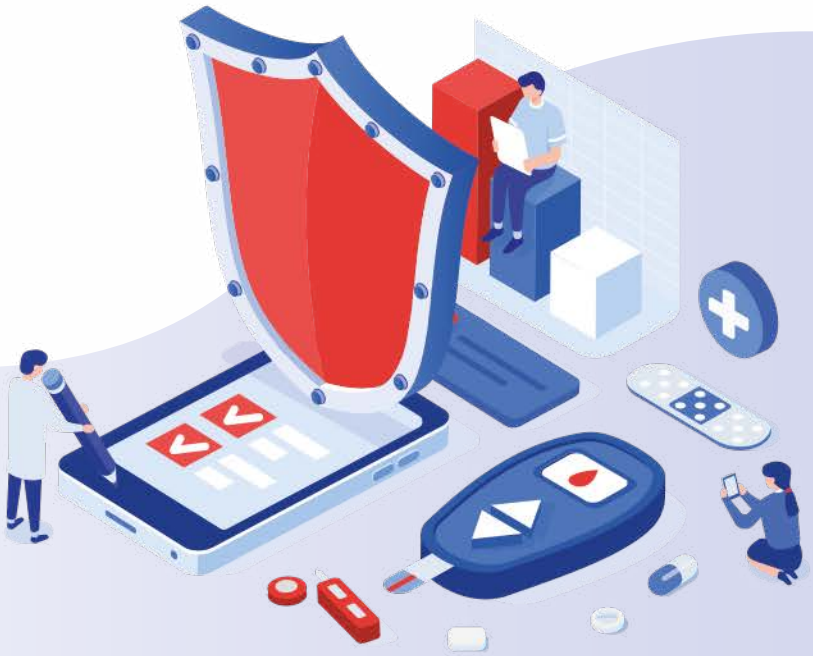
INPDP
الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

GUIDE DE SENSIBILISATION À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL POUR **LA RECHERCHE EN SANTÉ HUMAINE**



Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

Ce Guide fait partie de la "Boîte à outils" de sensibilisation du secteur de la santé à la protection des données personnelles, produite avec le soutien de l'Union européenne et le Conseil de l'Europe dans le cadre du «Projet d'appui aux instances indépendantes en Tunisie». Ni l'Union européenne, ni le Conseil de l'Europe ne pourront être tenus responsables de l'usage qui pourrait être fait des informations qu'elle contient.

I. ÉLÉMENTS DE CONTEXTE

Les données personnelles de santé constituent un matériau de recherche de base pour les communautés scientifiques. Leur traitement occupe une place centrale dans la stratégie de nombreux organismes agissant comme producteurs et comme utilisateurs de données personnelles sensibles dans le cadre d'activités de recherche en santé humaine.

Dans ce cadre, ces organismes doivent se fixer un devoir de vigilance et d'exemplarité concernant l'utilisation de ces données de manière à protéger les libertés fondamentales des individus, particulièrement lorsqu'il s'agit de données sensibles qui doivent être exploitées avec la plus grande rigueur, l'expertise et l'esprit critique nécessaire, dans le respect du cadre éthique et réglementaire.
Le présent guide a pour objectif de fournir aux communautés de recherche en santé une ressource pour s'approprier le cadre de la protection des données personnelles. Construit avec des chercheurs pour des chercheurs, il synthétise les règles applicables à chaque étape du cycle de vie des données et dégage les bonnes pratiques à mettre en œuvre en s'appuyant sur des exemples concrets.
Il ambitionne d'être un outil d'accompagnement aux questionnements légitimes lors de la construction et la réalisation d'un programme de recherche, la publication des résultats et la potentielle réutilisation des données.

Les différents thèmes abordés font référence à la règlementation nationale et européenne applicable en Tunisie sur la protection des données personnelles, à sa déclinaison pour les recherches en santé et présentent des exemples issus de situations rencontrées dans les laboratoires.

Le respect de cette règlementation n'est pas uniquement une question de conformité à la législation en vigueur, même si cette dimension est essentielle. Les bonnes pratiques induites dans la collecte, le traitement, le stockage et la diffusion des données peuvent contribuer à l'amélioration de la science elle-même et favoriser l'exploitation des bases de données. Il permet aux organismes de recherche d'acquérir la confiance des personnes qui concourent au progrès de la science.

II. LES PRINCIPALES DÉFINITIONS ET LEUR APPLICATION POUR LES RECHERCHES EN SANTÉ HUMAINE

Pour toute création d'une base de données de recherche en santé, il convient d'identifier le type de données traitées dans le cadre du projet. Cette étape conditionne l'application ou non des règles relatives à la protection des données personnelles et, le cas échéant, de celles applicables aux données personnelles sensibles, notamment de santé.

1. Qu'est-ce qu'une donnée à caractère personnel ?

Au sens de l'article 4 de la Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel, on entend par données à caractère personnel « toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telles par la loi. »

Les données à caractère personnel sont des données qui permettent d'identifier une personne physique, c'est-à-dire un être humain (dite « personne concernée »). La règlementation s'applique dès lors que l'identification des personnes est permise, peu importe que les données soient relatives à la vie privée, professionnelle ou publique. Cette identification peut être directe ou indirecte.
L'identification peut résulter d'une dénomination (le nom, le prénom ou l'adresse mail nominative apparaissant en clair), elle est alors **directe**.

Elle peut aussi résulter d'éléments relatifs à un individu et qui, seuls ou par recoupement ou l'utilisation de moyens techniques, permettent de retrouver l'identité d'une personne donnée. Elle est alors **indirecte**. Il en va ainsi, notamment :

- des identifiants relatifs à une personne (numéro d'identité national, numéro d'identification renvoyant à une table de correspondance où est consignée l'identité de la personne, numéro d'immatriculation à la sécurité sociale (CNSS), numéro de téléphone, relevé d'identité bancaire, données collectées via les cookies, adresse IP, …) ;
- des caractéristiques physiques (photographie, enregistrement vocal, caractéristiques physiologiques (taille, poids, âge, sexe), empreintes digitales, empreintes génétiques…);
- un faisceau de données qui, sans comporter le nom des personnes, permet de les identifier en raison de la taille réduite de l'échantillon, du type de population concernée, du nombre et de la nature de variables utilisées (dates, données géographiques).

Point de vigilance :

Un fichier de recherche ne peut pas être considéré comme anonyme au seul motif que les noms des participants à cette recherche n'y sont pas consignés. Pour savoir si vous traitez des données à caractère personnel, vous devez faire une analyse au cas par cas des risques d'identification en fonction du contexte et des moyens dont vous disposez ou dont d'autres utilisateurs disposent pour identifier les personnes. Vous traitez des données à caractère personnel, par exemple :

- si le jeu de données comporte la date et le lieu de naissance, le lieu de résidence de patients atteints d'une pathologie rare, ou s'il comporte la date et la commune de décès de personnes ;
- s'il existe un numéro d'ordre renvoyant à une table de correspondance, même si cette table est détenue par un tiers.

En cas de doute sur le caractère identifiant des données, il est recommandé de considérer les données comme identifiantes, jusqu'à la preuve du contraire.

2. Qu'est-ce qu'une donnée pseudonymisée ?

Au sens de l'article 3 de la Délibération n°4 du 5 septembre 2018 de l'Instance nationale de protection des données personnelles (INPDP) concernant le traitement des données à caractère personnel liées à la santé, on entend par « pseudonymisation », le « traitement de données à caractère personnel liées à la santé de manière à ne pas permettre l'identification directe de la personne concernée par le traitement en recourant à un code conservé séparément et soumis à des mesures techniques et organisationnelles afin d'éviter que la personne concernée par le traitement ne soit identifiée à l'aide de ses données personnelles. »

Les données sont dites **pseudonymes** lorsque l'attribution à une personne concernée nécessite le recours à des informations supplémentaires.

En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes d'un jeu de données (nom, prénom, etc.) par des données indirectement identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données relatives à des individus sans pouvoir les identifier de façon directe.

Cette définition couvre différentes techniques couramment utilisées en matière de recherche en santé :

- le recours à une table de correspondance entre le jeu de données pseudonymes (codées) nécessaire aux analyses et les données d'identité conservées séparément, classiquement utilisées dans les essais cliniques ;
- le chiffrement de données directement identifiantes pour les rendre incompréhensibles avec un secret qui permet de chaîner des données relatives à un individu et de suivre son parcours dans le temps sans permettre de l'identifier.

La pseudonymisation est un traitement de données personnelles assurant la confidentialité des données tout en préservant intégralement leur utilité. C'est un bon compromis entre les besoins de la recherche et la sauvegarde des intérêts des participants en limitant la gravité des impacts potentiels, notamment en cas d'atteinte à la confidentialité des données. Il convient donc d'y avoir recours dans le cadre d'un traitement de données à des fins de recherche scientifique lorsqu'il est nécessaire d'avoir des **informations exactes au niveau individuel** sans pour autant que les données directement identifiantes soient nécessaires pour mener cette recherche.

La pseudonymisation est une opération **réversible**, contrairement à l'anonymisation. En pratique, il est possible de retrouver l'identité des personnes dont les données ont été pseudonymisées. Cette opération peut être réalisée en accédant à des informations supplémentaires conservées séparément (la table de correspondance mettant en relation informations directement identifiantes et pseudonymes par exemple) ou encore grâce à des données tierces (permettant de ré-identifier les individus à partir de connaissances préalables, de sources publiques, privées, etc.).

