TRAITEMENT DE DONNÉES PROVENANT DE DOSSIERS DE PATIENTS

Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration

DOS-2019-04611

OBJET

1. La Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration (ci-après la ministre) sollicite le point de vue de l'Autorité de protection des données (ci-après l'APD) au sujet de plusieurs questions relatives au traitement de données à caractère personnel concernant la santé, plus précisément :

- le traitement primaire de données du dossier du patient et, en particulier, le partage de données entre professionnels des soins de santé (articles 36 à 40 de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé*)
- le traitement secondaire de données du dossier du patient ;
    - en vue de la recherche scientifique et de finalités dans le cadre de la santé publique ;
    - en vue de l'évaluation de la qualité des soins ;
- le traitement de données de santé dans le cadre d'essais cliniques.

EXAMEN DES QUESTIONS

1. Traitement primaire de données du dossier du patient et partage de données entre professionnels des soins de santé

2. Le 14 mai 2019, la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé* (ci-après la loi du 22 avril 2019) a été publiée au Moniteur belge. En vertu de son article 88, cette loi entre en principe en vigueur le 1er juillet 2021. La ministre sollicite le point de vue de l'Autorité au sujet d'une application de cette loi en conformité avec le RGPD[1], en particulier de ses articles 36 et suivants, concernant l'accès aux données de santé.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

3. Ainsi, la ministre interroge l'APD sur le traitement, d'une part, et le partage entre professionnels des soins de santé[2], d'autre part, de données de santé dans le cadre des soins (de santé)[3], plus particulièrement concernant :

- la portée du consentement dont il est question aux articles 36 et suivants de la loi du 22 avril 2019 ;
- la mise en œuvre technique de droits d'accès de professionnels des soins de santé dans des systèmes électroniques et télématiques.

4. L'article 36 de la loi du 22 avril 2019 dispose ce qui suit : "*Le professionnel des soins de santé a accès aux données à caractère personnel relatives à la santé du patient qui sont tenues à jour et conservées par d'autres professionnels des soins de santé à condition que le patient ait préalablement donné son* ***consentement éclairé*** *concernant cet accès.*
Lors de l'octroi du consentement visé à l'alinéa 1er, le patient peut ***exclure certains professionnels des soins de santé****.*
Le ***Roi*** *peut définir les modalités relatives au consentement visé à l'alinéa 1er*."

5. L'article 37 de la loi du 22 avril 2019 dispose ce qui suit : *"Le professionnel des soins de santé a uniquement accès aux données à caractère personnel relatives à la santé des patients avec lesquels il entretient une* ***relation thérapeutique****.*
Pour l'application de l'alinéa 1er, on entend par relation thérapeutique toute relation entre un patient et un professionnel des soins de santé dans le cadre de laquelle ***des soins de santé*** *sont dispensés.*
Le ***Roi*** *peut, avec indication des cas spécifiques d'échange de données à caractère personnel relatives à la santé du patient, désigner les catégories de professionnels des soins de santé qui, malgré le fait qu'en application de l'alinéa 2, ils entretiennent une relation thérapeutique avec le patient, n'ont pas accès à l'échange des données visées.*"

6. L'article 38 de la loi du 22 avril 2019 dispose ce qui suit : "*Le professionnel des soins de santé qui entretient une relation thérapeutique avec le patient, a uniquement accès aux données à caractère personnel relatives à la santé de ce patient dans le respect des* ***conditions*** *suivantes :*
1° la finalité de l'accès consiste à dispenser des soins de santé ;
2° l'accès est nécessaire à la continuité et à la qualité des soins de santé dispensés ;
3° l'accès se limite aux données utiles et pertinentes dans le cadre de la prestation de soins de santé."

