

Modalités de transfert de données personnelles dans le cadre d'un essai clinique à Gustave Roussy

SOMMAIRE

Abréviations

1. Définitions et exemples de données personnelles
2. La pseudonymisation des données
3. Le transfert des données dans le cadre d'une étude clinique promue par Gustave Roussy
4. Prérequis pour le transfert de données personnelles en dehors des études promues par Gustave Roussy
5. Cas particulier du transfert de données hors UE
6. Transfert des données personnelles dans le cadre de remboursement patient
7. Gestion d'une violation de données personnelles à Gustave Roussy

Liste des documents utilisés

Version 2.0

Réalisé le 03.03.2023

Par :



Jessica BENHAMOU
Chargée qualité

Abréviations

ARC P	Attaché de Recherche Clinique Promoteur
BBE	Bureau de Biostatistiques et d'Epidémiologie
CAR	Chargée d'Affaires Réglementaires
CIOMS	Council for International Organizations of Medical Sciences
CNIL	Commission nationale de l'informatique et des libertés
DM	Data Manager
DPI	Dossier Patient Informatisé
DPO	Data Protection Officer
DSUR	Development Safety Update Report
EMA	European Medicines Agency
GRT	Gustave Roussy Transfert
NIP	Note d'Information Patient
PV	Pharmacovigilance
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsable de la Sécurité des Systèmes d'Information
SAE	Serious Adverse Event
SDV	Source Data Verification

1. Définitions et exemples de données personnelles

Entré en vigueur le 25 mai 2018, le RGPD est une norme européenne qui encadre le traitement de données personnelles. Il définit comme une donnée à caractère personnel toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement.

Quels documents contenant des données personnelles sont susceptibles d'être transférés ?

- Les fiches de préscreening
- Les résultats d'examens et imageries
- Les formulaires SAEs
- CRF
- Compte-rendu d'hospitalisation/de consultation spécialisée et résultats d'examens complémentaires
- Documents de transmission d'échantillon
- Formulaire de satisfaction, de qualité de vie etc.



2. La pseudonymisation des données

La **pseudonymisation** est une méthode qui consiste à remplacer un jeu de données permettant d'identifier, directement (nom, prénom) ou indirectement (n° d'identification du patient, n° de téléphone, date de naissance, etc.) un patient. Cela permet d'assurer la **confidentialité** des données du patient.



Pseudonymisation du patient par:

- La première lettre de son nom
- La première lettre de son prénom
- Son mois et année de naissance (MM/AAAA) / Age
- Numéro d'inclusion dans une étude
- Les 2 premiers chiffres du département de résidence/naissance



Ce qui viole la confidentialité du patient

Nom, Prénom, Jour de naissance, Adresse, Numéro d'identification patient, Adresse et commune de résidence, Fonctions, Situation familiale, origine raciale, niveau de formation, photographie etc.

3. Le transfert des données personnelles dans le cadre d'une étude clinique promue par Gustave Roussy

La formalisation de la requête se fait via le formulaire en ligne :

<https://redcap.link/DataRequestClinicalTrialsGustaveRoussy>



1

La requête est envoyée à l'équipe Promotion :

EQUIPE PROMOTION

BPP : bpp.regulatory@gustaveroussy.fr

BBE : Statisticiens et Data Managers

PV : CTpharmacovigilance@gustaveroussy.fr

L'équipe promotion vérifie le cadre réglementaire de ce transfert, décide de saisir les autorités compétentes si nécessaire et donne son accord.

2

Points de vigilance :

- La conformité aux prérequis réglementaires en matière de protection des données est à vérifier (NIP et consentements) ;
- Ce transfert ne doit pas compromettre le bon déroulement de l'étude, en particulier en matière de levée d'aveugle.

3

Pseudonymisation des données (*cf. page 2*) par l'équipe promotion.

Points de vigilance :

- Vérifier que les données sont à jour ;
- Seules les données nécessaires sont transférées.

4

L'équipe promotion avertit le DPO du transfert des données :



donneespersonnelles@gustaveroussy.fr

5

Un contrat de transfert des données doit être établi. Il est conclu entre GR (via GRT /DPO) et chaque partenaire.

Ce contrat global doit mentionner les modalités de transfert (*Data Transfert Agreement*).

A titre d'exemple, les transferts de données de pharmacovigilance vers les partenaires industriels sont décrits dans contrats appelés *Safety Data Exchange Agreement*.



[GD-GRT](#)

L'équipe promotion effectue le transfert de données à partir de l'une des plateformes suivantes :

6



NEXTCLOUD



EUDRALINK



Plateforme sécurisée du promoteur/destinataire

Remarque : prévoir une date d'expiration de la disponibilité des documents sur la plateforme.

4. Prérequis pour le transfert de données personnelles en dehors des études promues par Gustave Roussy

1

La personne en charge du transfert de données vérifie le contexte, la finalité et le destinataire du transfert (*partenaires industriels, promoteurs, prestataires etc.*).
Il faut de plus s'assurer que le destinataire est en capacité d'assurer la sécurité des données confiées.

2

Un contrat est établi entre Gustave Roussy et le destinataire (GRT et DPO, le cas échéant)

3

Pseudonymisation des données et information au DPO.
Transfert des données sur une plateforme sécurisée (*cf. en page 3*)

5. Cas particulier du transfert des données hors UE

Gustave Roussy est autorisé à transférer des données personnelles, notamment des données de patients, hors de l'UE et l'EEE à condition d'assurer un niveau de protection suffisant et approprié de ces données, sous conditions.