Les données résultant d'une pseudonymisation sont donc considérées comme des données personnelles et leur traitement reste soumis aux principes de protection des données personnelles.

Dans sa délibération n°4, l'INPDP encourage le recours à la pseudonymisation dans le cadre de la recherche scientifique. La pseudonymisation réduit en effet le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée. À ce titre, elle concourt à la minimisation des risques pour les personnes.

Le choix de la technique de pseudonymisation appropriée dépend, entre autres, de deux facteurs :

le niveau de protection requis et l'utilité des données pseudonymisées pour les besoins de la recherche envisagée. Il est ainsi nécessaire de mettre en balance ces deux aspects en se posant les bonnes questions vis-à-vis du traitement envisagé :

- de quelles informations a-t-on réellement besoin ?
- a-t-on besoin de pouvoir lier les données d'un même individu ?

Quelle que soit la technique de pseudonymisation utilisée, les informations permettant de mettre en relation les pseudonymes générés et les données directement identifiantes revêtent une sensibilité importante (table de correspondance, clé de chiffrement, etc.). Il convient de s'assurer que la confidentialité de ces éléments est assurée par des **mesures techniques et organisationnelles appropriées**. Ces informations ne doivent ainsi être conservées que dans des conditions de nature à garantir leur confidentialité et seules des personnes autorisées doivent pouvoir y accéder et ce dans des conditions préalablement spécifiées. Dans sa Délibération n°3, l'INPDP préconise le recours à un organisme neutre et indépendant du responsable de traitement pour conserver ces données afin de garantir la confidentialité des « clés » permettant la ré-identification, (art. 30).

3. Données anonymes ou anonymisées ?

Au sens de l'article 3 de la Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé, on entend par « **anonymisation** », le « traitement des données à caractère personnel relatives à la santé de manière à ne pas permettre l'identification de la personne concernée pour le traitement. »

Les données anonymes ou anonymisées ne sont pas soumises à la règlementation relative à la protection des données personnelles, qu'elles soient anonymes initialement ou après une anonymisation par un traitement permettant de garantir que la personne concernée ne pourra pas être réidentifiée par la suite (données anonymisées). Travailler à partir de données anonymes ou anonymisées permet donc de s'affranchir de cette règlementation car la diffusion ou la réutilisation des données anonymisées n'est pas susceptible d'avoir un impact sur la vie privée des personnes concernées.

L'impossibilité d'identifier les personnes requiert une **évaluation des risques au cas par cas**. Elle s'apprécie au regard des **moyens raisonnablement susceptibles d'être utilisés** par le responsable de traitement ou par toute autre personne. Elle passe en pratique par la prise en considération du coût de l'identification, du temps nécessaire à celle-ci, des technologies disponibles, existantes mais aussi à venir.

En application du principe de « minimisation » des données, les données doivent être autant que possible dé-identifiées, voire anonymisées, si les objectifs de la recherche peuvent être atteints sans recours à des données identifiantes.

Toutefois, les chercheurs ont parfois besoin de traiter des données à caractère personnel pour recontacter les personnes concernées dans le cadre d'un suivi longitudinal, pour permettre leur éventuel chaînage ou leur appariement ou permettre une analyse fine des facteurs de risque pour la santé (ex : géocodage des adresses pour étudier les variations géographiques des problèmes de santé).

L'anonymisation des données n'est alors pas requise dès lors que la collecte de données identifiantes est nécessaire et proportionnée au besoin d'en connaître. Une analyse de pertinence et de proportionnalité au regard des objectifs de la recherche doit être effectuée au cas par cas et documentée dans les documents de conformité soumis à l'INPDP pour obtenir l'autorisation du traitement des données de santé.

Comment évaluer un processus d'anonymisation ?

Le Comité européen de protection des données, donne trois critères qui permettent de s'assurer qu'un jeu de données est véritablement anonyme :

- non-individualisation : il ne doit pas être possible d'isoler un individu dans le jeu de données
- non-corrélation : il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu
- non-inférence : il ne doit pas être possible de déduire de façon quasi certaine de nouvelles informations sur un individu

À défaut de remplir parfaitement ces trois critères, il doit être démontré, par une évaluation approfondie des risques d'identification, que le risque de ré-identification avec des moyens raisonnables est nul.

Pour approfondir :

- Avis sur les techniques d'anonymisation du Groupe de travail du G29 sur la protection des personnes à l'égard du traitement des données à caractère personnel.

L'impossibilité de pseudonymiser les données doit rester exceptionnelle et elle doit être documentée.

Les techniques d'anonymisation et de ré-identification étant amenées à évoluer régulièrement, il est indispensable d'effectuer une veille régulière afin de préserver, dans le temps, le caractère anonyme des données produites.

Si un jeu de données publié en ligne comme anonyme contient en réalité des données personnelles, il convient dès lors de procéder à son retrait dans les plus brefs délais.

En pratique, l'anonymisation suppose donc :

- une évaluation, au cas par cas, en tenant compte à la fois du contexte et du risque, de la technique ou de la combinaison des techniques d'anonymisation, étant entendu qu'aucune technique n'est infaillible;
- une réévaluation régulière au regard de l'évolution des techniques;
- la destruction irréversible des données initiales.

En règle générale et par défaut, il convient de considérer que les données personnelles traitées dans le cadre des projets de recherche en santé humaine ne peuvent pas être anonymisées. Dans l'hypothèse où une équipe de recherche estimerait qu'elle met en œuvre un processus d'anonymisation valide, il lui appartiendrait d'en apporter la preuve en fournissant l'évaluation des risques de ré-identification précitée, si besoin avec l'appui d'un expert externe.

Pour approfondir :

- Comprendre les grands principes de la cryptologie et du chiffrement
- Guide « Techniques et meilleures pratiques de pseudonymisation » de l'Agence européenne de cybersécurité (ENISA)
- Le guide de la CNIL relatif à l'anonymisation
- Guide d'Etalab sur la pseudonymisation de documents textuels par IA

Recommandations :

En matière de la recherche scientifique, l'INPDP encourage les chercheurs à recourir à l'anonymisation des données des personnes concernées chaque fois qu'elle est possible, (Délibération n°4 (Art. 30). Il en va de même de l'article 15.9 de la Recommandation CM/REC (2019) du Conseil de l'Europe en matière de protection des données de santé.

Si l'anonymisation n'est pas permise, les données doivent être pseudonymisées : l'article 67 de la Loi organique numéro 63 du 27 juillet 2004 portant sur la protection des données à caractère personnel, précise en ce sens que « Les données à caractère personnel ne doivent pas contenir des éléments susceptibles de révéler l'identité de la personne concernée, lorsque les exigences de la recherche scientifique le permettent ».

En cas de pseudonymisation des données, l'INPDP préconise le recours à un organisme professionnel neutre et indépendant chargé de faire le lien entre l'identité des personnes concernées et le symbole qui lui est attribué afin de garantir le respect de ces personnes.

En cas d'impossibilité de pseudonymiser les données quand cela empêche la réalisation des objectifs de la recherche, le recours à des données directement identifiantes doit rester exceptionnelle et justifiée dans la demande d'autorisation soumise à l'INPDP (ex : recours à des données directement identifiantes nécessaires au suivi longitudinal des personnes qui nécessite de les recontacter régulièrement). Les données directement identifiantes doivent alors être conservées de façon séparée des données pseudonymisées, accessibles à un nombre limité de personnes nommément habilitées et dans des conditions de nature à en garantir la confidentialité (ex : armoire fermée à clé).

4. Données sensibles et protection renforcée

Compte tenu de la sensibilité de certaines catégories de données, le législateur, dans la Loi organique n° 63 du 27 juillet 2004 portant sur la protection des données à caractère personnel, leur a consacré des dispositions particulières leur offrant une protection renforcée en raison des risques d'atteintes à la vie privée et à la dignité des personnes concernées qu'elles comportent (discrimination, exclusion…) (Art.13 et 14).

Quelles sont les catégories particulières de données ?

L'article 14. de la Loi n°2004-63 vise les données à caractère personnel qui concernent, directement ou indirectement, « l'origine raciale ou génétique, les convictions religieuses, les opinions politiques, philosophiques ou syndicales, ou la santé… »

Les données sensibles sont celles qui font apparaître directement ou indirectement :

- la santé (physique ou mentale),
- les données génétiques (par exemple ADN, caryotype),
- l'origine raciale,
- les opinions politiques,
- les convictions religieuses ou philosophiques,
- l'appartenance syndicale.

Sont également concernées :

- la vie sexuelle ou l'orientation sexuelle (telles que mentionnées dans la Convention n°108 du Conseil de l'Europe ratifiée par la Tunisie);
- les données biométriques aux fins d'identifier une personne physique de manière unique;
- les données à caractère personnel relatives aux infractions, à leur constatation, aux poursuites pénales, aux condamnations, aux mesures préventives ou aux antécédents judiciaires.

Les données de santé : une définition très large

L'article 3 de la Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé définit les « données de santé » comme étant « des données à caractère personnel qui consistent en toutes les données relatives à l'état de santé physique, mental ou psychologique de la personne physique concernée par le traitement, ainsi qu'aux caractéristiques génétiques héritées ou acquises, et qui fournissent des informations distinctives sur elle-même ou sur sa santé, résultant de l'analyse d'un échantillon biologique de cette personne, ainsi que des services de traitement médical qui lui sont fournis et qui divulgueraient ces données. »

Par ailleurs, l'article 3 de la Recommandation CM/REC (2019) du Conseil de l'Europe en matière de protection des données de santé définit les données relatives à la santé comme « toute donnée à caractère personnel relative à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé passé, actuel et futur de cette personne ».