---

[2] En vertu de l'article 2.2° de la loi du 22 avril 2019, il convient d'entendre par là : "*le praticien professionnel visé dans la loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé ainsi que le praticien d'une pratique non conventionnelle visée dans la loi du 29 avril 1999 relative aux pratiques non conventionnelles dans les domaines de l'art médical, de l'art pharmaceutique, de la kinésithérapie, de l'art infirmier et des professions paramédicales.*"

[3] En vertu de l'article 2.3° de la loi du 22 avril 2019, il convient d'entendre par là : "*les services dispensés par un professionnel des soins de santé en vue de promouvoir, de déterminer, de conserver, de restaurer ou d'améliorer l'état de santé d'un patient, de modifier son apparence corporelle à des fins principalement esthétiques ou de l'accompagner en fin de vie.*"

7. L'article 39 de la loi du 22 avril 2019 dispose ce qui suit : "*Lorsque, dans un **cas d'urgence**, il y a incertitude quant au consentement du patient concernant l'accès du professionnel des soins de santé aux données à caractère personnel relatives à la santé du patient, le professionnel des soins de santé, en vue de dispenser les soins de santé nécessaires dans l'intérêt du patient, a accès aux données visées dans le respect des conditions visées aux articles 37 et 38.*"

8. L'article 40 de la loi du 22 avril 2019 dispose ce qui suit : "*Le professionnel des soins de santé qui tient à jour et conserve les données personnelles relatives à la santé du patient prend les mesures nécessaires afin que **le patient puisse contrôler quelles personnes ont ou ont eu accès** à ses données personnelles relatives à la santé.*"

a. Portée du "consentement éclairé" au sens des articles 36 e.s. de la loi du 22 avril 2019 et du RGPD

9. La ministre veut savoir de quelle manière (spécifique) ce consentement éclairé doit être organisé, en particulier dans le cadre d'un partage de données dans un environnement hospitalier où un nombre potentiellement élevé de professionnels des soins de santé voudront accéder directement, dans le contexte d'une relation thérapeutique, aux informations de santé disponibles auprès d'autres prestataires de soins.

10. À l'article 4.11) du RGPD, le "consentement" est défini comme suit : *"toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement".* Selon l'article 7.3 du RGPD, "*la personne concernée a le droit de retirer son consentement à tout moment*".

11. À cet égard, les "*Lignes directrices sur le consentement au sens du règlement 2016/679*" (WP 259), rédigées par le Groupe de travail Article 29 sur la protection des données et révisées et établies pour la dernière fois le 10 avril 2018, peuvent servir de fil conducteur.

12. En ce qui concerne la portée du consentement aux articles 36 et suivants de la loi du 22 avril 2019, les éléments suivants attirent l'attention :

- L'Exposé des motifs précise notamment pour l'article 36 que : "*il ne s'agit pas d'un consentement dans le cadre duquel les professionnels de santé bénéficiant d'un accès sont désignés par le patient individuel. En revanche, le texte prévoit expressément que le patient peut exclure certains professionnels des soins de santé lorsqu'il donne son consentement.*" Cela semble suggérer que le consentement est en réalité plutôt un consentement général du fait que les données du patient peuvent être partagées avec d'autres professionnels des soins

de santé, à l'exception de ceux que le patient exclut expressément. L'intervention du Roi prévue en la matière pour fixer les modalités relatives au consentement n'est que facultative ("*Le Roi peut définir les modalités relatives au consentement visé à l'alinéa 1er.*").

- À l'article 37 de la loi du 22 avril 2019, le droit d'accès, qui est soumis au consentement précité, est réservé aux professionnels des soins de santé qui ont une relation thérapeutique avec le patient concerné, l'Exposé des motifs précisant certes que les termes "relation thérapeutique" doivent être compris dans un sens très large : *"La relation peut être de nature diagnostique, curative, préventive ou palliative, mais, par exemple, la médecine d'entreprise, la médecine des assurances et la médecine de contrôle relèvent en principe également de la définition de la relation thérapeutique.*" Le dernier alinéa prévoit toutefois que le Roi peut désigner des catégories de professionnels des soins de santé qui, en dépit d'une relation thérapeutique, sont quand même exclus du droit d'accès (l'Exposé des motifs se réfère à cet égard à l'exclusion de la médecine des assurances, la médecine de contrôle et la médecine légale qui établissent uniquement un diagnostic et qui n'agissent pas préventivement ni au niveau curatif). L'intervention du Roi est toutefois également facultative dans ce cas.
- À l'article 38 de la loi du 22 avril 2019, le droit d'accès d'un professionnel des soins de santé ayant une relation thérapeutique est en plus soumis aux conditions suivantes :
  - la finalité de l'accès consiste à dispenser des soins de santé ;
  - l'accès est nécessaire à la continuité et à la qualité des soins de santé dispensés ;
  - l'accès se limite aux données utiles et pertinentes dans le cadre de la prestation de soins de santé.

