

Date de publication sur legifrance: 23/10/2018

Commission Nationale de l'Informatique et des Libertés

Délibération n°2018-295 du 19 juillet 2018

Délibération n° 2018-295 du 19 juillet 2018 autorisant le Centre Hospitalier Universitaire de Nantes à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé EHOP. (Demande d'autorisation n° 2129203)

La Commission nationale de l'informatique et des libertés,
Saisie par le Centre Hospitalier Universitaire de Nantes d'une demande d'autorisation concernant un traitement automatisé de données à caractère personnel ayant pour finalité 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 la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-II-8° et 54 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié 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 ;

Sur la proposition de Mme Valérie PEUGEOT, commissaire, et après avoir entendu les observations de Mme Nacima BELKACEM, commissaire du Gouvernement,

Responsable du traitement	Le Centre Hospitalier Universitaire de Nantes (ci-après, le CHU de Nantes)
Sur la base légale et la finalité	Le CHU de Nantes souhaite disposer, à l'instar d'autres établissements de santé, d'un système d'information commun, sous la forme d'un entrepôt de données de santé, dénommé entrepôt EHOP. 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). Le traitement envisagé a pour finalité de constituer un entrepôt de données à caractère personnel comprenant notamment des données de santé.

	Ce dernier vise à permettre ultérieurement la réalisation, dans le domaine de la recherche, des activités suivantes : · dénombrement, faisabilité d'essais cliniques ; · (activité nécessitant l'identité complète des patients car visant à les recontacter pour proposition de participation à un essai clinique) ; · réalisation d'études non interventionnelles/observationnelles rétrospectives ; · épidémiologie ; · recherche en population ; · études médico-économiques ; · repérage de clusters, de cohortes ; S'agissant des finalités hors recherches, l'entrepôt EHOP vise à permettre les activités suivantes : · appui à la prise de décision médicale dans le cadre d'une médecine personnalisée; · maîtrise des vigilances et des risques ; · optimisation de l'organisation des soins et pilotage stratégique, médical et économique ; · évaluation de l'activité, des pratiques, études en santé publique ; · pour le Département d'Information Médicale : optimisation financière du codage, évaluation, recherche ; · validations techniques. La Commission relève qu'une gouvernance spécifique est prévue pour l'entrepôt. Ainsi, chaque protocole sera revu par le comité d'évaluation de la clinique des données, qui évaluera la pertinence scientifique et éthique des projets. 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 8-II 8° et 54 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 cependant 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 et les traitements de données de santé justifiés par l'intérêt public sont des traitements distincts qui devront faire l'objet de formalités propres au titre du chapitre IX 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 de Nantes, y compris les patients pris en charge avant la constitution de l'entrepôt, ainsi qu'aux professionnels de santé. <i>Les données relatives aux patients:</i> Les données relatives aux patients, issues du programme de médicalisation des systèmes d'information (PMSI) local, du dossier médical, infirmier et du dossier administratif, sont les suivantes : · Des données d'identification : · nom de jeune fille ; · date de naissance ; · numéro IPP ; · téléphone : il sera possible techniquement de désactiver la collecte de cette information. Cependant, celle-ci est indispensable pour recontacter les patients dans le cadre de <i>screening</i> d'étude, ainsi que pour les informer et leur demander leur non-opposition à l'utilisation de leurs données dans une étude ; · adresse postale et coordonnées de celle-ci (latitude et longitude) feront l'objet d'un post-traitement réalisé dans l'entrepôt ; cette fonctionnalité n'est pour l'instant pas activée dans l'architecture applicative prévue au CHU de Nantes mais permettra à terme de réaliser le <i>screening</i> lorsqu'une étude comprend un critère de recrutement des patients sur une aire géographique ; · adresse électronique ; · date de décès, civilité ; · pays et code postal de naissance ;

	· données de santé issues du dossier patient informatisé et du logiciel de soin ; · le cas échéant, données génétiques et génomiques issues de recherches antérieures non liées aux soins. Les dossiers patients classés en confidentialité ou hyper confidentialité , comprenant notamment les dossiers des personnes détenues et prises en charge au sein de l'établissement, ne figureront pas dans l'entrepôt. <i>Les données relatives aux professionnels de santé et aux utilisateurs :</i> Données d'identification dans l'entrepôt : nom, prénom, adresse électronique, téléphone, affiliation (service, établissement), nom et prénom du référent. Données d'identification des utilisateurs de l'entrepôt : nom, prénom, adresse électronique, login. 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	Les membres de l'équipe de soins, telle que définie par les dispositions de l'article L. 1110-12 du code de la santé publique, auront accès à l'ensemble des données contenues dans l'entrepôt concernant les patients qu'ils prennent en charge. Les professionnels membres du département d'information médicale (DIM) auront accès aux données dans le cadre de leurs missions actuelles. Les données des professionnels de santé sont destinées aux administrateurs de l'application, qui sont les utilisateurs du logiciel EHOP. Ces données intègrent les données d'identification dans l'entrepôt et les

