CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Délibération n° 2019-113 du 5 septembre 2019 autorisant l'Assistance publique — Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution et la mise en œuvre d'un entrepôt de données, dénommé « Banque nationale de données maladies rares » (BNDMR).

(Demande d'autorisation n° 2211418)

La Commission nationale de l'informatique et des libertés,

Saisie par l'Assistance publique — Hôpitaux de Paris d'une demande d'autorisation concernant un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'entrepôt de données dénommé « Banque nationale de données maladies rares » (BNDMR) ;

Vu 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 ;

Vu le 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 ;

Vu le code de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 44-3° et 66-III ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le dossier et ses compléments, et notamment l'analyse d'impact relative à la protection des données ;

Après avoir entendu Mme Valérie PEUGEOT, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Sur le responsable de traitement :

L'Assistance publique – Hôpitaux de Paris (ci-après l'« AP-HP »)

Sur la base légale et la finalité du traitement

La BNDMR a vocation à :

- centraliser et unifier à l'échelle nationale les données des patients atteints de maladies rares ;
- permettre la réalisation d'études épidémiologiques et médico-économiques.

Plus précisément, les finalités poursuivies par le traitement sont les suivantes :

- le pilotage des politiques publiques, la création et la publication d'indicateurs et l'établissement d'un rapport annuel sur les maladies rares ;
- la réalisation d'études de faisabilité ;
- la réalisation de recherches dans le domaine de la santé (recherches non interventionnelles impliquant la personne humaine ou recherches n'impliquant pas la personne humaine).

La Commission relève qu'une gouvernance spécifique est prévue pour la BNDMR, au moyen de deux comités : le comité de pilotage (COPIL BNDMR) et le comité scientifique (COSCI BNDMR). La Commission relève par ailleurs que les conditions de participation et d'accès à la BNDMR seront régies par une charte.

Le traitement a pour base légale l'exercice d'une mission d'intérêt public, au sens de l'article 6-1-e du Règlement général sur la protection des données (ci-après RGPD).

La Commission considère que la finalité du traitement est déterminée, explicite et légitime, conformément aux dispositions de l'article 5-1-b du RGPD.

Elle estime qu'il y a lieu de faire application des dispositions de l'article 44-3° et 66-III et suivants de la loi du 6 janvier 1978 modifiée, qui soumettent à autorisation les traitements comportant des données relatives à la santé et justifiés, comme en l'espèce, par l'intérêt public.

La Commission rappelle que les traitements de données de santé à caractère personnel qui seront mis en œuvre ultérieurement, à des fins de recherche, d'étude et d'évaluation dans le domaine de la santé sont des traitements distincts qui doivent faire l'objet de formalités propres au titre des articles 72 et suivants de la loi « informatique et libertés ».

Sur les données traitées :

La BNDMR regroupe les données d'ordre administratif et médical produites par les bases BaMaRa, issues des centres de référence maladies rares et centres de compétences maladies rares.

Les catégories de données à caractère personnel traitées concernant les patients sont les suivantes :

- informations signalétiques : date de naissance (jour, mois et année de naissance), lieux de naissance et de résidence (code INSEE), sexe ;
- numéro identifiant Maladies rares (IDMR) (identifiant non réversible constitué à partir des nom, prénom, date de naissance, sexe) ;
- données de santé : diagnostic(s) d'intérêt, observations médicales et paramédicales, traitements médicamenteux, données néonatales ;
- données du parcours de soins : numéro de prise en charge généré par le système, date de prise en charge, structure responsable de la prise en charge, contexte de la prise en charge ;

- participation à des recherches ou études, volonté de participer à des études, existence d'échantillon biologique ;
- notification de l'information individuelle.

La Commission prend par ailleurs acte que le nom de naissance, le prénom de naissance, la date de naissance, le sexe, le lieu de naissance, le lieu de résidence et l'identifiant national de santé (INS) seront traités dans le cadre de l'identito-vigilance et de réconciliation des identités. Ces données seront conservées sur un serveur temporaire le temps nécessaire aux opérations d'identito-vigilance. Le nom, le prénom et l'INS ne seront pas conservés dans la BNDMR une fois ces opérations réalisées.

Les données traitées concernant les professionnels prenant en charge les patients sont les suivantes :

- numéro d'inscription au répertoire partagé des professionnels de santé (RPPS) ;
- lieu d'exercice (numéro FINESS).