  Ces conditions s'inspirent manifestement des conditions associées à la forme juridique du "secret professionnel partagé", à la différence certes que dans la loi du 22 avril 2019, la notion de "soins de santé" est définie de manière très large, alors que le secret professionnel partagé semble toutefois limité au partage de secrets/d'informations nécessaires à la prestation et uniquement dans l'intérêt (de l'assistance) du patient concerné[4].
- Il n'y a aucune indication de la durée d'une relation thérapeutique ; combien de temps dure-t-elle après le contact/la consultation avec le patient ?

13. Il en résulte qu'un encadrement/une limitation supplémentaire du droit d'accès par un professionnel des soins de santé aux données tenues à jour et conservées par un autre professionnel des soins de santé s'impose quoi qu'il en soit, tant dans des arrêtés d'exécution à prendre que dans la mise en application de ceux-ci sur le terrain (mise en œuvre et intégration dans le dossier électronique du patient, associées à une notification qui est faite au patient concerné préalablement au consentement éclairé), et ce au moins en ce qui concerne les points suivants :

[4] La référence au partage de données "en vue de défendre les intérêts du patient", qui était encore reprise comme condition à l'article 39 (actuel article 38 de la loi du 22 avril 2019) de l'avant-projet de loi *relatif à la qualité de la pratique des soins de santé* tel que soumis à l'avis de l'Autorité de protection des données (avis n° 100/2018), a disparu de la version définitive de l'article 38.

- la finalité : prestation de soins préventifs/curatifs dans l'intérêt du patient par opposition aux soins de santé purement diagnostiques dans le cadre de la médecine des assurances, la médecine de contrôle et la médecine légale ; ces derniers soins de santé devant être exclus ;
- les modalités d'accès/d'exclusion : possibilité d'exclure/d'autoriser nominativement des professionnels des soins de santé, mais aussi d'exclure/d'autoriser des catégories[5] de professionnels des soins de santé (en prêtant attention à la validité dans le temps de l'accès, liée à la durée de la relation thérapeutique) ;
- les instructions éventuelles concernant la notification qui doit précéder le consentement éclairé du patient concerné, afin que le "patient moyen attentif/formé" sache parfaitement à quoi il consent et qu'il puisse également le faire en toute liberté[6].

14. Un refus de partage de données dans le secteur des soins de santé ne peut bien entendu pas porter préjudice au droit à des soins de qualité. L'absence d'accès à des informations de santé enregistrées précédemment concernant le patient n'empêche pas pour autant un professionnel des soins de santé exclu de prodiguer des soins de santé. L'exclusion de professionnels des soins de santé telle que prévue dans la loi du 22 avril 2019 se limite en effet à une exclusion d'accès à des données de santé du patient qui ont été enregistrées par d'autres prestataires de soins, mais n'empêche nullement le professionnel des soins de santé "exclu" de prodiguer des soins de santé et d'enregistrer/traiter lui-même les données de santé nécessaires en la matière. L'exclusion de professionnels des soins de santé conformément à l'article 36, deuxième alinéa de la loi du 22 avril 2019 ne doit donc en aucun cas perturber le bon fonctionnement de l'hôpital, et encore moins empêcher la dispense de soins.

15. Enfin, l'APD souligne avec insistance qu'une **intervention du Roi**, telle que prescrite de manière facultative aux articles 36 et 37 de la loi du 22 avril 2019, est réellement **indispensable** pour les points susmentionnés afin d'une part, de préciser la concrétisation/granularité du consentement et d'autre part, d'éviter à tout le moins que des professionnels des soins de santé qui agissent dans le cadre de la médecine des assurances, la médecine de contrôle et la médecine légale aient accès à un dossier de patient qui sert en effet essentiellement une finalité préventive/curative et non une finalité purement diagnostique (où ce n'est généralement pas l'intérêt du patient qui est visé) ; ces deux finalités distinctes sont tout à fait incompatibles à la lumière du principe de limitation des finalités. Ce point de

[5] L'article 13 du RGPD (concernant la notification) ainsi que l'article 9 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (concernant les mesures de sécurité) parlent aussi de "catégories de destinataires/de personnes".