	données d'identification des utilisateurs de l'entrepôt. Concernant les projets de recherche ultérieurs, les chercheurs et membres des équipes des chercheurs (biostatisticiens, ARC de monitoring, data managers...) n'appartenant pas à l'équipe de soins auront accès aux données indirectement identifiantes de l'entrepôt, dans la limite des données strictement nécessaires et pertinentes au regard de leurs fonctions. Seul le personnel habilité du CHU de Nantes, regroupé dans une cellule dédiée, pourra accéder à l'entrepôt, dans les limites de l'exercice des missions qui lui sont confiées. La Commission prend acte que seules des données codées ou anonymisées pourront faire l'objet de transfert hors de l'UE. La Commission considère que les catégories de destinataire n'appellent pas d'observation.
Sur l'information et les modalités d'exercice des droits	<i>S'agissant des patients :</i> Les personnes admises au CHU de Nantes postérieurement à la présente autorisation seront informées du traitement de données les concernant réalisés dans le cadre de la constitution de l'entrepôt, au moyen d'une note d'information remise en main propre lors de leur admission. Les personnes seront également informées par le biais d'un livret d'accueil lors de leur hospitalisation et par voie d'affichage dans les locaux des établissements. Les personnes admises préalablement à la présente autorisation seront informées de la constitution de l'entrepôt et des études menées à partir des données de l'entrepôt par le biais de campagnes d'information (réseaux sociaux, médias régionaux, communiqué de presse), des manifestations publiques au sein du CHU de Nantes et des affichages au sein de l'établissement qui renverront au site internet du CHU de

	Nantes. Le responsable de traitement envisage la publication d'une information sur son site internet afin d'annoncer la constitution de l'entrepôt et précisant que tout patient pris en charge par le CHU de Nantes, comprenant également les patients pris en charge antérieurement, peut s'opposer à l'utilisation de ses données dans l'entrepôt, ainsi qu'à des fins de recherche ultérieur. La note précisera que les patients ont la possibilité de s'opposer à la réutilisation de leurs données à des fins de recherche. L'existence et les modalités d'exercice des droits des personnes seront également détaillées. 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. La Commission relève par ailleurs que les patients sont informés de l'éventualité de l'utilisation des données à des fins de recherche dans le domaine de la santé. Elle rappelle que cette information générale ne peut se substituer à l'information individuelle prévue par les dispositions de l'article 58 de la loi Informatique et Libertés et qui devra être réalisée pour chaque traitement de données réalisé à partir des données de l'entrepôt, en application des dispositions du chapitre IX de la loi informatique et libertés . Les droits des personnes concernées, dont l'existence est rappelée dans les documents d'information, s'exerceront auprès du directeur de l'établissement ou du groupe hospitalier, ou en adressant un courriel à une adresse spécifique mentionnée sur les documents d'information. Concernant les modalités d'exercice du droit d'opposition, la Commission relève que le support d'information mentionne que les personnes peuvent s'opposer à l'utilisation des données les concernant pour la recherche, quel que soit le motif de l'opposition.
--	--

	Dans la mesure où l'article 57 de la loi Informatique et Libertés prévoit une faculté de s'opposer au traitement des données à caractère personnel sans motif, la Commission demande que la note d'information soit clarifiée afin de ne pas laisser supposer qu'un motif d'opposition à l'utilisation des données dans le cadre des recherches devrait être fourni. <i>S'agissant des professionnels de santé :</i> L'information leur sera délivrée dans l'application utilisée pour collecter les données et par une mention visible dans l'interface de l'utilisateur lors de chaque export de données. Une information générale ainsi qu'une information en Commission médicale d'établissement (CME) seront réalisées et diffusées à tous les professionnels. La Commission demande que les supports d'information soient complétés afin de contenir l'ensemble des mentions prévues par l'article 13 du RGPD. Sous réserve de la modification des documents d'information, 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 le CHU de Nantes d'une étude 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. S'agissant de l'accès à l'entrepôt de données de santé, la Commission observe que celui-ci se déroule en deux étapes. Dans un premier temps, les utilisateurs doivent remplir une demande à partir d'un portail accessible par Internet, spécifiant ainsi les jeux de données auxquels ils souhaitent accéder. La Commission prend note que pour cela, chaque utilisateur dispose d'un espace personnel et qu'une politique d'authentification reposant sur un

identifiant individuel et un mot de passe est mise en place pour y accéder. A cet égard, elle rappelle qu'une politique satisfaisante de mot 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.