En effet, les personnes dont les données sont traitées par Gustave Roussy doivent être informées :

- de l'**identité** des entités auxquelles les données seront transférées,
- la **nationalité** et le **pays** où seront stockées les données
- des **garanties de protection** de leurs données.

A titre d'exemple, cette information doit se retrouver **dans la notice d'information** (et/ou formulaire de consentement) remise au patient dans le cadre d'une recherche clinique.

Etapes supplémentaires en amont du transfert



Vérifier que le pays dispose d'un niveau de protection adéquat en matière de protection des données. Cette information est disponible sur la carte de niveau de protection des données dans le monde publiée par la CNIL (<https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>) ;



Vérifier l'éventuelle mise à jour des clauses contractuelles :

- Si le pays dispose d'un **niveau de protection adéquat**, aucune clause supplémentaire n'est à implémenter.
- Dans le cas contraire, les clauses contractuelles types de la Commission européenne, dans leur dernière version en vigueur, doivent être adossées au contrat. Elles constituent un outil de sécurité juridique supplémentaire et ne sont pas négociables.



donneespersonnelles@gustaveroussy.fr

6. Transfert de données personnelles dans le cadre de remboursements patients

Le promoteur ne doit avoir aucun accès aux données personnelles du patient. Ainsi, afin de garantir l'anonymisation du patient, le promoteur, doit faire appel à des **prestashop**s dans le cadre du remboursement des patients.

Un numéro de screening et/ou randomisation est attribué à chaque patient et doit être notifié sur chaque formulaire.

Les originaux sont transmis par courrier aux prestataires en charge du remboursement qui transmettent ces données anonymisées au chef de projet/ARC promoteur pour validation par mail.

Dans ce contexte, **un défaut d'anonymisation** porte atteinte à la confidentialité des données patients et constitue une **violation de données** à caractère personnel au sens du RGPD.

7. Gestion d'une violation de données personnelles à Gustave Roussy

Une violation de données personnelles :

- Est caractérisée lorsqu'il y a une atteinte à la confidentialité, à l'intégrité et / ou à la disponibilité des données.
- N'est pas un incident abstrait : même si elle concerne de la donnée, elle peut en effet entraîner des préjudices physiques, matériels et moraux importants sur les personnes.

Que faire lorsqu'on a connaissance d'une potentielle violation de données personnelles ?

Tout incident de sécurité impliquant des données personnelles (*salariés, donateurs, patients/public, clients de Gustave Roussy, prestataires, etc.*) doit :

1

Etre **signalée** au délégué à la protection des données le plus rapidement possible à partir du moment où celle-ci est **connue**, ou **simplement suspectée**



donneespersonnelles@gustaveroussy.fr

2

Etre **évaluée** et peut impliquer une enquête interne (DPO & RSSI)

3

Entraîner la mise en place de mesures correctives, organisationnelles et juridiques, le cas échéant

A qui est déclarée la violation de données personnelles ?



**Autorités,
CNIL**

Sur décision du **Directeur général**,
après recommandation du **DPO**



Patients

Atteinte grave à la vie privée, à la santé, vol de coordonnées, etc.

La décision de notifier à l'autorité de contrôle et / ou à la personne concernée dépend de la gravité du risque engendré par la violation. Les textes précisent que cela peut dépendre de la volumétrie des données / patients concernés. Toutefois, la CNIL adopte une interprétation très stricte des textes. A titre d'exemple, bien qu'une violation de données personnelles n'ait concerné qu'un patient, l'autorité de contrôle a considéré que celle-ci devait être notifiée à la personne concernée car des données de santé (données sensibles au sens du RGPD) étaient concernées.

Cas particulier d'une violation de données dans le cadre d'un essai clinique de médicaments

Les essais cliniques de médicaments sont soumis dès le 31 janvier 2023 selon le Règlement Européen.

Une violation de données peut faire l'objet d'une violation grave, appelée *Serious Breach* et définie dans le protocole de l'étude.

Dans ce cas, il faut suivre le circuit spécifique décrit dans la procédure DRC-M02-PO-008 : « Gestion des violations graves (Serious Breaches) », disponible sur la GED.



Exemples de violations de données personnelles survenues à Gustave Roussy



- * Signalement d'un SAE avec mention de l'adresse du patient sur le formulaire de déclaration ;
- * Enregistrement vocal par un ARC moniteur d'une discussion médicale avec un patient sans son accord ;
- * Vol d'un ordinateur portable et fichiers non enregistrés sur le réseau interne de GR (NAS) ;
- * Erreur d'intégration de compte-rendu patient sur le DPI ;
- * Perte de fichiers médicaux entraînant une indisponibilité de la donnée pouvant altérer la prise en charge du patient ;
- * Publication d'une photo sur les réseaux sociaux laissant apparaître de la donnée personnelle.

Conduite à tenir en cas de doute



En cas de doute sur une faille de données personnelles, veuillez contacter sans délai le service dédié à l'adresse mail suivante :



donneespersonnelles@gustaveroussy.fr

Liste des documents utilisés dans la rédaction de ce mémo

DIR-PDP-MO-004	Transférer des données personnelles hors de l'UE
DRC-R03-MO-012	Sauvegarde, sécurisation et transfert des données
DRC-R04-PO-009	Transfert de données de patients
DRC-R03-MO-003	Gestion des remboursements patients
DIR-PDP-MO-008	Pseudonymiser des données personnelles
DIR-PDP-PL-001	Politique générale de protection des données personnelles