[6] Un consentement libre implique un choix réel et un contrôle pour la personne concernée, sans conséquences négatives si l'on ne donne pas son consentement ou si on le retire. Un refus de partage de données dans le secteur des soins de santé ne peut en effet pas porter préjudice au droit à des soins de qualité. Dans le contexte des soins, il convient à cet égard d'accorder l'attention nécessaire à un éventuel déséquilibre entre les professionnels des soins de santé et le patient.

vue a déjà été confirmé explicitement dans ce contexte dans une recommandation de l'ancien Comité sectoriel de la Sécurité Sociale et de la Santé, section Santé[7].
L'APD rappelle la nécessité d'être consultée préalablement au sujet de ces arrêtés d'exécution, conformément à l'article 23 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*.

b. Mise en œuvre technique de droits d'accès dans des systèmes électroniques et télématiques – "Privacy by design" et "by default"

16. Étant donné que le traitement de données de patients implique le traitement de données de santé sensibles, le responsable du traitement devra, au niveau de la sécurité de l'information, respecter :

- non seulement les mesures techniques et organisationnelles habituelles (voir l'article 32 du RGPD)[8] – qui doivent assurer un niveau de sécurité approprié compte tenu d'une part, de l'état des connaissances et des coûts de mise en œuvre des mesures et d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels – parmi lesquelles :
  - la pseudonymisation et le chiffrement des données à caractère personnel ;
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes de traitement ;
  - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
  - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement
- mais aussi l'article 9 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, plus précisément :
  - désigner les catégories de personnes qui ont accès aux données à caractère personnel ainsi que leur qualité ;
  - tenir la liste des catégories des personnes ainsi désignées à la disposition de l'Autorité de protection des données ;

[7] Voir la recommandation n° 17/01 du 16 mai 2017 *relative à l'incompatibilité entre le rôle de prestataire de soins ayant une relation thérapeutique et le rôle de médecin-conseil, contrôleur ou expert à la demande d'un tiers à l'égard du même patient* (voir : https://www.ehealth.fgov.be/ehealthplatform/fr/comite-sectoriel/documents).

[8] Pour la mise en œuvre concrète de ces mesures, on peut faire référence à la recommandation de la Commission de la protection de la vie privée visant à prévenir les fuites de données (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf) et aux mesures de référence de la Commission de la protection de la vie privée qui devraient être prises en considération lors de chaque traitement de données à caractère personnel (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf).

- veiller à ce que les personnes ainsi désignées soient tenues au respect du caractère confidentiel des données.

17. Les "Mesures de référence" en matière de sécurité applicables à tout traitement de données à caractère personnel, auxquelles il est fait référence dans la note de bas de page 24, évoquent notamment la "sécurisation logique des accès" et la mise en œuvre de "mécanismes de journalisation et de traçage". Une institution doit ainsi notamment s'assurer que les données à caractère personnel ne soient accessibles, en fonction de leur classification, que pour les personnes (et logiciels d'application) qui ont été expressément autorisées à cet effet. Cela implique la mise en œuvre d'une bonne gestion des utilisateurs et des accès[9].

18. La mise en œuvre d'un mécanisme pour le contrôle et la surveillance (a posteriori) de l'accès effectif à un dossier de patient est également nécessaire, en particulier lorsque des droits d'accès et d'utilisateur définis au préalable peuvent être "violés/annulés" par des professionnels des soins de santé. Comme pour chaque traitement de données à caractère personnel, un tel mécanisme de contrôle devra être déployé en respectant les principes de protection des données de l'article 5 du RGPD (licite, transparent, lié à une finalité et proportionnel). Il va de soi qu'un travailleur/prestataire de soins conserve (une partie de) sa vie privée sur le lieu de travail mais cela ne signifie pas que l'employeur ne peut exercer aucun contrôle sur ce travailleur[10].

19. L'article 40 de la loi du 22 avril 2019 dispose aussi expressément que le professionnel des soins de santé qui conserve des données de patients prend les mesures nécessaires afin que le patient puisse contrôler quelles personnes ont ou ont eu accès à ses données de santé.

