***25.*** **AMM.** *Declaration d'HELSINKI.* 1964.

**26. AMM.** *Déclaration de TOKYO.* 1975.

**27. *OMS, CIOMS.*** *Déclaration de MANILLE.* 1981.

**28. ICH,** *Les bonnes pratiques cliniques.* 1990**.**

**29. Parlement Européen**. *Directive 2001/20/CE.* 2001.

**30. Ministère de la santé, France.** *Loi santé publique*. 2004.

**31. Ministère de la santé, France.***Loi bioéthique.* 2004**.**

**32. Parlement Européenne.** *Règlement (UE) n°536/2014***.** 2016**.**

**33.** *Donnée personnelle.* **CNIL.** [En ligne] 2018. [Consulté : 16/01/2019.] https://www.cnil.fr/fr/definition/donnee-personnelle.

**34.** *"Safari" ou la chasse aux Français.* **LeMonde,** 1974.

**35. CNIL.** *Méthodologie de référence 001***.** 2016**.**

**36. CNIL.** *Méthodologie de référence 002***.** 2015**.**

**37. CNIL.** *Méthodologie de référence 003.* 2016**.**

**38. CNIL.** *Méthodologie de référence 004.* 2018**.**

**39. CNIL.** *Méthodologie de référence 005.* 2018**.**

**40. CNIL.** *Méthodologie de référence 006.* 2018**.**

**41.** *Violation de données.* **CNPD.public.** [En ligne] 2018. [Consulté : 01/05/2019.] https://cnpd.public.lu/fr/professionnels/obligations/violation-de-donnees/violation-donnees-rgpd.html.

**42.** *Recherches dans le domaine de la santé : la CNIL adopte de nouvelles mesures de simplification.* **CNIL.** [En ligne] 2018. [Consulté : 01/05/2019.] https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-la-cnil-adopte-de-nouvelles-mesures-de-simplification.

**43.** *Analyse d'Impact Relative à la Protection des Données.* **CNIL.** [En ligne] 2018. [Consulté : 01/05/2019.] https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour.

**44.** *Les données de santé, nouvel Eldorado de l'économie des données privées ?* **Archinfo.** [En ligne] 2017. [Consulté : 10/02/2019.] https://archinfo24.hypotheses.org/3669.

**45.** *Dark Web : combien coûtent vos données sur le marché.* **LebigData.** [En ligne] 2018. [Consulté : 10/02/2019.] https://www.lebigdata.fr/dark-web-cout-donnees.

**46.** *Baltimore : une ville paralysée par les hackers.* **LCI.** 2019**.**

**Référence photo de couverture :**

**Photo libre de droit**, https://pixabay.com/fr/photos/ordinateur-s%C3%A9curit%C3%A9-cadenas-pirate-1591018/

# TABLE DES ANNEXES.

*ANNEXE n°1 - Fiche de registre de traitement de données personnelles.*

## Fiche de registre ref-000

| Description du traitement | |
|---|---|
| Nom / sigle | |
| N° / REF | ref-000 |
| Date de création | |
| Mise à jour | |

| Acteurs | Nom | Adresse | CP | Ville | Pays | Tel |
|---|---|---|---|---|---|---|
| Responsable du traitement | | | | | | |
| Délégué à la protection des données | | | | | | |
| Représentant | | | | | | |
| Responsable(s) conjoint(s) | | | | | | |

| Finalité(s) du traitement effectué | |
|---|---|
| Finalité principale | |
| Sous-finalité 1 | |
| Sous-finalité 2 | |
| Sous-finalité 3 | |
| Sous-finalité 4 | |
| Sous-finalité 5 | |

| Mesures de sécurité | |
|---|---|
| Mesures de sécurité techniques | |
| Mesures de sécurité organisationnelles | |

| Catégories de données personnelles concernées | Description | Délai d'effacement |
|---|---|---|
| Etat civil, identité, données d'identification, images... | | |
| Vie personnelle (habitudes de vie, situation familiale, etc.) | | |
| Informations d'ordre économique et financier (revenus, situation financière, situation | | |
| Données de connexion (adress IP, logs, etc.) | | |
| Données de localisation (déplacements, données GPS, GSM, etc.) | | |

*Fiche de registre de traitement de données personnelles page 1*

## Fiche de registre ref-000

| Données sensibles | Description | Délai d'effacement |
|---|---|---|
| Données révèlant l'origine raciale ou ethnique | | |
| Données révèlant les opinions politiques | | |
| Données révèlant les convictions religieuses ou philosophiques | | |
| Données révèlant l'appartenance syndicale | | |
| Données génétiques | | |
| Données biométriques aux fins d'identifier une personne physique de manière unique | | |
| Données concernant la santé | | |
| Données concernant la vie sexuelle ou l'orientation sexuelle | | |
| Données relatives à des condamnations pénales ou infractions | | |
| Numéro d'identification national unique (NIR pour la France) | | |

| Catégories de personnes concernées | Description |
|---|---|
| Catégorie de personnes 1 | |
| Catégorie de personnes 2 | |

| Destinataires | Description | Type de destinataire | |
|---|---|---|---|
| Destinataire 1 | | | |
| Destinataire 2 | | | |
| Destinataire 3 | | | |
| Destinataire 4 | | | |

| Tranferts hors UE | Destinataire | Pays | Type de Garanties | | Lien vers le doc |
|---|---|---|---|---|---|
| Organisme destinataire 1 | | | | | |
| Organisme destinataire 2 | | | | | |
| Organisme destinataire 3 | | | | | |
| Organisme destinataire 4 | | | | | |

**EXIGENCES ET APPLICATION DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL EN CRO EN FRANCE.**

L'informatisation du monde de la santé crée un marché florissant du domaine, mais également une convoitise nécessitant l'intensification quasi perpétuelle des mesures de sécurité. Le cadre réglementaire de la recherche clinique en France est en constante évolution. Les entreprises expertes dans le domaine, sont confrontées à de nombreuses exigences, en particulier dans le cadre de Recherches Impliquant la Personne Humaine (RIPH).

Dans ce contexte évolutif mais également concurrentiel, l'application du RGPD (Règlement Général sur la Protection des Données) a augmenter le niveau d'exigences relatif au traitement des données personnelles. Il est capital pour les CRO (Contrat Research Organization / Organisation de recherche par contrat) de disposer d'outils synthétisant l'ensemble des mesures à mettre en place.

L'objectif de ce mémoire est de réaliser une analyse de ce cadre réglementaire et de proposer deux outils méthodologiques permettant d'y répondre.

**Mots-clés : recherche clinique, protection des données, cro, riph, rgpd, santé**

---

**REQUIREMENTS AND APPLICATION OF THE PROTECTION OF PERSONNAL DATA PROTECTION IN CRO IN FRANCE.**

The computerization of the world of health creates a thriving market in this field but also a lust that requires the near-perpetual intensification of the security measures. The French regulatory framework of clinical research is in constant evolution. The health data expert's enterprises have to face a lot of requirements, notably in case of research involving Human person (RIPH).

In this changing context, but also competing context, the application of the GDPR (Global Data Protection Regulation) has increased the personal data processing protection requirements.

It is essential for the CRO (Contract Research Organization) to have a tools that synthetize the complete measures to set-up.

The aim of this document is to produce a regulatory framework analysis and to propose two methodological tools to answer them.

**Key words: clinical research, data protection, cro, riph, gdpr, health**