Les catégories de données à caractère personnel traitées concernant les agents de l'AP-HP utilisateurs de la BNDMR sont les suivantes :

- nom, prénom ;
- adresse courriel ;
- code APH ;
- données de connexion.

La Commission considère que les données dont le traitement est envisagé sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement, conformément aux dispositions de l'article 5-1-c du règlement général sur la protection des données.

La Commission est informée que les données recueillies sont susceptibles d'être complétées dans le cadre de la mise en œuvre du Plan National Maladies Rares (PMNR)3 (2018-2022), qui confie de nouvelles missions à la BNDMR. Le responsable de traitement indique cependant qu'il s'agira toujours de données relatives à la santé recueillies dans le cadre du soin, relevant d'un niveau de sensibilité comparable aux données décrites dans la demande initiale.

Il appartiendra au responsable de traitement de déterminer si les évolutions nécessitent de soumettre à la Commission une demande de modification de la présente autorisation.

Par ailleurs, le responsable de traitement envisage, dans un second temps, un appariement entre les données de la BNDMR et du système national des données de santé (SNDS). Une telle modification devra faire l'objet de formalités spécifiques auprès de la Commission.

Sur les destinataires :

Pour la constitution et gestion de l'entrepôt de données : la BNDMR est accessible aux membres de la cellule opérationnelle BNDMR, au sein des locaux de l'AP-HP.

Pour la diffusion d'indicateurs : le ministère de la santé, les ARS, ainsi que les Centres maladies rares partenaires et les industriels sont destinataires des résultats exacts représentant les effectifs réels des indicateurs.

Pour la réalisation d'études de faisabilité et la réalisation de recherches dans le domaine de la santé (recherches non interventionnelles impliquant la personne humaine ou recherches n'impliquant pas la personne humaine), peuvent être destinataires des données :

- les professionnels de santé des centres de référence maladies rares (CRMR) et centres de compétences maladies rares (CPMR), appartenant à l'équipe de soin et portant sur des données des patients qu'ils prennent directement en charge ;

- les professionnels de santé des CRMR et CPMR (éventuellement associés à des partenaires extérieurs) portant sur les données de patients pris en charge dans plusieurs services ou établissements, voire des patients de l'ensemble des CRMR et CPMR ;

- des organismes extérieurs issus du secteur public ou privé, sous réserve que les traitements sollicités présentent un caractère d'intérêt public.

Plus particulièrement, le résultat des études de faisabilité (réalisées sous la responsabilité de l'AP-HP) est communiqué aux destinataires par la cellule opérationnelle de la BNDMR sous la forme d'un chiffre global de patients concernés.

Les résultats des tests de correspondance sont communiqués aux destinataires par la cellule opérationnelle de la BNDMR sous la forme d'un pourcentage de patients concernés.

Lorsque les recherches sont réalisées sous la responsabilité de l'AP-HP, les données restent dans l'entrepôt et sont traitées exclusivement par les membres de la cellule opérationnelle BNDMR, après validation par le COSCI BNDMR.

Lorsque les recherches sont réalisées sous la responsabilité d'une entité autre que l'AP-HP, des données indirectement identifiantes et strictement nécessaires à la finalité du traitement pourront être extraites de l'entrepôt et transmises à l'investigateur tiers, dans des conditions garantissant leur sécurité et leur confidentialité et après validation par le COSCI BNDMR.

La Commission demande qu'une vigilance particulière soit accordée, notamment dans le cadre des activités du COSCI, aux traitements ultérieurs nécessitant une extraction des données de la BNDMR au regard de leur sensibilité particulière et des risques élevés de réidentification.

La Commission considère que les catégories de destinataires n'appellent pas d'observation.

Sur l'information et les modalités d'exercice des droits :

Patients inclus dans le projet de recherche CEMARA (demande n° 1187326) :

La Commission a autorisé en 2007 un traitement de données ayant pour finalité la réalisation d'un projet de recherche intitulé CEMARA. Ce projet avait pour vocation l'évaluation et l'élaboration de stratégies sanitaires visant à améliorer la prise en charge des patients atteints de maladies rares.

Les données recueillies dans le cadre de l'étude ont été intégrées dans l'application BaMaRa.