20. Bien que la réglementation n'ait jamais été aussi claire sur ce point auparavant[11], l'accès pour le patient à l'identité de celui qui a eu accès à son dossier a toutefois déjà été recommandé en tant que bonne pratique et moyen efficace dans le cadre d'une confiance (légitime) du patient dans le traitement de ses données de santé[12].

21. L'article 12.1 du RGPD précise que le responsable du traitement (en l'occurrence l'hôpital) prend les mesures appropriées pour fournir à la personne concernée toute information visée notamment à

---

[9] Voir également la recommandation de la Commission de la protection de la vie privée n° 01/2008 du 24 septembre 2008 *relative à la gestion des accès et des utilisateurs dans le secteur public* (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2008_0.pdf).

[10] Voir également concernant ce thème : https://www.autoriteprotectiondonnees.be/la-vie-privee-sur-le-lieu-de-travail.

[11] Ainsi, l'article 15 du RGPD prévoit un droit d'accès pour la personne concernée notamment au sujet : "[des] *destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées*".

[12] Voir à cet effet la recommandation n° 11/01 du 19 avril 2011 de l'ancien Comité sectoriel de la Sécurité Sociale et de la Santé *relative au droit d'accès du patient aux destinataires de son dossier médical* (https://www.ehealth.fgov.be/ehealthplatform/fr/comite-sectoriel/documents) ainsi que l'avis de la Commission fédérale "Droits du patient" du 21 novembre 2017 relatif au dossier patient (https://organesdeconcertation.sante.belgique.be/fr/documents/20171121-avis-le-dossier-patient).

l'article 15 du RGPD (c'est-à-dire le droit d'accès) d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

22. Les nouveaux principes de "privacy by design" et de "privacy by default" instaurés par l'article 25 du RGPD sont également clairs à cet égard :

"*1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.*
2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.
3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément attestant du respect des exigences énoncées aux paragraphes 1 et 2 du présent article."

23. Il appartient donc au responsable du traitement d'utiliser les systèmes de télématique et/ou les logiciels de dossiers de patients qui permettent la mise en œuvre des garanties et principes en matière de protection des données ainsi que la garantie des droits des personnes concernées, dont l'accessibilité des données[13].

24. L'APD souhaite rappeler ici l'article 35 du RGPD : le responsable du traitement effectue une analyse d'impact relative à la protection des données lorsqu'un traitement - par le recours à de nouvelles technologies - est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, compte tenu de la nature, de la portée, du contexte et des finalités du traitement. Une telle analyse est même requise (notamment) dans le cas d'un traitement à grande échelle de catégories particulières de données à caractère personnel, dont les données de santé. Le dossier électronique du

[13] Voir : Guidelines 4/2019 on Article 25 Data Protection by Design and by Default du Comité Européen de la Protection des Données (EDPB), adoptées le 13 novembre 2019.

patient dans un hôpital devra communément être qualifié de traitement à grande échelle de données de santé sensibles.

2. Traitement secondaire de données du dossier du patient

25. La ministre s'interroge notamment sur le fondement juridique dans le cadre d'un traitement ultérieur de données du dossier du patient à des fins de recherche scientifique, d'une part, et d'évaluation de la qualité des soins, d'autre part.

2.1. Traitement secondaire de données du dossier du patient à des fins de recherche scientifique

a. Base juridique

26. Tout comme la Directive européenne 95/46 et l'ancienne loi vie privée[14], le RGPD, en son article 5.1.b), ne considère pas non plus le traitement ultérieur de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique[15] ou historique ou à des fins statistiques[16] comme incompatible avec les finalités initiales, à condition que l'article 89.1 du RGPD soit respecté. Le considérant 50 du RGPD confirme en la matière explicitement qu'un tel traitement ultérieur doit être considéré comme une opération de traitement licite compatible avec les finalités initiales. Le considérant 50 stipule également que dans le cas d'un traitement ultérieur compatible, aucune base juridique distincte n'est requise.

27. Cela implique donc que pour le traitement ultérieur de données de patients à des fins de recherche scientifique, on ne doit pas chercher un fondement juridique (complémentaire) dans les articles 6.1 et 9.2 du RGPD, comme par exemple le consentement explicite des patients concernés. Cela semble répondre aux préoccupations du monde académique selon lesquelles la nécessité d'une

---

[14] Loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*.