L'état de santé s'entend de **l'état de santé physique et mentale, présent, passé ou futur de la personne** et comprend très largement :

- toute information sur l'identification du patient dans le système de soins,
- toutes les prestations de services de santé,
- des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques),
- toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source.

Sont concernées :

- les données qui permettent d'indiquer la pathologie dont peut être atteint un individu (données de santé « **par nature** ») ; antécédents médicaux, maladies, prestations de soins, résultats d'examens, traitements, handicap, etc;
- le croisement de données qui permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne (ex : croisement d'une mesure de poids avec l'âge, la taille, etc.); ce sont des données de santé **par croisement ;**
- les données qui deviennent des données de santé en raison de l'utilisation qui en est faite au plan médical, y compris dans le cadre d'une recherche en santé portant sur des échantillons biologiques humains (données de santé **par destination**).

L'article 3 de la Délibération N° 4 définit les « données génétiques » comme étant les « données à caractère personnel relatives aux caractéristiques génétiques ou acquises d'une personne physique, qui fournissent des informations distinctives sur elle-même ou sur son état de santé, résultant notamment de l'analyse d'un échantillon biologique de cette personne. »

Pour approfondir :

- Voir la fiche thématique CNIL "Qu'est-ce qu'une donnée de santé ?"

Quelles sont les règles régissant les données sensibles ?

Des règles plus strictes sont applicables à ces données « sensibles ».

Les articles 13 et 14 de la Loi n°2004-63 soumettent cette catégorie particulière de données à un **principe d'interdiction de traitement sauf à pouvoir se prévaloir d'une des exceptions limitativement énumérées par la loi**.

Cette interdiction de principe n'interdit pas le traitement de ces données sensibles mais il faut, pour pouvoir les traiter :

1. Pouvoir justifier d'une des exceptions légales à l'interdiction

Parmi les exceptions mentionnées par les articles 14 et 62 de la loi n°2004-63, le traitement de données de santé est possible notamment, dans les cas suivants applicables à la recherche en santé humaine :

- la personne concernée, ses héritiers ou son tuteur, a donné son consentement à un tel traitement par n'importe quel moyen laissant une trace écrite;
- le traitement est nécessaire à la réalisation de finalités prévues par la loi ou les règlements;
- le traitement s'avère nécessaire pour le développement et la protection de la santé publique entre autres pour la recherche sur les maladies;
- le traitement s'avère nécessaire à des fins historiques ou scientifiques;
- le traitement s'effectue dans le cadre de la recherche scientifique dans le domaine de la santé.

  Sont notamment concernées les données recueillies dans le cadre d'essais cliniques ou celles obtenues ultérieurement à partir de matériel biologique d'origine humaine.

2. Entourer le traitement de ces données sensibles de garanties appropriées (de fond et de procédure)

Parmi les garanties à mettre en place, en plus des formalités à accomplir (V. rubrique formalités) :

- apprécier la nécessité du traitement de données relatives à la santé pour une recherche scientifique au regard de la finalité poursuivie par le projet de recherche, du risque encouru par la personne concernée et, en matière de données génétiques, par sa famille biologique (Délibération n°4, art. 28)

- adapter les mesures de sécurité aux risques inhérents à la sensibilité de ces informations

5. Qu'est-ce qu'un traitement de données à caractère personnel ?

Un traitement est défini comme **une opération ou un ensemble d'opérations** appliquées à des données à caractère personnel, effectuées ou non à l'aide de moyens automatisés.

L'article 3 de la Délibération n°4 de l'INPDP définit le traitement de données à caractère personnel comme étant « les opérations réalisées d'une façon automatisée ou manuelle et qui ont pour but notamment la collecte des données à caractère personnel, leur accès, leur enregistrement, leur sauvegarde, leur organisation, leur correction, leur exploitation, leur utilisation, leur envoi, leur diffusion, leur publication, leur liaison à d'autres données, leur communication, leur transfert, leur exposition de quelque manière que ce soit, l'anonymisation de leur identité, leur pseudonymisation, leur effacement ou leur destruction. »

Les principes de protection des données à caractère personnel s'appliquent à toute opération effectuée sur des données à caractère personnel quel que soit le support (papier, électronique, vidéo, photographique…) et le procédé utilisé (manuel ou automatisé). Il peut s'agir d'une application informatique, de la constitution d'un fichier ou d'un questionnaire, par exemple.

Le traitement au sens de la règlementation vise ainsi notamment la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. La collecte constitue en elle-même un traitement, même si elle est effectuée sur support papier. Les fichiers papier doivent être protégés dans les mêmes conditions.

6. Le cadre juridique applicable au traitement de données de santé dans le domaine de la recherche médicale

Le traitement de données de santé dans le cadre de la recherche en santé humaine est soumis notamment à la réglementation suivante :

- Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, telle que mise à jour à la lumière de la Convention n°108 ratifiée par la loi organique n° 2017-42 du 30 mai 2017, portant approbation de l'adhésion de la République tunisienne à la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel n° 181 concernant les autorités de contrôle et les flux transfrontières de données et notamment la Section III. Du traitement des données à caractère personnel dans le cadre de la recherche scientifique (articles 66 à 68)
- Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel relative à la santé et notamment la Section IV. De la recherche scientifique (articles 28 à 32)
- Décret n° 2007-3004 du 27 novembre 2007 fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel
- Conseil de l'Europe : Convention 108 et Recommandation CM/Rec (2019)2 en matière de protection des données relatives à la santé

En outre, le traitement des données de santé nécessaires à la recherche en santé humaine peut être soumis aux dispositions du Règlement général sur la protection des données (RGPD), dans le cas où :

- le traitement effectué prévoit le recours à un sous-traitant établi sur le territoire de l'Union européenne;
- le traitement vise les personnes se trouvant sur le territoire de l'UE pour (critère du ciblage) leur offrir des biens ou des services ou suivre leur comportement au sein de l'UE (patients, participants européens aux recherches).

À noter que pour la recherche en santé, la loi Informatique et libertés française s'applique en plus du RGPD, dès lors que les données traitées concernent des résidents français, que le responsable de traitement soit établi en France ou non.
(voir QR code à la fin du document pour textes et références législatives)

III. LES ACTEURS DE LA PROTECTION DES DONNÉES DE SANTÉ

Il s'agit ici d'identifier le rôle de chacun des acteurs vis-à-vis du ou des traitements de données de santé.

Acteur(s)	Définition	Exemple(s)/Explications
Responsable du traitement de données	Il s'agit de toute personne physique ou morale, tunisienne ou étrangère, appartenant au secteur privé ou public, qui détermine la nature des données à caractère personnel liées à la santé, la finalité ainsi que les modalités de leur traitement. C'est celui qui décide qu'un traitement de données doit être mis en place, qui y a intérêt, et qui détermine son but, le type de données collectées, les catégories de personnes concernées, les destinataires et la durée de conservation (moyens essentiels du traitement). La loi n°2004-63 (Art.63) et la Délibération n°4 (Art.2) de l'INPDP ont précisé les personnes morales ou physiques qui sont habilitées à traiter les données de santé.	Pour les études qui exigent un promoteur, le responsable du traitement est le promoteur de la recherche. Le responsable du traitement n'a pas nécessairement lui-même accès aux données ou à toutes les données. Par exemple, le promoteur n'a pas en général accès aux données directement identifiantes collectées par les centres investigateurs. De même, les partenaires industriels peuvent commander des analyses de données et n'en recevoir que les résultats.

Responsable conjoint ou co-responsable de traitement de données	Il peut y avoir plusieurs responsables de traitement lorsque plusieurs personnes physiques ou morales déterminent les finalités et moyens du même traitement. La finalité du traitement doit être la même pour tous les co-responsables, mais leur degré d'implication peut être inégal. Leurs décisions concernant les moyens peuvent être prises en commun ou de façon convergente.	Dans le cadre d'une recherche réalisée en collaboration avec d'autres personnes physiques ou morales, ces autres personnes peuvent être qualifiées de co-responsables. Elles doivent définir de façon transparente leurs obligations respectives par voie d'accord. Les personnes concernées pourront exercer leurs droits à l'égard et à l'encontre de chacun d'entre eux.
Responsable d'un autre traitement de données	Il peut notamment s'agir du responsable d'un traitement réalisé avec les mêmes données, mais dont la finalité est différente. Cette situation se rencontre notamment en cas de réutilisation des données.	Dans le cas d'une recherche portant sur des données collectées dans le cadre des soins, l'hôpital est responsable du traitement de données dont la finalité est le soin, et l'organisme de recherche est responsable du traitement dont la finalité est la recherche.
Sous-traitant	Il s'agit de toute personne physique ou morale, indépendante du responsable de traitement, qui traite des données de santé pour le compte du responsable du traitement et sous son contrôle. Le sous-traitant n'effectue pas de traitement pour ses propres besoins et n'a donc pas vocation à conserver les données à l'issue de la prestation. Le sous-traitant peut être amené à déterminer certains aspects opérationnels du traitement qualifiés de moyens non essentiels (par exemple, le type de logiciel ou de serveur utilisé), . Il peut y avoir sous-traitance en cascade (le sous-traitant sous-traite lui-même certaines opérations). La notion de sous-traitance est proche de celle de prestation. Il convient de rappeler que ces notions juridiques ne préjugent en rien de la nature des travaux à réaliser et s'appliquent même si l'activité du sous-traitant est très technique et requiert une expertise particulière. Le sous-traitant doit présenter des garanties adaptées pour assurer la sécurité et la confidentialité des données. Ces garanties doivent être précisées notamment dans le contrat qui lie le responsable de traitement et le sous-traitant. Ce dernier précise également leurs engagements respectifs pour le traitement de données.	Par exemple, l'organisme qui héberge les données pour le compte du responsable de traitement est un sous-traitant. L'hébergeur est la personne qui procède au stockage des données personnelles liées à la santé sans les traiter. Société de sondage : passation d'une enquête par un institut de sondage. Le sous-traitant est en charge de la collecte des informations auprès des personnes concernées ; le chercheur récupère les informations ainsi obtenues. Dans certains cas, il est possible que ces données soient pseudonymisées par le sous-traitant. Les équipes de recherche qui réalisent certains travaux pour les besoins d'une recherche promue par un tiers (hôpital, notamment) agissent en tant que sous-traitant, au sens de la règlementation.
Destinataires	Il s'agit de toutes les personnes et services, habilitées en raison de leurs fonctions, à recevoir communication des données. En principe, seules les personnes qui relèvent du responsable de traitement ou du sous-traitant sont susceptibles d'être destinataires des données.	Les chercheurs et autres personnels scientifiques des unités qui traitent les données, ainsi que les personnels des services informatiques susceptibles d'y avoir accès sont des destinataires.

