

Date de publication sur legifrance: 05/11/2019

Commission Nationale de l'Informatique et des Libertés

DELIBERATION n°2019-103 du 5 SEPTEMBRE 2019

Délibération n° 2019-103 du 5 septembre 2019 autorisant le centre hospitalier universitaire de Lille à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, intitulé « INCLUDE »

(Demande d'autorisation n° 2202081)

La Commission nationale de l'informatique et des libertés,
Saisie par le centre hospitalier universitaire de Lille d'une demande d'autorisation concernant un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données de santé ;
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 » (règlement général sur la protection des données) ;
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 et suivants ;
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 ;
Sur la proposition de Mme Valérie PEUGEOT, commissaire, et après avoir entendu les observations de Mme Nacima BELKACEM, commissaire du Gouvernement,

Formule les observations suivantes :

Sur le responsable du traitement
Le centre hospitalier universitaire de Lille (le CHU de Lille).

Sur la finalité et la base légale du traitement
L'entrepôt de données de santé du CHU de Lille a pour finalité de permettre la réalisation de recherches, d'études et d'évaluations dans le domaine de la santé par les professionnels du CHU et ses partenaires extérieurs (établissements de santé, instituts de recherches, université, industriels du médicament et des dispositifs médicaux). Plus précisément, il a vocation à faciliter la réalisation d'études internes et multicentriques impliquant ou n'impliquant pas la personne humaine, d'analyses médico-économiques à visée décisionnelle et stratégique ou d'épidémiologie hospitalière, de recherches visant à réaliser des modèles prédictifs en matière de vigilance sanitaire, de qualité et de sécurité des soins, le pré-screening de patients à finalité d'essais cliniques, la conception d'outils

d'aide à la décision médicale fonctionnant à partir de dispositif d'intelligence artificielle.

La Commission relève qu'une gouvernance spécifique est prévue par le CHU pour l'entrepôt de données via la constitution d'un comité scientifique et éthique compétent pour déterminer l'utilisation qui sera faite des données de l'entrepôt, notamment dans le cadre de projets de recherche multicentriques, ainsi que d'un comité stratégique et opérationnel.

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

La Commission considère que les finalités poursuivies sont déterminées, explicites et légitimes, conformément aux dispositions de l'article 5-1-b RGPD.

La Commission estime qu'il y a lieu de faire application des dispositions des articles 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, à partir des données extraites de l'entrepôt de données de santé du CHU de Lille, sont des traitements de données distincts de l'entrepôt qui doivent faire l'objet de formalités propres conformément aux dispositions des articles 72 et suivants de la « loi informatique et libertés ».

Sur les données traitées

Les données de l'entrepôt sont relatives aux patients pris en charge par le CHU, y compris les patients pris en charge avant la constitution de l'entrepôt, ainsi qu'aux professionnels de santé.

S'agissant des données relatives aux patients, provenant du système d'information hospitalier et recueillies dans le cadre des soins (dossier patient informatisé, dossiers médicaux spécialisés, - dossier des urgences, d'imagerie, de réanimation, de biologie médicale, d'anesthésie, de suivi de bloc opératoire -, logiciels utilisés pour le programme de médicalisation des systèmes d'information et pour le suivi des vigilances sanitaires) :

- données d'identification : adresse, date et lieu de naissance, numéro d'identification ;
- données liées à la vie personnelle : situation familiale et habitude de vie ;
- données liées à la vie professionnelle : situation professionnelle, scolarité, formation, exposition professionnelle ;
- données d'ordre économique et financier : couverture sociale et appréciation sur les difficultés sociales des personnes ;
- données sensibles : données de santé (pathologies, affections, antécédents médicaux, données relatives aux soins, données d'imagerie, de biologie, situations et comportements à risque, données génétiques, etc.), données relatives à la présumée origine raciale ou ethnique.

S'agissant des données relatives aux professionnels de santé :

- données d'identification : civilité, nom et prénom ;
- données liées à la vie professionnelle : matricule, intitulé du poste, pôle, service, unité fonctionnelle au sein desquels le professionnel est affilié, adresse électronique professionnelle.

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 RGPD.

Sur les destinataires

Sous réserve de respecter les dispositions spécifiques de la loi « informatique et libertés » applicables à la réalisation des recherches, études et évaluations dans le domaine de la santé, les professionnels de santé du CHU de Lille et les professionnels membres du département de l'information médicale auront accès, pour l'exercice de leurs missions, à l'ensemble des données contenues dans l'entrepôt et aux fins de réaliser les recherches, études et évaluations visées dans la présente autorisation,

Sous cette même réserve, les partenaires extérieurs du CHU de Lille (établissements de santé, instituts de recherche, universités, industriels du médicament et des dispositifs médicaux) auront également accès aux données de santé de l'entrepôt qui seront strictement nécessaires et pertinentes au regard des objectifs des recherches, études et évaluations qu'ils mènent à partir desdites données. La Commission relève, d'une part, que l'accès des industriels sera limité à des données anonymisées au sens de l'avis du G29 n° 05/2014 du 10 avril 2014 relatif aux techniques d'anonymisation et que, d'autre part, le CHU exclut l'accès de l'entrepôt aux professionnels du secteur bancaire et assurantiel.

