Le Directeur de l'accompagnement juridique

Monsieur Renan TARGHETTA
DIRECTEUR DE LA RECHERCHE ET DE L'INNOVATION
CENTRE HOSPITALIER UNIVERSITAIRE DE MONTPELLIER
CENTRE ADMINISTRATIF ANDRE BENECH
191 AVENUE DU DOYEN GASTON GIRAUD
34295 - MONTPELLIER

N/Réf. : TD/LAT/NAT241018

DEMANDE D'AUTORISATION N° 2233463
A rappeler dans toute correspondance

Décision DT-2024-014 autorisant le CENTRE HOSPITALIER UNIVERSITAIRE DE MONTPELLIER à mettre en œuvre un traitement automatisé de données ayant pour finalité la constitution d'un entrepôt de données de santé, dénommé « eDOL ». (Demande d'autorisation n° 2233463).

La Commission nationale de l'informatique et des libertés,

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 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

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 la décision du 21 septembre 2023 portant délégation de signature du secrétaire général de la Commission nationale de l'informatique et des libertés ;

Saisie d'une demande d'autorisation relative à un traitement de données à caractère personnel dans le domaine de la santé ;

Considérant que ce traitement, dont la finalité présente un caractère d'intérêt public, relève des dispositions de la section 3 du chapitre III du titre II de la loi du 6 janvier 1978 modifiée ;

Considérant que le traitement présente les caractéristiques et répond aux conditions suivantes :

Sur les points de non-conformité au référentiel concerné	Le dossier de demande mentionne que le traitement envisagé est conforme aux dispositions du référentiel « entrepôt de données dans le domaine de la santé », à l'exception : - de la nature des données traitées (IRIS) ; - de la conservation de données d'identification dans la base principale de l'entrepôt ; - des règles encadrant l'accès et la réunion de données directement identifiantes ; - de la durée de conservation des données ; - des modalités d'information des professionnels de santé ; - de certaines mesures de sécurité. En dehors de ces points, qui font l'objet d'un examen spécifique dans la présente autorisation, ce traitement devra respecter le cadre prévu par le référentiel.
Sur la finalité du traitement, sa licéité et les conditions permettant de traiter des données concernant la santé	Le traitement envisagé a pour finalités : - la réalisation de recherches, études et évaluations dans le domaine de la santé ; - le fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ; - l'amélioration de la qualité de l'information médicale ; - l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information ; - la gestion des recours contre tiers ; - la réalisation d'études de faisabilité (pré-screening) ; - la gestion des urgences sanitaires ; - l'exportation de données pseudonymisées vers des registres conformes au référentiel « entrepôt de données dans le domaine de la santé » ou autorisés par la CNIL ; - l'exportation de données pseudonymisées dans le cadre de la mise en œuvre de politique d'amélioration continue de la qualité et de la sécurité des soins et de gestion des risques par le responsable de traitement, tel que prévu à l'article L. 6111-2 du code de la santé publique. Les données contenues dans cet entrepôt ne pourront, par analogie avec les finalités « interdites » d'utilisation du Système national des données de santé (SNDS), être exploitées ni à des fins de promotion des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique en direction de professionnels de santé ou d'établissements de santé, ni à des fins d'exclusion de garanties des contrats d'assurance, ni de modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