Une fois une demande effectuée et celle-ci validée par les administrateurs de l'entrepôt, les utilisateurs sont autorisés à consulter les jeux de données. La Commission relève que la consultation et la manipulation des données n'est réalisable qu'à partir du réseau informatique interne du CHU de Nantes.

Ainsi, afin d'accéder aux sous-ensembles de données demandés, les utilisateurs de l'entrepôt doivent s'authentifier à l'aide d'une carte à puce individuelle et d'un code à quatre chiffres.

La Commission observe que des profils d'habilitation définissent donc les accès, rôles et informations disponibles aux différents utilisateurs de l'entrepôt. La création de chaque sous-ensemble de données est conditionnée à une durée d'utilisation. Les permissions d'accès sont donc supprimées pour tout utilisateur n'étant plus habilité. Une revue globale des habilitations est opérée de façon régulière afin de s'assurer du bon effacement des habilitations.

La Commission prend note que seul un petit ensemble de personnes est habilité à accéder à l'entrepôt dans son intégralité afin de l'administrer et de gérer les demandes d'accès des utilisateurs. S'agissant de l'accès à l'entrepôt pour ces personnels, la Commission observe qu'outre une authentification par carte à puce individuelle et code à quatre chiffres, un couple identifiant/mot de passe est utilisé. Elle rappelle que la politique de mot de passe doit suivre les recommandations citées précédemment.

La Commission note qu'en fonction des demandes qui seront effectuées auprès des

différents comités impliqués dans la gouvernance de l'entrepôt (comité stratégique, comité opérationnel, comité d'évaluation), les données pourront faire l'objet d'agrégation pour permettre la production de statistiques ou être pseudonymisées afin de ne fournir aux utilisateurs que les seules données strictement nécessaires aux besoins des recherches.

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. En particulier, la Commission rappelle la nécessité d'écarter toute donnée identifiante comme le prénom, nom, nom de jeune fille, adresse postale, adresse électronique, numéro de téléphone, date de naissance/décès, lieu de naissance/décès, NIR, numéro de visite, identifiant technique, etc. La Commission prend note que la pseudonymisation sera réalisée à l'aide d'algorithmes de hachage à clé secrète. Elle rappelle la nécessité d'utiliser des algorithmes à l'état de l'art et de mettre en œuvre des procédures de gestion de clés adaptées, permettant de se prémunir des attaques par force brute. La Commission observe qu'en cas de nécessité, il est techniquement possible de ré-identifier un patient, par exemple pour revenir vers lui et sous réserve que cette opération soit autorisée.

Il est de plus 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 faite avec vigilance, notamment si elle met en œuvre des outils automatisés et donc pour lesquels des erreurs sont susceptibles d'advenir.

La Commission prend note qu'en cas de

nécessité, par exemple à des fins de collaboration avec des partenaires externes au CHU de Nantes, les données peuvent faire l'objet d'une anonymisation afin d'être communiquées. La Commission rappelle qu'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, et de la transmettre à la Commission. À défaut, si ces trois critères ne pouvaient 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.

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 Nantes à partir d'un navigateur web. 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.

Des mesures sont prévues pour assurer le cloisonnement du traitement. Le réseau de l'entreprise 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. Enfin, un système de prévention d'intrusion est mis en place et des tests sont régulièrement réalisés.

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. La Commission prend note que le CHU de Nantes est hébergeur agréé de données de santé dans les conditions du décret n°2006-6 du 4 janvier 2006. 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 les autres caractéristiques du traitement	Le CHU de Nantes souhaite conserver les

	données contenues dans l'entrepôt pendant la durée prévue par les dispositions légales et réglementaires applicables en matière de conservation des dossiers médicaux de 20 ans. Concernant les recherches, l'accès aux données de l'entrepôt par les demandeurs est limité à ce qui est nécessaire à l'étude ou l'analyse. Le CHU de Nantes a précisé que les extractions réalisées pour des recherches impliquant la personne humaine seraient détruites au bout de 15 ans d'archivage. La commission considère que 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.
--	--

Autorise, conformément à la présente délibération, le CHU de Nantes à mettre en œuvre le traitement susmentionné.

Pour la Présidente

Le Vice-Président délégué

Marie-France MAZARS

Nature de la délibération: AUTORISATION