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

Sur l'information et les droits des personnes

Conformément à l'article 69 de la loi « informatique et libertés », les personnes auprès desquelles sont recueillies les données à caractère personnel ou à propos desquelles de telles données sont transmises doivent être destinataires d'une information individuelle, incluant les éléments prévus à l'article 13 ou 14 du RGPD.

S'agissant des patients dont les données ont été collectées préalablement à la présente autorisation :

La Commission relève que le CHU de Lille souhaite alimenter l'entrepôt de données de santé avec les données des patients venus au CHU depuis 2008. Elle observe que, compte tenu du nombre de patients concernés (plus de 1 million), de l'incertitude concernant leur statut vital, de l'ancienneté d'une partie des données, du coût économique engendré par l'information individuelle, le CHU en tant que responsable de traitement estime qu'informer individuellement les patients constituerait un effort disproportionné. En application de l'article 14-5-b du RGPD et de l'article 69 de la loi « informatique et libertés » modifiée, 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 révélerait 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 préalablement à la présente autorisation et que des mesures appropriées seront mises en œuvre, notamment au moyen d'une information collective sur la constitution de l'entrepôt par voie d'affichage dans les locaux du CHU, une mention sur son site web et le livret d'accueil remis aux patients, l'utilisation des réseaux

sociaux et une publi-information dans le journal local.

La Commission relève que les supports d'information collective qui lui ont été remis à l'appui de sa demande ne font pas explicitement mention de la constitution de l'entrepôt, de sa finalité et des droits des personnes concernées. Elle demande que ces supports d'information soient complétés sur ces points pour être conformes aux exigences des articles 13 et 14 du RGPD.

S'agissant des patients dont les données seront collectées postérieurement à la présente autorisation (nouveaux patients ou patients en cours de suivi) :

La Commission relève que le personnel du CHU de Lille (médecins, infirmiers, secrétaires médicales, agents du bureau des entrées) procédera, à partir de la remise d'un document écrit, à une information du patient ainsi qu'au recueil de son consentement. Celui-ci sera réalisé, dans un premier temps, par saisie manuelle dans le système d'information hospitalier et que le CHU envisage à terme de mettre en place un système interopérable de collecte du consentement du patient permettant à celui-ci d'exprimer son consentement avant, pendant et après sa venue à l'hôpital et de revenir sur celui-ci. La Commission indique que le système interopérable de recueil du consentement envisagé à terme ne devra pas se substituer à l'actuel système de saisie manuelle, afin de faciliter l'expression du consentement de tous les patients. Par ailleurs, le CHU procédera également à une information collective (mise à disposition d'un document écrit dans les salles d'attente des consultations, mention spécifique dans le livre d'accueil et sur le site internet du CHU). La Commission rappelle que l'information individuelle délivrée devra être strictement conforme aux exigences des articles 13 et 14 du RGPD et devra porter spécifiquement sur l'entrepôt, ses finalités et les droits des personnes concernées.

S'agissant des professionnels de santé :

L'information individuelle de ces professionnels est assurée via une information accompagnant la fiche de paie et le magazine interne du CHU de Lille.

Les droits des personnes concernées (patients et professionnels de santé), s'exercent auprès du délégué à la protection des données du CHU de Lille par l'envoi d'un message électronique ou d'un courrier postal.

Sous réserve de la modification des supports d'information collective mis à disposition des patients, la Commission considère que les modalités d'information retenues et d'exercice des droits sont satisfaisantes.

Sur les mesures de sécurité

La Commission prend note de la réalisation par le CHU de Lille 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 de la vie privée dans la constitution de l'entrepôt de données de santé. Sous réserve que les mesures correctrices proposées dans la partie dédiée aux axes d'amélioration de l'analyse d'impact produite soient effectivement mises en œuvre, elle formule les observations suivantes.

S'agissant de l'accès à l'entrepôt de données de santé :

La Commission observe que ceux-ci sont délivrés par un comité scientifique et éthique participant de la gouvernance de l'entrepôt. A la suite du dépôt d'une demande et de sa validation, les administrateurs de l'entrepôt préparent les données qui seront mises à disposition des requérants. La Commission relève qu'il conviendra de s'assurer que chaque jeu de données créé dispose d'une durée d'utilisation limitée et préalablement définie.

Différents profils d'habilitation sont prévus afin de gérer les accès aux données en tant que besoin. Les permissions d'accès sont supprimées pour tout utilisateur n'étant plus habilité. La Commission rappelle qu'une revue globale doit être opérée de façon régulière afin de s'assurer du bon effacement des habilitations. Chaque utilisateur dispose d'un compte d'utilisation unique, individuel et nominatif.