	Les utilisations futures des données contenues dans cet entrepôt s'inscriront dans le cadre des dispositions des articles 66 et 72 et suivants de la loi « informatique et libertés », qui imposent que chaque projet de recherche, étude ou évaluation soit justifié par l'intérêt public. Ces traitements devront faire l'objet de formalités propres.
Sur les données traitées	Cet entrepôt sera alimenté par des données à caractère personnel issues des programmes de données des applicatifs de production de soins du responsable de traitement et de son applicatif de gestion administrative des patients. Les données à caractère personnel de patients versées dans l'entrepôt sont, en dehors des catégories de données visées dans le référentiel, les zones géographique IRIS. Le numéro d'inscription au répertoire national d'identification des personnes physiques Identifiant national de santé (NIR-INS) des patients sera traité afin d'alimenter l'entrepôt. Il sera conservé chiffré et pseudonymisé de façon irréversible pour alimenter l'entrepôt. Concernant les professionnels de santé n'exerçant plus au sein du Centre Hospitalier Universitaire de Montpellier, seules les informations concernant leur fonction, leur service et leur unité d'exercice seront versées dans l'entrepôt.
Sur la conservation des données	Les données versées dans l'entrepôt sont conservées quarante ans à compter de leur collecte dans le cadre du soin puis supprimées. Ce processus de suppression des données sera planifié et réalisé une fois par mois. Cette durée a été scientifiquement justifiée dans le dossier de demande, au regard des pathologies étudiées et des recherches envisagées ultérieurement, notamment en matière d'affections présentant une physiopathologie débutant pendant la période in utero, dès la naissance ou dans l'enfance. La durée de conservation standard des traces sur le bastion d'administration est d'un an. La zone de journalisation disposera d'une durée de rétention similaire. Il est rappelé que ces traces ne doivent pas contenir de données de santé ou de secrets (mot de passe, empreinte cryptographique, etc.). Les vidéos des sessions administrateur et utilisateur seront conservées pendant deux mois. Il est rappelé que ces vidéos peuvent contenir des données de santé et des secrets et ne pourront pas être exportées hors du périmètre de l'entrepôt. Ces durées de conservation des données n'excèdent pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées,

	conformément aux dispositions de l'article 5-1-e) du RGPD.
Sur les accédants et les destinataires des données	Pourront accéder aux données uniquement : - les porteurs de projets d'étude, d'évaluation ou de recherche dans le domaine de la santé ayant réalisé les formalités nécessaires auprès de la CNIL ; - les personnels spécifiquement habilités, soumis au secret professionnel, dans les strictes limites de leur besoin d'en connaître, pour l'exercice de leurs missions s'inscrivant dans les finalités de l'entrepôt « eDOL ». Des documents tenus à jour indiquent la ou les personnes compétentes pour chaque responsable de traitement pour délivrer l'habilitation à accéder aux données, la liste des personnes habilitées à accéder à ces données, leurs profils d'accès respectifs et les modalités d'attribution, de gestion et de contrôle des habilitations. La qualification des personnes habilitées et leurs droits d'accès doivent être régulièrement réévalués, conformément aux modalités décrites dans la procédure d'habilitation établie par le responsable de traitement.
Sur l'information des personnes	***S'agissant des patients pris en charge antérieurement à la constitution de l'entrepôt et n'étant plus suivis :*** En application de l'article 14 du RGPD, l'obligation d'information individuelle de la personne concernée peut faire l'objet d'exceptions, notamment 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, 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, il sera fait exception au principe d'information individuelle des patients pris en charge antérieurement à la constitution de l'entrepôt et n'étant plus suivis. Des mesures appropriées seront mises en œuvre, notamment par des communiqués de presse, sur les réseaux sociaux, ainsi que par la diffusion sur le site web du responsable de traitement d'une information comportant l'ensemble des mentions prévues par le RGPD. ***S'agissant des patients admis ou réadmis postérieurement à la constitution de l'entrepôt :*** Au moment de leurs prises de rendez-vous ou de leurs connexions à l'un des portails patients du CHU de Montpellier, les patients et, le cas échéant, leurs représentants légaux seront informés du traitement et de la possibilité de consulter une note d'information

	comportant l'ensemble des mentions prévues par le RGPD par le biais d'une page spécifique sur le site web du responsable de traitement. Pour chaque création de séjour, une note d'information sera envoyée automatiquement au patient, par courrier électronique. Si le patient n'a pas d'adresse électronique, un courrier papier individuel lui sera envoyé. Les supports d'information devront, en tout état de cause, mentionner explicitement, que l'exercice des droits par les personnes, notamment leur droit d'opposition, n'aura pas de conséquence sur leur prise en charge médicale. En outre, le responsable de traitement procédera à une information collective, par des communiqués de presse, sur les réseaux sociaux, ainsi que par la diffusion sur son site web, d'une information comportant l'ensemble des mentions prévues par le RGPD. ***S'agissant des professionnels de santé :*** Les professionnels de santé seront informés individuellement au moyen d'une note d'information. Cette information sera délivrée par le biais du portail « ressource humaine » du responsable de traitement ainsi que par le biais d'une fiche complémentaire à l'envoi du bulletin de salaire. Il sera fait exception au principe d'information individuelle des professionnels de santé n'exerçant plus au sein du Centre Hospitalier Universitaire de Montpellier. Des mesures appropriées seront mises en œuvre, notamment par des communiqués de presse, sur les réseaux sociaux, ainsi que par la diffusion sur le site web du responsable de traitement, d'une information comportant l'ensemble des mentions prévues par le RGPD.
Sur la sécurité des données et la traçabilité des actions	Le responsable de traitement a réalisé et transmis à l'appui de la demande d'autorisation une analyse d'impact relative à la protection des données spécifique à la création de l'entrepôt « eDOL », ainsi qu'une comparaison détaillée des mesures de sécurité planifiées ou mises en place dans l'entrepôt avec les exigences de sécurité mentionnées dans le référentiel « entrepôt de données dans le domaine de la santé ». Les points de non-conformité vis-à-vis de ce référentiel relevés par le responsable de traitement sont les suivants : - L'inclusion du sexe, du mois et de l'année de naissance, de la date de décès, de la zone géographique IRIS dans la base de données principale de l'entrepôt. - La réunion de données directement identifiantes des patients aux fins suivantes :