[15] Le considérant 159 du RGPD dispose notamment ce qui suit : *"Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé.* (…)*Par «fins de recherche scientifique», il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique. Pour répondre aux spécificités du traitement de données à caractère personnel à des fins de recherche scientifique, des conditions particulières devraient s'appliquer, en particulier, en ce qui concerne la publication ou la divulgation d'une autre manière de données à caractère personnel dans le cadre de finalités de la recherche scientifique. Si le résultat de la recherche scientifique, en particulier dans le domaine de la santé, justifie de nouvelles mesures dans l'intérêt de la personne concernée, les règles générales du présent règlement s'appliquent à l'égard de ces mesures.*

[16] Le considérant 162 du RGPD dispose notamment ce qui suit : *"Par « fins statistiques », on entend toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques. Ces résultats statistiques peuvent en outre être utilisés à différentes fins, notamment des fins de recherche scientifique . Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier.*"

demande complémentaire de consentement pour une réutilisation de données de patients pourrait faire obstacle à la recherche scientifique.

28. En outre, un consentement, qui par définition peut être retiré à tout moment, ne semble pas toujours constituer la base juridique la plus stable et donc la plus recommandée pour le traitement de données à caractère personnel à des fins de recherche.

b. Garanties appropriées en matière de minimisation des données et de sécurité

29. En vertu de l'article 89.1 du RGPD, ce traitement ultérieur à des fins de recherche scientifique doit toutefois être soumis à des garanties appropriées qui garantissent la mise en place de mesures techniques et organisationnelles pour assurer le respect du principe de 'minimisation des données'. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.
L'anonymisation de données de santé de manière à ce que la ré-identification ne soit pas possible mais permettant néanmoins leur utilisation pour la recherche scientifique est très difficile. Certains États membres ont dès lors développé des centres d'accès sécurisés pour le partage et l'utilisation anonymes de données à des fins de recherche.

30. Il va de soi que le traitement ultérieur de données de patients à des fins de recherche scientifique doit en outre aussi respecter toutes les autres dispositions du RGPD sur le plan de la transparence, de la limitation des finalités, de la proportionnalité et de la sécurité de l'information[17].
Ainsi, les patients concernés devront être dûment informés de la recherche scientifique visée (voir l'article 14 du RGPD[18]) et des droits qui leur sont conférés par le RGPD (dont le droit d'accès, le droit de rectification, le droit à l'effacement des données[19], le droit à une limitation du traitement et le droit de s'opposer au traitement - articles 15 à 21 du RGPD).

C. Conditions supplémentaires

[17] Des développements récents permettent également de plus en plus d'analyser des données sensibles tout en maintenant la protection de ces données : cela est possible en traitant les données sous une forme cryptée au moyen de techniques telles que le cryptage homomorphique et de ventiler les données sur plusieurs serveurs et de les analyser ensuite avec des techniques de Multi-Party Computation (MPC). D'autres mesures techniques à envisager -en fonction du cas concret- sont : query-based and question-and-answer-based systems (dynamic anonymization), differantial privacy and sythetic data.

[18] L'article 14.5 du RGPD prévoit certes une exception à cette obligation d'information lorsque celle-ci se révèle impossible ou exigerait des efforts disproportionnés ou est susceptible de rendre impossible ou de compromettre gravement la réalisation des finalités de recherche. Le chercheur fournit alors des efforts afin de rendre publiques les informations d'une autre manière.

[19] L'article 17.3 du RGPD prévoit toutefois que la personne concernée ne peut pas faire valoir le droit à l'effacement lorsque cela est susceptible de rendre impossible ou de compromettre gravement la réalisation des finalités de recherche.

31. Dans la mesure où un chercheur voudrait limiter les droits des personnes concernées mentionnés aux articles 15, 16, 18 et 21 du RGPD, celui-ci doit, conformément à l'article 89.2 du RGPD, respecter également les dispositions du Titre 4 (articles 186 et suivants) de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.*

32. Étant donné que le traitement ultérieur de données de patients à des fins de recherche scientifique implique le traitement de données de santé sensibles, sur le plan de la sécurité de l'information, le chercheur devra, outre les mesures techniques et organisationnelles habituelles (voir l'article 32 du RGPD), également respecter l'article 9 de la loi susmentionnée du 30 juillet 2018 (voir le point 19).