Les personnes concernées	Il s'agit des personnes physiques dont les données à caractère personnel font l'objet d'un traitement. Par exemple, les participants aux études qui acceptent de prêter leur concours à la recherche. L'INPDP estime que certaines catégories de personnes sont particulièrement vulnérables en raison du déséquilibre de la relation entre la position de la personne concernée et le responsable de traitement. Elle classe notamment dans cette catégorie les enfants, les employés, les patients, dont les personnes dont les facultés de discernement sont altérées, les demandeurs d'asile ou les personnes âgées. Le caractère vulnérable des personnes concernées est un des critères à prendre en considération pour déterminer si un traitement doit donner lieu à une analyse d'impact.	
Le Délégué à la protection des données (DPO)	Le délégué à la protection des données à caractère personnel est « la personne désignée par le responsable du traitement et qui veille à assurer le respect des règles de protection des données personnelles et répond aux demandes d'accès aux données personnelles. » (Délibération n°4- Art.3 de l'INPDP) Le délégué de la protection des données personnelles accomplit les tâches suivantes, avec toute impartialité et indépendance : • tenir un registre des activités de traitement effectuées par le responsable du traitement et/ou le sous-traitant ; toute personne concernée peut y accéder à sa demande; • accepter les demandes d'accès aux données personnelles; • réglementer toutes les activités internes liées à la protection des données personnelles; • préparer un programme d'action pour améliorer la protection des données à caractère personnel en coopération avec le responsable du traitement; • préparer un rapport annuel sur les activités liées à la protection des données personnelles qui est envoyé à l'INPDP et publié sur le site internet de l'organisme de recherche; • faire le lien entre la structure responsable du traitement et l'Instance nationale de protection des données personnelles. (Délibération n°4- Art.15).	Conformément à l'article 15 de la Délibération n°4 de l'INPDP, et compte tenu de la sensibilité des données traitées, chaque responsable du traitement amené à traiter des données de santé dans le cadre de la recherche en santé humaine doit désigner un chargé de protection des données à caractère personnel, informer l'Instance de la décision de nomination et la communiquer au public. La désignation d'un délégué à la protection des données est ainsi un gage de sécurité juridique. En outre, sa désignation, de même que son rattachement au plus haut niveau de la hiérarchie, témoignent de l'engagement d'un organisme en faveur de la protection des données personnelles. Le DPO est un acteur clé de la démarche de conformité des traitements effectués par le responsable de traitement. Outre les tâches prévues par la Délibération n°4, il pourra : • sensibiliser et former les chercheurs et les personnels qui traitent les données de santé au sein de l'organisme au respect de la réglementation et à la définition de bonnes pratiques adaptées au responsable du traitement; • veiller à la bonne tenue de la documentation requise par les textes; • être associé en temps utile à toutes les questions relatives à la protection des données par anticipation et dès le montage des projets;

		• prodiguer des conseils utiles lors de la réalisation d'une analyse d'impact pour les traitements les plus sensibles. Le responsable du traitement doit mettre à la disposition du délégué à la protection des données les moyens humains et matériels requis pour effectuer ses tâches.
Instance nationale de protection de données personnelles (INPDP)	Il s'agit de l'autorité compétente pour la protection des données personnelles en Tunisie. Vous trouverez des informations sur la règlementation sur son site internet : www.inpdp.nat.tn	L'INPDP veille au respect de l'ensemble des règles de la protection des données à l'occasion de l'examen des demandes d'autorisation dont elle doit être saisie en cas de recours à des données de santé et en coordination avec les structures médicales compétentes.

L'identification des différents acteurs se fait par traitement, c'est-à-dire par type d'opération sur les données. Un même organisme peut être responsable d'un traitement et sous-traitant, selon l'opération.

L'identification des différents acteurs doit se baser sur la réalité factuelle et ne peut être décidée par convention.

Cette phase peut être délicate en cas de pluralité d'intervenants ou de traitements successifs, mais elle est essentielle pour la suite ; aussi convient-il d'y apporter le plus grand soin.

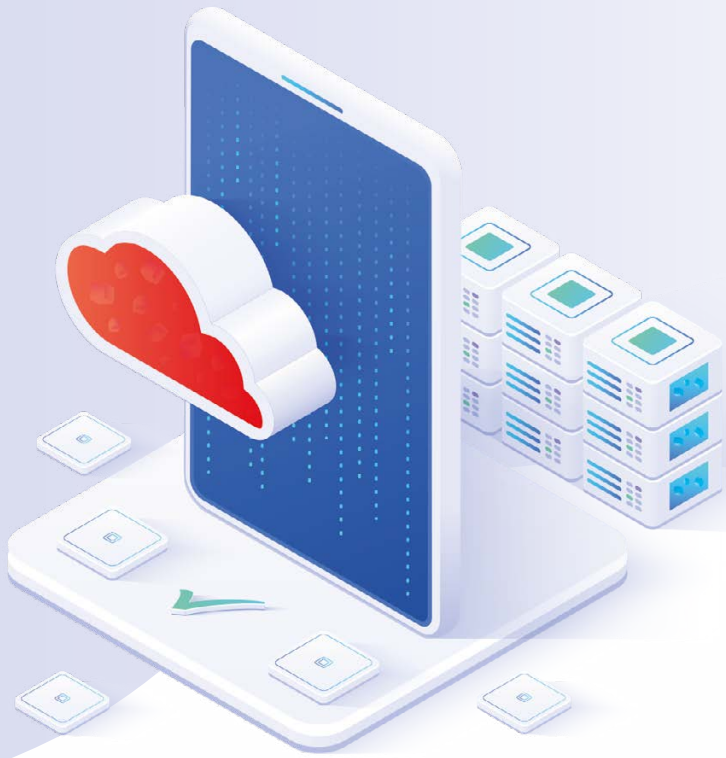
Voici quelques questions qu'il peut être utile de se poser :

- le traitement s'effectue-t-il en plusieurs phases ?
- qui collecte ou reçoit les données ?
- qui sont les différents organismes intervenant dans le traitement ?
- qui a pris l'initiative du traitement des données et qui en bénéficie ?
- qui décide des moyens essentiels du traitement (type différence de caractères de données collectées, catégories de personnes concernées, destinataires, durée de conservation) ?
- qui décide du calendrier de l'étude ?

Lorsque plusieurs acteurs interviennent, il est nécessaire d'organiser leurs rapports et, en particulier, la répartition de leurs obligations concernant les données à caractère personnel par voie contractuelle.

Pour approfondir :

- Le Guide du sous-traitant de la CNIL
- Lignes directrices du CEPD n°07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant (notamment les logigrammes des pages 49 à 51)
- La fiche thématique CNIL sur délégué à la protection des données
- CNIL, Guide pratique RGPD - Délégués à la protection des données



IV. LES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Avant d'engager son projet de recherche et lorsque celui-ci contient des données à caractère personnel, le responsable du projet scientifique doit s'assurer du respect des principes de la protection des données personnelles:

- la licéité du traitement, soit le fondement du traitement;
- la limitation des finalités du traitement ;
- la minimisation ou la pertinence et la proportionnalité des données et l'exactitude des données ;
- la sécurisation et la protection des données ;
- la limitation de la conservation des données ;
- la loyauté et la transparence des informations sur l'utilisation des données.

Chaque traitement de données à caractère personnel doit être analysé à la lumière de ces principes dès la phase de conception des projets qui impliquent un traitement de données personnelles, puis tout au long de la vie du projet.

Cette analyse doit être documentée afin de répondre aux exigences de conformité et de responsabilité.