Une politique d'authentification reposant sur un identifiant individuel et un mot de passe est mise en place pour permettre les accès des utilisateurs aux jeux de données l'entrepôt. Cette politique d'authentification est conforme aux délibérations de la Commission n° 2017-012 du 19 janvier 2017 et n° 2017-190 du 22 juin 2017 concernant les recommandations relatives aux mots de passe. Elle est renforcée dans le cas des administrateurs ayant accès à des données de santé en portant la taille minimum des mots de passes à 14 caractères associés à un mécanisme de verrouillage de l'accès au compte en cas saisie multiple de mots de passe erronés.

La Commission note qu'en fonction des demandes qui seront effectuées, les données pourront faire l'objet de différents types de pré-traitements. Elles pourront ainsi être agrégées, pseudonymisées ou anonymisées.

La Commission relève que les processus d'anonymisation et de pseudonymisation des données ne sont pas encore définis. Elle n'est donc pas en mesure de se prononcer sur leur validité. La Commission rappelle que :

dans le cas de l'anonymisation : il conviendra de démontrer la conformité de la solution et des techniques d'anonymisation mises en œuvre, aux trois critères définis par l'avis du G29 n°05/2014 du 10 avril 2014 précité, et de la transmettre à la Commission. Cet avis retient qu'un traitement de données est a priori anonyme dès lors qu'il n'est possible ni d'individualiser, ni de corréler, ni d'interférer les données. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification devrait être menée. Cette étude consiste à démontrer que les risques, liés à la publication du jeu de données, n'ont pas d'impact sur la vie privée et les libertés des personnes concernées.

dans le cas de la pseudonymisation : les données manipulées ne doivent 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. En particulier, la Commission rappelle la nécessité d'écarter toute donnée identifiante comme le prénom, le nom, le nom de jeune fille, l'adresse postale, l'adresse électronique, le numéro de téléphone, la date de naissance/décès, le lieu de naissance/décès, le NIR, le numéro de visite, l'identifiant technique, etc.

Dans le cas où il serait envisagé d'avoir recours à la pseudonymisation de documents non structurés (comme des comptes-rendus médicaux par exemple), la Commission rappelle qu'une telle opération doit être réalisée avec vigilance, notamment si elle met en œuvre des outils automatisés pour lesquels des erreurs sont susceptibles d'advenir.

Les actions des utilisateurs accédant à l'entrepôt font l'objet de mesures de traçabilité. En particulier, sont tracées les connexions à l'entrepôt (identifiants, date et heure) et les requêtes et opérations réalisées. La Commission recommande 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 observe que l'entrepôt est accessible uniquement sur le réseau interne du CHU de Lille à partir d'une interface prévue à cet effet. L'accès est sécurisé au moyen du

protocole HTTPS. Celui-ci utilise des canaux de communication chiffrés et assure l'authentification de la source et du destinataire. Concernant le recours à ce protocole, la Commission recommande d'utiliser la version de TLS la plus à jour possible.

S'agissant de l'accès aux données pseudonymisées accessibles via l'intranet du CHU, 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 du code de la santé publique.

La Commission relève toutefois qu'il est envisagé à terme d'ouvrir la possibilité d'accès distant. Elle rappelle à ce titre qu'il conviendra de préciser les modalités de délivrance et les moyens de sécurité mis en œuvre, cela afin d'assurer l'effectivité des mesures au regard des risques que de tels accès pourraient faire peser sur le traitement.

Concernant la sécurisation des données :

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 réseaux aux machines identifiées et autorisées.

La Commission note que les mises à jour des logiciels sont installées de manière régulière. Des mesures spécifiques sont prévues pour garantir la disponibilité des données et services. Une politique de lutte contre les maliciels est définie et des logiciels antivirus sont installés et régulièrement mis à jour sur tous les matériels prenant part au traitement. Enfin, une politique de maintenance des environnements informatiques est définie, assurant que des mesures appropriées relatives à la sécurité des données sont mises en œuvre. Les interventions font ainsi l'objet d'une traçabilité.

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.

L'accès aux locaux hébergeant les équipements prenant part au traitement est restreint au moyen de portes verrouillées contrôlées par un moyen d'authentification personnel. Des mesures de détection et de protection contre les risques d'incendie, de dégâts des eaux et de perte d'alimentation électrique sont proposées. Enfin, un plan de continuité de l'activité est prévu, permettant de reprendre l'activité en réduisant le plus possible l'impact d'un sinistre.

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 la durée de conservation des données

Les données seront conservées conformément aux durées de conservation prévues par les dispositions de l'article R. 1112-7 du code de la santé publique pour la conservation des dossiers médicaux des patients.

La Commission considère que les durées de conservation prévues n'excèdent pas la durée nécessaire aux finalités pour lesquelles les données sont collectées et traitées, conformément aux dispositions de l'article 5-1-e) du RGPD.

Autorise, conformément à la présente délibération, le CHU de Lille à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données de santé visant à réaliser des recherches, études et évaluations dans le domaine de la santé.

Pour la Présidente La Vice-Présidente déléguée

Sophie LAMBREMON

Nature de la délibération: Autorisation