33. Par souci d'exhaustivité - et sans préjudice de toutes les autres obligations imposées par le RGPD et la loi du 30 juillet 2018 -, j'attire encore votre attention sur l'obligation de tout responsable du traitement de vérifier s'il est nécessaire ou non de désigner un délégué à la protection des données (article 37 du RGPD)[20] et/ou de réaliser une analyse d'impact relative à la protection des données (article 35 du RGPD)[21].
En effet, la recherche scientifique avec des données de santé sensibles pourra probablement être considérée en général comme un "traitement à grande échelle de catégories particulières de données à caractère personnel" pour lequel, en vertu de l'article 35 du RGPD, une analyse d'impact relative à la protection des données doit être réalisée.

34. Enfin, il convient aussi de rappeler l'article 42, § 2, 3° de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé* qui prescrit que la Chambre sécurité sociale et santé du Comité de sécurité de l'information doit accorder une autorisation de principe pour toute communication de données à caractère personnel relatives à la santé, sauf dans les cas suivants :

---

[20] Pour des directives en la matière, voir :

- Informations sur le site Internet de l'Autorité : https://www.autoriteprotectiondonnees.be/dossier-thematique-delegue-a-la-protection-des-donnees

- Recommandation de la Commission de la protection de la vie privée n° 04/2017 *relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données (RGPD), en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité* ;

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf)

- Lignes directrices du Groupe 29 (WP 243)

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp243rev01_fr.pdf)

[21] Pour des directives en la matière, voir :

- Informations sur le site Internet de l'Autorité : https://www.autoriteprotectiondonnees.be/analyse-dimpact-relative-a-la-protection-des-donnees

- Recommandation d'initiative de la Commission de la protection de la vie privée n° 01/2018 du 28 février 2018 *concernant l'analyse d'impact relative à la protection des données et la consultation préalable*.

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018_2018.pdf)

- Lignes directrices du Groupe 29 (WP 248)

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp248%20rev.01_fr.pdf).

- si la communication est effectuée entre des professionnels des soins de santé qui sont tenus au secret professionnel et qui sont associés en personne à l'exécution des actes de diagnostic, de prévention ou de prestation de soins à l'égard du patient ;
- si la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, après avis de l'Autorité de protection des données ;
- dans les cas déterminés par le Roi, après avis de l'Autorité de protection des données ;
- lorsque des données sont communiquées entre des instances d'une même Communauté ou Région, qui ne font pas usage des services de base de la plate-forme eHealth.

2.2. Traitement secondaire de données du dossier du patient en vue de l'évaluation de la qualité des soins

35. Pour autant que ce traitement secondaire puisse être qualifié de traitement ultérieur en vue de finalités "statistiques", comme visé à l'article 5.1.b) du RGPD, on applique les mêmes principes que ceux exposés ci-avant au point 2.1 et celui-ci est réputé être "non incompatible" avec le traitement initial. À défaut et en l'absence de prescriptions réglementaires en la matière, l'éventuel caractère compatible devra être examiné par le responsable du traitement.

Base juridique

36. Comme exposé ci-avant, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes et ces données ne peuvent ensuite pas être traitées ultérieurement de manière incompatible avec ces finalités.

37. Dans la mesure où le traitement (ultérieur) de données du dossier du patient en vue de l'évaluation de la qualité des soins n'est pas encadré réglementairement de manière claire, le responsable du traitement devra vérifier, en vertu de l'article 6.4 du RGPD, si la finalité d'évaluation de la qualité des soins est compatible avec la prestation de soins proprement dite pour laquelle les données ont été collectées initialement dans le dossier du patient. À cet effet, le responsable du traitement tient compte notamment :

- du lien entre les deux finalités ;
- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données à caractère personnel (s'agit-il de catégories particulières de données à caractère personnel ?) ;
- des conséquences possibles du traitement ultérieur prévu pour les personnes concernées ;

- de l'application de garanties appropriées, dont éventuellement le cryptage et la pseudonymisation.