Principes	Contenu	Point(s) d'attention
Loyauté et transparence	Les établissements légalement habilités à mener des recherches médicales ne sont fondés à utiliser les données de santé dans le cadre de projets de recherche scientifique qu'après en avoir informé la personne concernée, conformément aux dispositions de la (Délibération n°4 Art. 29 de l'INPDP). Ces principes de loyauté et de transparence exigent que les personnes dont les données sont traitées dans le cadre de recherches scientifiques disposent de droits sur elles afin d'en conserver la maîtrise. Le respect des droits des personnes concernées est une obligation qui pèse sur chaque responsable de traitement. Elle passe en premier lieu par le principe de **loyauté** et de **transparence** à l'égard de la personne concernée. En matière de recherche en santé, cette transparence est une garantie essentielle reconnue aux participants de la recherche en contrepartie de la levée du secret professionnel.	Respecter le **droit à l'information** des personnes concernées sur les principaux éléments du traitement, fournie de façon claire. (finalité, base légale, destinataires, durée de conservation, etc.), L'information doit être délivrée individuellement à chaque personne participant à la recherche, que les données soient recueillies auprès d'elle ou de tiers. L'information dans le cadre des traitements de données personnelles doit être articulée avec celle fournie dans le cadre de la recherche en santé humaine. Elle doit être **préalable** à la collecte des données, **sauf en cas d'impossibilité** d'information, lorsqu'il s'agit par exemple d'un traitement de données **à des fins documentaires dans le cadre de l'intérêt public ou à des fins de recherche scientifique** ou historique ou de travail statistique. (Délibération n°4-Art.23).
	Cette analyse permet aux personnes concernées de comprendre les objectifs de la recherche, les modalités de leur participation, la portée de l'accord qu'elles donnent et de maîtriser l'utilisation qui sera faite de leurs données. Elle conditionne et facilite l'exercice de leurs droits. Elle permet d'instaurer une relation de confiance avec les chercheurs et l'organisme dont ils dépendent. **Le droit à l'information des personnes concernées** est le premier droit de ces personnes et l'un des plus importants car il conditionne tous les autres droits. Elles doivent être clairement informées des modalités pratiques d'exercice des droits, et les démarches à effectuer ne doivent pas être de nature à les décourager.	L'impossibilité d'information préalable ne peut être invoquée que lorsque les données n'ont pas été obtenues auprès des personnes concernées elles-mêmes et elle doit être dument justifiée auprès de l'INPDP au regard, par exemple, du nombre de personnes concernées, de l'ancienneté des données, du fait que les personnes ont déménagé et ont été perdues de vue, etc. L'INPDP sera très attentive à cette justification lorsqu'elle se prononcera sur le caractère impossible de l'information. L'information doit être délivrée dans un **langage clair** et être facilement accessible. Cette information individuelle peut être délivrée par : • la remise d'une notice d'information aux personnes concernées, • l'envoi d'un courrier postal ou électronique. Il est de bonne pratique de doubler l'information individuelle d'une information générale dans les lieux de soins qui transmettent des données à caractère personnel pour permettre des activités de recherche (affichage dans les locaux, mention dans le livret d'accueil, etc.)

		Lorsque la personne concernée est frappée d'incapacité, il faut informer la personne qui la représente légalement. (Délibération n°4- Art.23) de l'INPDP. Réfléchir en amont aux besoins de réutilisation des données, de partage, de transfert, et penser à en informer les personnes concernées. Pour connaître les informations à faire figurer dans les documents d'information, se reporter au tableau plus loin (Voir page 27 du présent document).
	Respecter **le droit d'accès** des personnes qui consiste à pouvoir demander si des données les concernant sont traitées, obtenir des informations sur ce(s) traitement(s) et une copie de leurs données pour en vérifier le contenu.	La réponse à cette demande doit intervenir dans les meilleurs délais à compter de sa réception.
	Respecter le **droit de rectification** qui permet aux personnes concernées d'obtenir la modification des données inexactes ou incomplètes les concernant.	La rectification doit être signalée aux tiers destinataires des données, sous réserve d'impossibilité ou d'efforts disproportionnés pour ce faire.
	Respecter **le droit à l'effacement** ou **droit à l'oubli** qui permet, dans certains cas, d'obtenir la suppression des données auprès du responsable d'un traitement. Dans ce cas, ces données doivent être détruites ou l'identité de la personne concernée doit être anonymisée (Délibération n°4 -Art.31 de l'INPDP)	Ce droit n'est pas applicable, dans le cadre de la recherche scientifique, **s'il est susceptible d'en affecter la valeur scientifique.** Il risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement (biais, obligation de fournir des données dans le cadre de procédures règlementaires, etc.). Il convient alors de documenter l'analyse et d'informer les personnes concernées que leurs droits font l'objet de restrictions.
	Respecter le **droit à la limitation du traitement** qui permet, dans certains cas, d'obtenir que soit gelée temporairement l'utilisation de certaines ou de la totalité des données des personnes.	La limitation doit être signalée aux tiers destinataires des données, sous réserve d'impossibilité ou d'efforts disproportionnés pour ce faire.
	Respecter le **droit d'opposition** permet, en principe, de s'opposer à tout moment au traitement de ses données, y compris après avoir donné son consentement.	

	Le droit à la portabilité est le droit de la personne concernée de transférer ses données personnelles d'un responsable du traitement à un autre.	Compte tenu des difficultés pratiques d'application de ce droit au domaine de la recherche scientifique, les organismes et laboratoires de recherche doivent réfléchir aux modalités de mise en œuvre effective de ce droit dès la conception du projet dans le respect de la réglementation applicable.
	Respecter **le droit de ne pas faire l'objet d'une décision exclusivement fondée sur un traitement automatisé** produisant des effets juridiques concernant une personne ou l'affectant de manière significative.	Une « décision automatisée » est une décision prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus. A priori, une telle décision n'interviendra pas dans le cadre d'un traitement à finalité de recherche scientifique en santé.
Licéité du traitement de données	**Déterminer la base légale du traitement.** La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter ces données. Le traitement des données à caractère personnel qui concernent, directement ou indirectement la santé des personnes est en principe interdit (Loi organique n° 2004-63- Art.14). Toutefois, ce traitement est possible lorsqu'il s'effectue dans le cadre de la recherche scientifique dans le domaine de la santé (Loi organique n° 2004-63-Art. 62). Les conditions de traitement des données de santé à des fins de recherche scientifique sont évaluées par l'INPDP en coordination avec les structures médicales spécialisées.	Les données de santé peuvent être traitées pour les besoins de la recherche scientifique et ne nécessitent pas toujours un consentement de la personne concernée. **Attention :** Ne pas confondre le **consentement à la participation à la recherche** qui peut être requis en raison de la qualification réglementaire de la recherche et le **consentement au traitement des données**, retenu comme base légale d'un traitement. Le consentement de la personne peut être requis dans le cadre d'une recherche en santé sans constituer pour autant la base légale du traitement. Conformément aux dispositions de l'article 29 de la Délibération n°4 de l'INPDP, les données de santé ne peuvent être utilisées dans le cadre de recherches scientifiques que si la personne concernée a été informée et a donné son consentement. **Point de vigilance :** Conformément aux dispositions de l'article 28 de la Loi n°63-2004, « le traitement des données à caractère personnel qui concerne **un enfant** ne peut s'effectuer qu'après l'obtention du consentement de son tuteur et de l'autorisation du juge de la famille. Le juge de la famille peut ordonner le traitement même sans le consentement du tuteur lorsque l'intérêt supérieur de l'enfant l'exige. Le juge de la famille peut, à tout moment, revenir sur son autorisation.»

	Publication des résultats de la recherche. Délibération n°4-Art.32. « Les données à caractère personnel liées à la santé ne peuvent être publiées à des fins de recherche scientifique dans une forme ou d'une manière permettant l'identification de la personne concernée, sauf si cette personne accorde son consentement sur la publication et en vertu d'une autorisation de l'INPDP, conformément aux dispositions de l'article 65 de la loi susmentionnée ».	
Limitation de la finalité	**Déterminer la finalité du traitement.** Elle correspond à l'objectif poursuivi. C'est l'objectif principal poursuivi par la recherche. Les données : • sont collectées pour des finalités déterminées, explicites et légitimes, et • ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. La finalité doit être en lien avec les missions ou les activités de l'établissement, de l'entité. Le traitement dans le cadre de la recherche scientifique doit être effectué dans un but légitime et ne pas porter atteinte aux droits et libertés fondamentaux des personnes concernées. La nécessité d'un tel traitement s'apprécie au regard de sa finalité, des risques auxquels la personne concernée pourrait être exposée, ainsi que les membres de sa famille s'il s'agit de recherche génétique. S'il s'avère impossible de déterminer la finalité du traitement dans le cadre de la recherche scientifique avant de commencer à collecter les données de santé, les personnes concernées sont autorisées à donner leur consentement pour chaque recherche séparément ou pour des parties déterminées de la recherche, chaque fois que la finalité du traitement le permet.	Cela exclut toute collecte de données au hasard ou à des fins préventives. Si la collecte obéit à plusieurs objectifs distincts, il est nécessaire de l'indiquer clairement pour permettre à la personne de comprendre la portée de l'accord qu'elle donne. Les participants à la recherche doivent être clairement informés de l'intention du responsable du traitement d'effectuer un traitement ultérieur des données personnelles pour une finalité autre que l'étude pour laquelle les données ont été initialement collectées. Il peut s'agir de recherches ultérieures dans le cadre d'une réutilisation secondaire de données/échantillons biologiques collectés. Il est important d'anticiper, faute de quoi une transmission de données personnelles ne sera possible que moyennant une nouvelle information des personnes. Cette information générale conditionne toute transmission de données personnelles en vue d'un autre traitement. Dans la note d'information initiale, penser à renvoyer vers un site internet, par exemple, auquel les personnes pourront se reporter pour ne pas avoir à informer de nouveau la personne avant la mise en œuvre d'un nouveau traitement.