En application de l'article 14-5-b du RGPD, l'obligation d'information individuelle de la personne concernée peut faire l'objet d'exceptions dans l'hypothèse où la fourniture d'une telle information se révèle impossible, exigerait des efforts disproportionnés ou compromettrait gravement la réalisation des objectifs du traitement. En pareils cas, conformément au RGPD, le responsable de traitement prend des mesures appropriées pour protéger les droits et libertés, ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

En l'espèce, la Commission relève qu'il sera fait exception au principe d'information individuelle des personnes s'agissant des patients dont les données ont été recueillies dans le cadre du projet de recherche CEMARA et que des mesures appropriées seront mises en œuvre, notamment par la diffusion sur le site web dédié à la BNDMR et par voie d'affichage d'une information relative au traitement dont la mise en œuvre est envisagée.

Patients inclus dans l'application BaMaRa avant la création de la BNDMR

A compter de l'année 2017, année du déploiement de l'application BaMara, les patients ont été individuellement informés par la remise d'une note d'information :

- du traitement des données les concernant, dans le cadre des soins ;
- de la réutilisation de ces données pour des projets de recherche, dans le cadre de la future BNDMR ;
- des modalités d'exercice de leurs droits.

La note d'information renvoie le patient sur la page dédiée à la transparence du site web de la BNDMR, sur laquelle le détail de tous les traitements mis en œuvre sera tenu à jour. Le professionnel de santé prenant en charge le patient est tenu de tracer dans l'application BaMaRa, au moyen d'une case à cocher, la remise de l'information et la non-opposition du patient à l'utilisation des données le concernant dans le cadre de la BNDMR.

Le droit d'opposition s'exercera, à tout moment, soit directement auprès du clinicien, soit auprès de la cellule opérationnelle BNDMR par message électronique (à l'adresse indiquée sur le formulaire d'information) ; dans cette dernière hypothèse, la case prévue afin d'exercer le droit d'opposition sera cochée *a posteriori* et les données déjà transmises seront supprimées.

Patients pris en charge postérieurement à la présente autorisation

Les personnes prises en charge postérieurement à l'autorisation seront informées de la création de la BNDMR ainsi que des traitements mis en œuvre à partir de la BNDMR au moyen d'une notice d'information remise individuellement par le professionnel de santé les prenant en charge. Ce professionnel sera tenu de tracer dans l'application BaMaRa, au moyen d'une case à cocher, la remise de l'information et la non-opposition du patient à l'utilisation des données le concernant à des fins de recherche.

La notice d'information individuelle renvoie à un portail de transparence mis à disposition du public sur le site web dédié à la BNDMR. Chacun des traitements (indicateurs de pilotage, études de faisabilité, tests de correspondance, recherches impliquant ou n'impliquant pas la personne humaine, etc.), mis en œuvre à partir des données de la BNDMR, y sera documenté.

Les droits des personnes s'exercent auprès de l'AP-HP, plus spécifiquement auprès du délégué à la protection des données, *via* un formulaire dédié sur le site web de la BNDMR, ou en adressant un courriel à une adresse spécifique mentionnée sur la note d'information.

La Commission demande que les supports d'information soient complétés afin de contenir l'ensemble des mentions prévues par les articles 13 et 14 du RGPD.

Sous cette réserve, la Commission considère que ces modalités d'information et d'exercice des droits sont satisfaisantes.

Sur les mesures de sécurité :

En premier lieu, la Commission prend note de la réalisation par l'AP-HP d'une analyse d'impact sur la protection des données ayant permis de construire et de démontrer la mise en œuvre des principes de protection des données dans la constitution de l'entrepôt de données de santé.

La Commission prend note que l'AP-HP est hébergeur agréé de données de santé. Une politique de sauvegarde est mise en œuvre. Les sauvegardes sont testées régulièrement afin de vérifier leur intégrité. Le transfert des sauvegardes est sécurisé. Elles sont stockées dans un endroit garantissant leur sécurité et leur disponibilité. De plus, lors de la mise au rebut, le matériel remisé est nettoyé de toute donnée à caractère personnel. Les supports de stockage usagés ou en panne font l'objet d'une procédure de destruction ou d'effacement.

La Commission prend acte qu'un chiffrement des données stockées au sein de la BNDMR est mis en place. La Commission considère que la nature des données exige que celles-ci fassent l'objet de mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité, tant au niveau des bases de données que des sauvegardes.

La Commission note que les données stockées au sein des différentes bases BaMaRa font l'objet d'une pseudonymisation. Une fois pseudonymisées, ces données seront transmises par flux sécurisé vers la zone de stockage de la BNDMR.

La Commission rappelle que le recours à la pseudonymisation doit assurer que les données manipulées ne peuvent plus être attribuées à une personne précise sans avoir recours à des informations supplémentaires, ces informations supplémentaires devant être conservées séparément et soumises à des mesures techniques et organisationnelles adéquates.