38. Étant donné que l'évaluation de la qualité des soins est étroitement liée à la prestation de soins proprement dite et à la manière dont celle-ci doit se faire de préférence, on peut partir du principe que les patients concernés peuvent raisonnablement s'attendre à un tel traitement ultérieur. En outre, on peut supposer qu'une évaluation de la qualité des soins aura en principe des conséquences favorables pour les soins ultérieurs dispensés aux patients (concernés). Un traitement secondaire de données de patients en vue de l'évaluation de la qualité des soins pourra dès lors communément[22] être considéré comme compatible avec la finalité initiale de la prestation de soins proprement dite.

39. Il n'empêche bien entendu que le responsable du traitement ultérieur de données de patients à des fins d'évaluation de la qualité des soins devra en outre respecter toutes les autres dispositions du RGPD en matière de transparence, de finalité, de proportionnalité et de sécurité de l'information. Plus particulièrement, on peut partir du principe que le "contrôle de qualité" pourra généralement être réalisé à l'aide de données anonymes, ou éventuellement à l'aide de données à caractère personnel pseudonymisées ; la proportionnalité ou la minimisation de données signifie en effet non seulement une limitation aux variables nécessaires mais aussi une pseudonymisation ou une anonymisation de ces variables quand c'est possible.

3. Traitement de données de santé dans le cadre d'essais cliniques

40. La ministre se renseigne également quant au fondement juridique recommandé pour le traitement de données à caractère personnel concernant la santé dans le cadre d'essais cliniques.

Base juridique

41. En vertu de l'article 9.1 du RGPD, le traitement de données de santé est en principe interdit. Cette interdiction connaît toutefois un certain nombre d'exceptions énumérées de manière exhaustive à l'article 9.2 du RGPD, parmi lesquelles :

- le traitement pour lequel la personne concernée a donné son consentement explicite ;
- le traitement qui est nécessaire en vue de la recherche scientifique conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre.

[22] Eu égard au principe de "responsabilité", il incombe bien entendu au responsable du traitement de refaire le test de compatibilité énoncé à l'article 6.4 du RGPD pour chaque traitement (ultérieur) concret.

42. Lors du traitement de données de santé dans le cadre d'essais cliniques, il faut faire clairement la distinction entre d'une part, le consentement éclairé qui est obligatoire pour la participation à l'essai clinique[23] et d'autre part, un éventuel consentement servant de fondement juridique pour le traitement de données à caractère personnel y afférent, dans le cadre du RGPD[24].

43. Étant donné que pour une personne qui accepte de participer à un essai clinique, il n'est pas possible de refuser le traitement de ses données à caractère personnel en la matière, on peut difficilement parler d'un consentement donné librement, comme le requiert néanmoins l'article 4.11) du RGPD. En outre, un consentement, qui est par définition susceptible d'être retiré à tout moment (article 7.3 du RGPD), ne semble pas toujours constituer le fondement juridique le plus stable et donc le plus recommandé pour des essais cliniques, et pour la recherche scientifique en général.

44. Le fondement juridique pour le traitement de données de santé (sensibles) dans le cadre d'études cliniques doit donc être trouvé dans une combinaison de l'article 6.1.e) ("mission d'intérêt public") ou de l'article 6.1.f) ("intérêt légitime")[25] du RGPD d'une part et de l'article 9.2.j) ("archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ") du RGPD d'autre part.

45. De nouveau, dans le cadre d'une étude clinique, le responsable du traitement de données à caractère personnel concernant la santé doit respecter toutes les autres dispositions du RGPD, tant en matière de transparence, de finalité, de proportionnalité que de sécurité de l'information.

[23] Voir la loi du 7 mai 2004 *relative aux expérimentations sur la personne humaine*, la loi du 19 décembre 2008 *relative à l'obtention et à l'utilisation de matériel corporel humain destiné à des applications médicales humaines ou à des fins de recherche scientifique* et la loi du 7 mai 2017 *relative aux essais cliniques de médicaments à usage humain*.

[24] Voir l'avis 3/2019 de l'EDPB du 23 janvier 2019 *concernant les questions et réponses sur l'interaction entre le règlement relatif aux essais cliniques et le règlement général sur la protection des données*, en particulier les points 15 e.s.

[25] L'article 6.1, *in fine*, du RGPD prévoit explicitement que l'article 6.1.f) ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.