	Réutilisation des données recueillies pour une finalité initiale à des fins de recherche scientifique ultérieures : Les informations recueillies pour une finalité peuvent être réutilisées pour poursuivre un autre objectif, à condition que cet objectif soit compatible avec la finalité initiale. La Loi organique n°63-2004 donne aux médecins la possibilité de communiquer les données à caractère personnel en leur possession, recueillies dans le cadre de la prise en charge médicale, à des personnes ou des établissements effectuant de la recherche scientifique dans le domaine de la santé, suite à une demande émanant de ces personnes ou établissements, et sur la base d'une autorisation de l'INPDP.	Les traitements ultérieurs à des fins de recherche scientifique sont présumés être compatibles avec la finalité initiale. **Point de vigilance :** Cela ne dispense pas pour autant du respect des autres conditions (licéité, minimisation, etc.), d'informer les personnes concernées et d'obtenir une autorisation, s'il y a lieu, pour le nouveau traitement mis en place.
Minimisation des données, pertinence et proportionnalité	**Ne collecter que les données strictement nécessaires.** Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.	Il n'est pas possible de collecter de données «au cas où», à titre préventif.
	Anonymiser, voire pseudonymiser les données dès que possible. Limiter au maximum les zones de commentaires libres et les questions ouvertes et privilégier les menus déroulants et les thesaurus existants. Si des zones de commentaires sont indispensables, documenter l'analyse et sensibiliser les personnes qui doivent les remplir sur les données pertinentes à y faire figurer.	
	Justifier systématiquement la pertinence de la collecte de données identifiantes (noms, prénoms, adresse postale ou électronique nominative) ou « sensibles » (données biométriques, par exemple).	
Exactitude des données	S'assurer que les données sont exactes et, si besoin mises à jour et, le cas échéant, supprimer les données obsolètes.	

Limitation de la conservation	Sauf si un texte juridique fixe une durée légale, définir une durée appropriée au regard de la finalité du traitement. Les données à caractère personnel ne peuvent pas être stockées sans limitation de durée et doivent, par principe, être archivées, détruites ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte. La fin de la durée de conservation des données ne coïncide pas nécessairement avec la durée de vie des données. Le cycle de conservation des données peut être divisé en trois étapes : la conservation des données en « **base active** » lorsqu'elles sont nécessaires à la réalisation des objectifs de la recherche. Elle est variable d'une recherche à l'autre en fonction du temps nécessaire à la réalisation des objectifs (temps nécessaire à la collecte, à l'analyse, et/ou au besoin de revenir aux données pour refaire les analyses après publication). C'est pourquoi cette durée doit être fixée en lien avec les scientifiques. **l'archivage intermédiaire** lorsque les données ne sont plus utilisées par les chercheurs mais présentent encore un intérêt administratif pour l'organisme. Les données sont conservées sur support distinct et sont consultées de manière ponctuelle et motivée. **l'archivage définitif** pour les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction.	
	Détruire, anonymiser ou archiver les données une fois l'objectif atteint par le projet de recherche.	Une conservation pour une durée plus longue dans l'intérêt de la recherche scientifique est possible. Par dérogation au principe de conservation limitée de données, une fois la finalité du traitement atteinte, il est possible de conserver des données à caractère personnel liées à la santé pour effectuer des recherches scientifiques, historiques ou statistiques, à condition que ces recherches répondent à un intérêt public et moyennant l'anonymisation de l'identité des personnes concernées. (Délibération n°4- Art. 10 de l'INPDP)

Sécurité des données	Mettre en œuvre des mesures organisationnelles visant à garantir un niveau de sécurité adapté au risque.	Limiter les destinataires, sensibiliser les destinataires, définir des habilitations, s'assurer que les personnes destinataires sont soumises à une obligation de confidentialité, choisir des sous-traitants présentant des garanties suffisantes, etc.
	Prendre toutes les dispositions pour protéger les données et empêcher qu'elles soient détournées ou réutilisées à des fins non prévues, pour respecter leur intégrité et leur confidentialité. Le niveau de sécurité doit être adapté au risque. L'article 13 de la Délibération n°4 de l'INPDP a déterminé les obligations liées à la sécurité. Le responsable du traitement des données à caractère personnel liées à la santé ou le sous-traitant doit prendre toutes les mesures nécessaires pour maintenir la sécurité de ces données et empêcher des tiers de les consulter, de les modifier, de les endommager ou de les détruire. En particulier, le responsable du traitement doit prendre les précautions suivantes : • ne pas placer les équipements et outils utilisés pour le traitement de ces données personnelles dans des circonstances ou des endroits permettant leur accès par des personnes non autorisées; • rendre impossible à toute personne non autorisée de consulter ces données, qu'elles soient contenues sur des supports écrits ou électroniques, de les copier, de les modifier ou de les transférer; • ne pas apporter des modifications à la plateforme de traitement sans avoir obtenu une autorisation de l'INPDP; • empêcher l'utilisation du système de traitement d'informations par des personnes non autorisées; • ne pas consulter les données, les copier, les modifier, les détruire ou les effacer lors de leur communication ou du transfert de leur support écrit ou électronique; • mettre en place une technique permettant la vérification ultérieure de l'identité des personnes ayant accédé au système d'informations, des données consultées et de l'historique de ces opérations;	Authentifier les utilisateurs, gérer les habilitations, tracer les accès et gérer les incidents, sécuriser les postes de travail et les supports mobiles, pseudonymiser, chiffrer les données, installer un antivirus, installer un pare-feu, sécuriser les échanges avec d'autres organismes, protéger les locaux, etc. Authentifier les utilisateurs Il est en particulier recommandé de définir un identifiant unique par utilisateur et d'interdire les comptes partagés entre plusieurs utilisateurs. Dans le cas d'une authentification basée sur des mots de passe, il est également conseillé de stocker les mots de passe de façon sécurisée. Ce qu'il faut éviter : • communiquer son mot de passe à autrui; • stocker ses mots de passe dans un fichier en clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes; • enregistrer ses mots de passe dans son navigateur sans mot de passe maître; • utiliser des mots de passe ayant un lien avec soi (nom, date de naissance, etc.); • utiliser le même mot de passe pour des accès différents; • conserver les mots de passe proposés par défaut; • s'envoyer par e-mail ses propres mots de passe; • créer ou utiliser des comptes partagés par plusieurs personnes; • accorder à un utilisateur plus de privilèges que nécessaire; • oublier de supprimer les comptes utilisateurs des personnes ayant quitté l'organisme ou ayant changé de fonction. Gérer les habilitations : Limiter les accès aux seules données dont un utilisateur a besoin. En pratique, il s'agit ainsi de circonscrire l'accès des utilisateurs aux seules données strictement nécessaires en fonction des tâches et domaines de responsabilité de chacun. Une attention particulière doit également être apportée à la suppression des permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à une ressource informatique ou un équipement, ainsi qu'à la fin de leur contrat.

- préserver les données par la création de copies de réserve sécurisées;
- vérifier chaque opération de mise à jour, d'effacement ou de communication effectuée sur les données, et établir des mesures spécifiques pour surveiller les données et leurs bases de données.

Article 14 de la Délibération n°4 de l'INPDP :

« Dans les cas mentionnés par l'article précédent, le système de traitement doit être soumis à un audit de la sécurité informatique et la demande d'autorisation présentée à l'Instance doit être jointe à une copie du rapport d'audit.
Le traitement des données à caractère personnel liées à la santé doit bénéficier de la protection nécessaire pour assurer la préservation des droits et libertés fondamentaux des personnes concernées par ces données.»
Les règles de cette protection sont régies par un cahier des charges émis par une décision commune entre l'INPDP, l'Agence nationale de la sécurité informatique et l'Instance nationale de l'évaluation et de l'accréditation en santé.
Ces règles sont revues périodiquement afin de permettre la mise en place des procédures et techniques adéquates pour protéger davantage les données personnelles, objet de traitement, contre toute opération susceptible de les endommager, les détruire illégalement ou de manière urgente, ou les perdre. Le système de traitement doit garantir un droit d'accès à ces données sécurisé par la prise de mesures de protection adéquates.
En outre, un système d'audit interne devrait être mis en place pour permettre le suivi de toutes les opérations d'accès aux bases de données et ses mises à jour, et pour identifier les personnes qui ont effectué ces opérations. »

Mesures de sécurité en cas d'hébergement de données : (Délibération n°4- Art. 16 de l'INPDP.)

Les données personnelles de santé sont sensibles, il est donc impératif de prendre des précautions spécifiques pour leur hébergement, notamment les suivantes :

Précautions à prendre :

- tracer les accès aux données et prévoir des procédures pour gérer les incidents;
- informer les utilisateurs de la mise en place d'un dispositif de journalisation;
- protéger son poste de travail et sécuriser l'informatique mobile;
- être équipé d'un antivirus régulièrement mis à jour;
- disposer de « pare-feu » (« *firewall* ») logiciel.
- prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.