La Commission prend note que la pseudonymisation sera réalisée à l'aide d'algorithmes de hachage permettant la création du numéro Identifiant Maladies rares (IDMR) à partir des nom, prénom, date de naissance et sexe. A cet égard, la Commission recommande l'utilisation d'un algorithme de hachage à clé secrète.

La Commission prend note que différents profils d'habilitation sont prévus pour permettre de préparer et d'effectuer l'extraction des données de la BNDMR, cela afin de gérer les accès aux données en tant que de besoin. Les accès sur les données de l'entrepôt sont réalisés au sein même du réseau interne de l'AP-HP, afin de permettre notamment la préparation des données agrégées. Les données agrégées sont ensuite disponibles sur le portail web de l'AP-HP pendant une fenêtre de temps d'une semaine maximum.

L'accès au portail est sécurisé au moyen de canaux de communication chiffrés et assure l'authentification de la source et du destinataire.

Concernant le recours au protocole HTTPS, la Commission recommande d'utiliser la version de TLS la plus à jour possible. De plus, des mesures sont prévues pour assurer le cloisonnement du traitement. Le réseau fait l'objet de mesures de filtrage ayant pour but de restreindre l'émission et la réception des flux réseau aux machines identifiées et autorisées.

S'agissant de l'accès aux données pseudonymisées accessibles via l'intranet de l'APHP, la Commission recommande la mise en place d'une politique d'authentification forte. Elle rappelle en outre que l'accès aux données de santé par des professionnels de santé doit se faire conformément aux référentiels d'interopérabilité et de sécurité en application de l'article L 1110-4-1 du CSP.

La Commission constate par ailleurs que l'accès aux données agrégées disponibles via le portail de l'AP-HP repose sur un identifiant individuel et un mot de passe. A cet égard, elle rappelle qu'une politique satisfaisante de mots de passe doit être conforme à sa délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe. Elle recommande notamment que les clés d'accès soient transmises *via* un canal distinct du courriel.

Une journalisation des opérations de consultation, création et modification des données de la BNDMR est mise en place. Les journaux font l'objet d'une analyse mensuelle.

La Commission recommande en outre de réaliser un contrôle des traces de manière automatique, afin de détecter les comportements anormaux et de générer des alertes le cas échéant. La Commission recommande également que des mesures soient mises en œuvre pour assurer l'intégrité des traces et que l'administrateur qui est en mesure de consulter les traces des accès n'accède pas aux données de santé.

La Commission relève que des mesures de gestion des incidents de sécurité et des violations de données sont mises en place. Elle rappelle la nécessité de mettre en place une procédure de gestion des incidents et des violations de données qui soit documentée, régulièrement mise à jour, et éprouvée à travers des tests réguliers.

Les mesures de sécurité décrites par le responsable de traitement sont conformes à l'exigence de sécurité prévue par les articles 5-1-f et 32 du RGPD. La Commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Sur les durées de conservation :

Données relatives aux patients

Les données nécessaires aux opérations d'identito-vigilance (nom de naissance, prénom de naissance, date de naissance, sexe, lieu de naissance, lieu de résidence et INS) sont conservées sur un serveur temporaire pour la durée de la réalisation desdites opérations (durée inférieure à une journée). Elles sont ensuite supprimées.

Les autres données sont conservées pendant 20 ans. A l'issue de ce délai, les données seront supprimées.

Les données relatives aux demandes d'exercice des droits (identité du demandeur, type de pièce justificative, date de réponse, copie de la réponse) seront conservées durant cinq ans. Les pièces justificatives sont conservées pendant un an.

Données relatives aux professionnels prenant en charge les patients :

Les données sont conservées pendant 20 ans. A l'issue de ce délai, les données seront supprimées.

Données relatives aux agents AP-HP utilisateurs de la BNDMR :

Les journaux de connexion sont conservés cinq ans. Les informations associées aux comptes sont conservées un an après le départ de l'agent.

La Commission considère que ces durées de conservation des données n'excèdent pas celles nécessaires aux finalités pour lesquelles les données sont collectées et traitées, conformément aux dispositions de l'article 5-1-e du RGPD.

Dans ces conditions, la Commission autorise l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution et la mise en œuvre d'un entrepôt de données, intitulé « Banque nationale de données maladies rares ».

La présidente

Marie-Laure DENIS

M-L. De