	o l'amélioration de la qualité de l'information médicale ; o l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information ; o la gestion des recours contre tiers ; o le fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ; o la réalisation d'études de faisabilité (pré-screening) permettant un retour au dossier du patient de la part les professionnels de santé l'ayant pris en charge le patient ; o la gestion des urgences sanitaires ; o l'exportation de données pseudonymisées en cas de demande des registres, à condition que de tels registres aient été déclarés conformes au référentiel « entrepôt de données dans le domaine de la santé » ou qu'ils bénéficient d'une autorisation de la CNIL montrant que les exigences sécurité du référentiel sont respectées ; o l'exportation de données pseudonymisées concernant la mise en œuvre de politique d'amélioration continue de la qualité et de la sécurité des soins et une gestion des risques par le responsable de traitement, tel que prévu à l'article L. 6111-2 du code de la santé publique. Aux fins de réalisation de ces finalités, sans préjudice des procédures de réidentification décrites dans les exigences SEC-REI-1 et suivantes du référentiel « entrepôt de données dans le domaine de la santé » : - la réidentification des patients permettant de faire le lien avec le système d'information clinique du responsable de traitement, sera réalisée grâce aux IPP et IEP des personnes concernées ; - les extractions seront transmises exclusivement vers le système d'information clinique du responsable de traitement ; - le dossier médical d'un patient ne pourra être consulté que par les professionnels de santé participant à sa prise en charge, conformément aux dispositions de l'article L. 1110-4 du code de la santé publique (le cas échéant par l'équipe de soin). Ces non-conformités ont été dûment justifiées et compensées par la mise en œuvre de mesures techniques et organisationnelles à l'état de l'art.

	Par ailleurs, certaines mesures de sécurité techniques et organisationnelles prévues afin d'améliorer la conformité au référentiel « entrepôt de données dans le domaine de la santé » sont actuellement en cours d'implémentation, notamment : - la mise en place d'espaces de travail accessibles aux utilisateurs ; - le chiffrement au repos des supports de stockage et des tables de correspondance de l'entrepôt ; - la génération de l'identifiant interne via une fonction de hachage cryptographique à l'état de l'art résistante aux attaques par force brute ; - la génération des identifiants spécifiques aux espaces de travail via une fonction de hachage cryptographique à l'état de l'art résistant aux attaques par force brute ; - la mise en place d'outils permettant la détection de comportements anormaux ; - la journalisation des requêtes dans les bases de données ; - la mise en place d'une authentification multifacteur ; - la mise en place d'un bastion spécifique ; - la migration d'une application de pilotage et de production d'indicateurs hors du périmètre de l'entrepôt. Les mesures de sécurité, qui devront être opérationnelles lors de la mise en œuvre du traitement, devront répondre aux exigences prévues par les articles 5,1, f) et 32 du règlement général sur la protection des données compte tenu des risques identifiés par le responsable de traitement. Il appartiendra au responsable de traitement de procéder à une réévaluation régulière des risques pour les personnes concernées et une mise à jour, le cas échéant, de ces mesures de sécurité.

AUTORISE, le CENTRE HOSPITALIER UNIVERSITAIRE DE MONTPELLIER à mettre en œuvre le traitement décrit ci-dessus.

Thomas DAUTIEU

Signature numérique de Thomas DAUTIEU
Date : 2024.08.02 16:07:25 +02'00'