	Précautions prises par le responsable du traitement : • interdire l'hébergement en dehors du territoire national; • l'hébergement sur le territoire national doit se faire exclusivement chez des hébergeurs agrées. L'hébergeur doit être qualifié et accrédité pour cette tâche en vertu d'une décision conjointe émise par l'INPDP, l'Agence nationale de la sécurité informatique et l'Instance nationale de l'évaluation et de l'accréditation en santé; • l'espace dédié au stockage et à l'archivage des dossiers médicaux doit être bien adapté et aménagé avec toutes les garanties de sécurisation des lieux et une limitation des accès; • mener des actions de sensibilisation d'envergure; • obtenir le consentement de la personne concernée; • organiser l'opération d'hébergement en vertu d'un contrat entre le responsable du traitement et l'hébergeur, qui doit être approuvé par l'INPDP. **Précautions prises par l'hébergeur :** • limiter l'accès aux données hébergées à la personne concernée ou à son représentant, et au responsable du traitement ou au sous-traitant; • n'utiliser les données par l'hébergeur que pour la finalité d'hébergement; • en cas de cessation d'activité, l'hébergeur doit restituer les données à caractère personnel liées à la santé au responsable du traitement, et il lui est interdit d'en conserver une copie; • l'hébergeur doit désigner un médecin inscrit au tableau de l'Ordre des médecins, qui sera responsable du maintien de la confidentialité des données personnelles objet d'hébergement et de la prise de décisions concernant l'accès des personnes concernées ou de leurs représentants à leurs données personnelles conformément aux termes du contrat d'hébergement et à la législation en vigueur.	
	Signaler les violations de données à l'INPDP dans les meilleurs délais.	
	Signaler, le cas échéant, les violations de données aux personnes concernées dans les meilleurs délais.	

Les informations à communiquer à la personne concernée en cas de recherche scientifique (Délibération n°4 - Art. 23 et 29 de l'INPDP) :

La personne concernée bénéficie d'un droit à une information préalable, transparente, claire et exacte autant que possible sur :

- l'identité du responsable du traitement et les données le concernant ainsi que celles du sous-traitant, le cas échéant ;
- la finalité du traitement et la base juridique ou contractuelle sur laquelle elle a été fondée ;
- la nature de la recherche scientifique à réaliser, les choix que cette recherche offre et les conditions les plus importantes de l'utilisation des données à caractère personnel liées à la santé, y compris les modalités de communication avec la personne concernée et de son information ;
- les organismes auxquelles les données sont transmises ;
- la durée et les conditions de conservation des données, y compris les modes d'accès et la possibilité de les publier ;
- les droits et garanties prévus par la loi qui sont les suivants :

    - droit d'accès : les conditions et les modalités d'exercice du droit d'accès aux données, les demandes de leur mise à jour ou de leur effacement
    - droit d'opposition de la personne concernée au traitement de ses données de santé
    - droit de rétraction à tout moment
    - droit de refuser l'utilisation de ses données à des fins de recherche scientifique

    Le rejet ou la rétraction n'est pas accepté dans les cas d'urgences sanitaires, mais les garanties fondamentales exigées pour l'opération de traitement sont conservées.

- la possibilité de traiter les données ultérieurement à une autre fin prévue par la loi et conformément aux dispositions de la délibération n°4 de l'INPDP ;
- les outils techniques utilisés pour traiter les données ;
- la possibilité de déposer une plainte auprès de l'INPDP en cas de litige sur le traitement des données.

En outre, il est recommandé d'ajouter :

- les catégories de données en particulier quand elles sont sensibles ;
- les transferts de données à l'étranger envisagés ;
- en cas de collecte indirecte, les catégories de données à caractère personnel concernées et leur provenance (par exemple le dossier médical) et si c'est le cas, si elles sont issues de sources publiques.

Pour approfondir :

- Guide de la CNIL « Traitement de données de santé : comment informer les personnes concernées ? »
- Guide RGPD du développeur

Un exemple de mentions d'information :

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier / un traitement par *[identité et coordonnées du responsable de traitement]* pour une recherche visant à *[finalités du traitement]*. La base légale du traitement est [*base légale du traitement*] et nécessite le traitement de vos données personnelles de santé à des fins de recherche scientifique.

À cette fin, les données suivantes vous concernant seront recueillies dans la mesure où ces données sont nécessaires à la recherche *[à adapter]* : données de santé issues du dossier médical, résultats d'analyses, données issues de questionnaires, données issues de l'assurance maladie, habitudes de vie, origines ethniques, données relatives à votre vie sexuelle…. Des échantillons biologiques seront recueillis selon les modalités suivantes *[à compléter s'il y a lieu]*

Ces données ne feront pas apparaître vos noms et prénoms mais seront associées à un code ou à un numéro d'ordre. Elles seront transmises à XXX *[à adapter en fonction des catégories de destinataires internes et externes à l'établissement de recherche XXX et des missions qui leurs sont dévolues]*.

Les informations concernant votre identité ne seront connues que de *[à adapter]* et conservées dans des conditions de nature à garantir leur confidentialité. Les données collectées seront communiquées aux seuls destinataires suivants : *[destinataires des données nominatives / destinataires des données pseudonymisées le cas échéant]*.

Les données seront conservées pendant *[durée de conservation des données prévue par le responsable du traitement ou critères permettant de la déterminer avec suffisamment de précisions (ex : X années après la dernière publication scientifique, dont l'organisme indique une date projetée)]*.

Vos données seront hébergées auprès de (*[à adapter]* et accessibles aux seules personnes habilitées à les connaitre pour le besoin de leurs missions dans le cadre de la recherche scientifique (chargés des analyses, médecins, chercheurs, etc.)

Vous pouvez obtenir communication des données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données. Vous pouvez retirer à tout moment votre consentement au traitement de vos données. Vous pouvez également vous opposer au traitement de vos données.
Si vous souhaitez exercer ces droits et obtenir communication des informations vous concernant, vous pouvez vous adresser au médecin qui vous suit dans le cadre de la recherche et qui connaît votre identité.

Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez contacter (*le cas échéant*, notre délégué à la protection des données (DPO) ou le service chargé de l'exercice de ces droits) : *[électronique, postale, coordonnées téléphoniques, etc.]*

Si vous estimez, après nous avoir contactés, que vos droits ne sont pas respectés, vous pouvez adresser une réclamation à l'INPDP (Adresse : http://www.inpdp.nat.tn et adresse mail : inpdp@inpdp.tn).

V. QUELLES SONT VOS OBLIGATIONS DÉCLARATIVES ?

Les organismes légalement habilités à mener des recherches en santé humaine doivent s'assurer que la recherche scientifique respecte **les principes fondamentaux de la protection des données à caractère personnel** tels que cités précédemment. En outre, ils doivent effectuer une **demande d'autorisation auprès de l'INPDP** (1), et réaliser une analyse d'impact relative à la protection des données dès lors que le traitement des données de santé est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (2).

1. Accomplir une formalité préalable particulière auprès de l'INPDP pour le traitement des données de santé dans le cadre de la recherche scientifique

Tout traitement de données à caractère personnel liées à la santé est soumis, en plus de la déclaration de traitement, à une **autorisation de traitement des données de santé** préalables de l'Instance.

Textes juridiques :

- Articles 7 et 14 de la Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
- Dispositions du Décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel
- Article 8 de la Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

Le formulaire d'autorisation de traitement des données de santé doit être accompagné, suivant les situations spécifiques du traitement, d'une copie des documents suivants :

- dépôt de la demande ou de la décision de la Direction de la pharmacie et du médicament du ministère de la santé quand la réglementation soumet ce traitement de données à cette procédure
- décision du comité d'éthique sectoriel concernant le programme de recherche médicale
- dépôt de la demande d'autorisation ou de la décision du Comité de protection des personnes (CPP)
- dossier de recherche clinique médicale comprenant :
  un résumé du protocole de la recherche clinique
  le cahier d'observation électronique
  le contrat avec le promoteur et les investigateurs
- formulaire d'information des patients
- formulaire du recueil du consentement éclairé
- lettre d'information des employés sur le traitement des données personnelles de santé par la structure de gestion en interne (Ressources humaines)
- charte éthique à l'intention du personnel ayant à traiter les données personnelles portant sur les obligations du respect du secret professionnel, du respect des normes de sécurité et de confidentialité des données.

En outre, les médecins responsables du traitement des données de santé sont autorisés à communiquer ces données à des personnes ou institutions effectuant des recherches scientifiques ou des statistiques dans le domaine de la santé, et **cette communication est soumise à une autorisation préalable de l'Instance**. (Délibération n°4- Art. 28)

Pour approfondir :

- Consulter le manuel de procédures émis par l'INPDP
- Consulter les formulaires de l'INPDP à remplir : http://www.inpdp.nat.tn/formulaires.html

2. Réaliser une analyse d'impact relative à la protection des données (AIPD)

Lorsque le traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (dommage physique, dommage moral, perte d'emploi, refus d'un prêt ou d'une assurance, etc.), le responsable de traitement doit mener une analyse d'impact des opérations de traitement sur la protection des données.

L'analyse d'impact est un outil d'évaluation qui doit permettre de vérifier le respect des principes fondamentaux de la protection des données personnelles et la bonne gestion des risques liés à la sécurité des données. Elle permet au responsable de traitement de disposer d'une preuve du respect de ses obligations concernant la conception du traitement.

Les risques qui sont analysés sont les risques pour la personne résultant de la mise en œuvre d'un traitement (dommages physiques, matériels, préjudice moral tels que discrimination, vol, usurpation d'identité, perte financière, atteinte à la réputation…) et non les risques pour l'organisme en cas de non-conformité.

Une AIPD peut concerner un seul traitement ou un ensemble de traitements similaires.

L'analyse d'impact est nécessaire pour les traitements les plus à risques. Il est de bonne pratique de réaliser une telle analyse dans le cadre des activités de recherche dans le domaine de la santé. C'est particulièrement le cas pour :

- les recherches médicales portant sur des personnes vulnérables (patients, salariés, personnes âgées, enfants, personnes faisant l'objet de mesures de protection judiciaire, etc.) et incluant le traitement de leurs données génétiques;

- la constitution d'un registre ou d'une base de données de santé à grande échelle (entrepôt de données ou collection d'échantillons biologiques) pour utilisation à des fins de recherches ultérieures.

Que contient une analyse d'impact ?

- **Une présentation claire et synthétique du traitement**

Vue d'ensemble du traitement de données à caractère personnel

Présenter de façon synthétique la finalité, le contexte, les enjeux de santé publique de l'étude en mentionnant les éventuels soutiens dont bénéficie le projet (financiers, associations de patients…) et les avis éthiques et scientifiques favorables au projet s'il en existe.

Cycle de vie des données

Présenter de façon synthétique

- les données personnelles concernées, leurs destinataires et leur durée de conservation, une description des processus et des supports de données pour l'ensemble du cycle de vie des données depuis leur collecte jusqu'à leur effacement;
- une évaluation plus juridique de la nécessité et de la proportionnalité du traitement au regard des principes généraux de la protection des données;
- une évaluation plus technique des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) et de leurs impacts potentiels sur la vie privée.

Quand et comment réaliser une analyse d'impact ?

Une analyse d'impact doit être réalisée **avant la mise en place** d'un nouveau traitement de données et doit être mise à jour tout au long du traitement, à l'occasion notamment d'une évolution significative.
La réalisation d'une analyse d'impact nécessite **la collaboration étroite de tous les opérateurs concernés par le traitement** : les métiers (maîtrise d'ouvrage), les équipes chargées de la mise en œuvre (maîtrise d'œuvre), les services chargés d'apporter un appui réglementaire ou technique, les partenaires et les sous-traitants qui doivent fournir leur aide et les informations nécessaires à la réalisation de l'AIPD.
Les résultats de l'analyse d'impact doivent être adressés pour avis à un responsable informatique et au DPO pour validation, si un DPO a été désigné. Si le rapport d'analyse montre un **risque résiduel** élevé, c'est au responsable de traitement que revient la responsabilité d'accepter les risques au vu des avis émis.

L'avis des personnes concernées ou de leurs **représentants** (association de patients…) peut être documenté. Cet avis peut être recueilli par différents moyens en fonction du contexte (par le biais d'une enquête, d'un sondage, d'une question formelle, de la participation des patients à la gouvernance du projet).

Pour tout conseil sur la réalisation de l'analyse d'impact, n'hésitez pas à contacter le DPO.

Pour approfondir :

- La CNIL propose différents outils tels que des guides méthodologiques ainsi qu'un logiciel open source d'aide à la rédaction des AIPD, disponibles sur son site web.
- L'ensemble des outils développés par la CNIL (guide, infographie, délibérations, logiciel)
- Le logiciel développé par la CNIL
- CNIL, Les bases de connaissances PIA
- Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise
- Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD), modifiées et adoptées le 4 octobre 2017.
- FAQ de la CNIL sur les Guidelines PIA

VI. LES TRANSFERTS DE DONNÉES DE SANTÉ À L'ÉTRANGER

1. Définition du transfert de données hors la Tunisie

On parle de transfert de données hors la Tunisie lorsque les données sont transférées depuis le territoire tunisien vers un ou plusieurs pays étranger.

Le transfert peut s'effectuer par communication, copie ou déplacement de données ou par un accès à distance à une base de données située en Tunisie. Il n'est donc pas nécessaire qu'il y ait un déplacement physique des données pour qu'il y ait transfert, au sens de la réglementation en vigueur.

Cette situation est susceptible de s'appliquer dans le cadre d'une réutilisation, que le récipiendaire des données qui se trouve hors la Tunisie soit un sous-traitant ou un autre responsable d'un traitement.

2. Encadrement des transferts de données personnelles hors la Tunisie

Textes juridiques :

Le transfert des données personnelles à l'étranger est réglementé par :

•la Loi organique n° 2004-63 (Articles 50, 51 et 52)

- Article 50. Loi 2004-63 : « Il est interdit, dans tous les cas, de communiquer ou de transférer des données à caractère personnel vers un pays étranger lorsque ceci est susceptible de porter atteinte à la sécurité publique ou aux intérêts vitaux de la Tunisie. »

- Article 51. Loi 2004-63 : « Le transfert vers un autre pays des données personnelles faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si ce pays assure un niveau de protection adéquat apprécié au regard de tous les éléments relatifs à la nature des données à transférer, aux finalités de leur traitement, à la durée du traitement envisagé, et le pays vers lequel les données vont être transférées ainsi que les précautions nécessaires mises en œuvre pour assurer la sécurité des données. Dans tous les cas, le transfert des données à caractère personnel doit s'effectuer conformément aux conditions prévues par la présente loi. »

- Article 52. Loi 2004-63 : « Dans tous les cas, l'obtention de l'autorisation de l'Instance pour effectuer le transfert des données à caractère personnel vers l'étranger est obligatoire. L'Instance doit statuer sur la demande d'autorisation dans un délai maximum d'un mois à partir de la présentation de la demande.

  Lorsque les données à caractère personnel à transférer concernent un enfant, la demande est présentée au juge de la famille. »

• la Délibération n°3 du 5 septembre 2018 de l'INPDP portant identification des États ayant un niveau de protection adéquat en matière de protection des données personnelles.

• la Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé (Art.21)

- Article 21 : « Outre le consentement de la personne concernée, le transfert à l'étranger des données à caractère personnel liées à la santé est soumis à une autorisation préalable de l'Instance qui prend sa décision en fonction du respect de deux conditions, à savoir:
  - o le pays vers lequel le transfert sera effectué est inclus dans la liste déterminée par la délibération de l'Instance, et qui assure un niveau approprié de protection des données à caractère personnel.
  - o la finalité du traitement de ces données nécessite ce transfert. »

Les transferts de données de santé dans le domaine de la recherche scientifique hors de la Tunisie sont interdits. Les données de santé ne peuvent être traitées qu'en Tunisie. Toutefois, l'activité de recherche scientifique est par essence internationale, comme en atteste la pandémie de covid-19.

Exceptionnellement et en cas de transferts de données de santé à l'étranger, ces transferts doivent respecter des garanties de fond et de procédures.

3. Conditions de transferts des données de santé à l'étranger

Condition n°1 : Transferts vers un pays adéquat

Le transfert de données à l'étranger ne peut s'effectuer que vers un pays disposant d'un niveau de protection adéquat.

L'INPDP a publié la liste des pays ayant un niveau de protection adéquat dans sa

Délibération n°3 du 5 septembre 2018 portant identification des États ayant un niveau de protection adéquat en matière de protection des données personnelles.

En outre, s'il est envisagé de transférer des données de santé vers un autre pays que ceux mentionnés dans la liste précitée, et pour ne pas bloquer les recherches envisagées, l'INPDP fera un examen au cas par cas, à l'occasion de l'instruction des demandes d'autorisation qui lui seront soumises, des garanties offertes par ce pays et statuera sur l'équivalence de protection.

Cette appréciation sera effectuée au regard des éléments relatifs à :

- la nature des données à transférer,
- les finalités de leur traitement,
- la durée du traitement envisagé,
- les précautions nécessaires mises en œuvre pour assurer la sécurité des données.

Dans le cas où il est envisagé de transférer les données vers un pays non adéquat, des garanties appropriées doivent être mises en place pour rétablir une équivalence de protection :

- des mesures contractuelles encadrant le transfert,
- des mesures techniques, telles que la pseudonymisation ou le chiffrement des données,
- des mesures de transparence et d'information à l'égard des personnes concernées mentionnant les pays destinataires et les garanties qui encadrent le transfert.

Condition n°2 : Accomplissement d'une formalité préalable auprès de l'INPDP

Dans tous les cas, le transfert des données de santé dans le cadre de la recherche scientifique est soumis à une autorisation de transfert à l'étranger suite à une demande déposée auprès de l'INPDP.

La demande d'autorisation doit être accompagnée des documents suivants :

une copie des conditions générales de protection des données avec le partenaire étranger,
une preuve de l'information des personnes concernées sur le transfert de leurs données à l'étranger,
les modalités de recueil du consentement des personnes concernées qui laisse une trace écrite

Pour approfondir :

- Consulter le manuel de procédures de l'INPDP
- Le guide de la CNIL « Transfert de données hors de l'UE : le cadre général prévu par le RGPD » (liste l'ensemble des solutions et renvoie vers d'autres guides spécifiques à chacune)
- Le guide de la CNIL « Clauses contractuelles types de la Commission européenne »
- Le guide de la CNIL « Transfert de données hors UE – dérogations pour des situations particulières »
- Les recommandations du CEPD n°01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE du 10 novembre 2020 (version ouverte à la consultation)
- Les recommandations du CEPD n°02/2020 sur les garanties essentielles européennes pour les mesures de surveillance du 10 novembre 2020 (version ouverte à la consultation)
- Les recommandations du CEPD n°02/2018 sur les dérogations de l'article 49 du 25 mai 2018 et n°03/2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19 du 21 avril 2020 (en particulier, points 58 et suivants)

RÉFÉRENCES "POUR APPROFONDIR"

http://www.inpdp.nat.tn/Liens_recherche.pdf

TEXTES ET RÉFÉRENCES LÉGISLATIFS

http://www.inpdp.nat.tn/Liens_rech_textes.pdf

Instance nationale de protection des données personnelles (INPDP)
Adresse : 1, Rue Mohamed Moalla, 1002, Mutuelleville, Tunis B.P. 525
Tél. : 71 799 853 / 71 799 711
Fax : 71 799 823
inpdp@inpdp.tn