

Date de publication sur legifrance: 27/03/2019

Commission Nationale de l'Informatique et des Libertés

DELIBERATION n°2018-369 du 20 DECEMBRE 2018

Délibération n° 2018-369 du 20 décembre 2018 autorisant la société Compugroup Medical Solutions à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé

(Demande d'autorisation n° 2135377)

La Commission nationale de l'informatique et des libertés,

Saisie par la société Compugroup Medical Solution 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, 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 Eve JULLIEN, adjoint au commissaire du Gouvernement,

Formule les observations suivantes :

Responsable du traitement

La société Compugroup Medical Solutions, société par actions simplifiée (ci-après, la société CGM ou CGM), propose des logiciels d'aide à la prescription destinés aux professionnels de santé.

Sur la base légale et la finalité

La société CGM envisage de créer un entrepôt de données de santé pseudonymisées à destination d'organismes publics ou privés aux fins de mener des études observationnelles dans le domaine de la santé.

L'entrepôt a vocation à permettre de mener des études observationnelles portant sur des pathologies ou des pratiques de soins commandées par des organismes publics (tels que instituts ou centres de recherche) ou privés (tels que des laboratoires pharmaceutiques) auprès de CGM.

Plus précisément, les études observationnelles porteront sur l'évaluation de pratiques de

soins, l'efficacité d'un médicament sur une période définie ou l'établissement de statistiques à partir de données préalablement anonymisées afin de produire des indicateurs d'activité.

L'entrepôt est constitué à partir des données transmises, sous la forme pseudonymisée, par des professionnels de santé utilisant les progiciels AxiSanté ou HelloDoc édités par CGM. CGM génère à partir de ces données des résultats agrégés et anonymisés, à destination d'organismes publics ou privés souhaitant réaliser des études observationnelles dans le domaine de la santé.

Un comité est chargé d'examiner les projets de recherche des clients de la société CGM afin de garantir le caractère d'intérêt public des utilisations à venir des données. Ce comité sera géré par un professionnel de santé, salarié de CGM, et sera composé de personnes extérieures à la société.

Le traitement a pour base légale l'article 6, 1. f) du Règlement général sur la protection des données (ci-après RGPD), intérêts légitimes poursuivis par le responsable de traitement.

La Commission considère que la finalité du traitement présentée 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 en ce que l'entrepôt permettrait de connaître l'évolution de la prise en charge de la population atteinte d'une même pathologie et d'agir sur les pratiques de soins en matière de politique de santé.

La Commission tient à rappeler que les utilisations futures des données contenues dans cet entrepôt s'inscrivent dans le cadre des dispositions du chapitre IX de la loi, qui lui impose que chaque demande de recherche, étude ou évaluation réponde à une exigence d'intérêt public. Ainsi, la Commission estime que l'utilisation des données contenues dans le traitement qui sera mis en œuvre par CGM ne saurait, par analogie aux finalités « interdites » d'utilisation du système national des données de santé (SNDS), être exploitées à des fins de promotion des produits de santé en direction des professionnels de santé ou d'établissements de santé ou à des fins d'exclusion de garanties des contrats d'assurance et de modification de cotisations ou primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

De même, la Commission rappelle l'interdiction de constituer et d'utiliser, à des fins de prospection ou de promotion commerciales, des fichiers composés à partir des données issues directement ou indirectement des prescriptions médicales, dès lors que ces fichiers permettent d'identifier directement ou indirectement le prescripteur (art. L. 4113-7 du code de la santé publique).

Enfin, 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 de la section II 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 les professionnels de santé utilisant, dans le cadre de leur activité, les logiciels édités par le responsable de traitement ainsi qu'aux professionnels de santé.

Les données relatives aux patients sont les suivantes:

des données d'identification : le genre, la tranche d'âge, l'identifiant unique généré à partir du nom, prénom, date et rang de naissance, sexe et département ;
des données de santé : les données de biologie, les pathologies, les informations relatives à la prescription, la date de la dernière consultation chez un spécialiste, le statut tabagique, l'activité physique, la vaccination.

Les données relatives aux professionnels de santé sont les nom, prénom, adresse professionnelle et numéro RPPS.

La Commission prend acte que le dossier précise qu'aucun traitement du NIR n'est envisagé par la société CGM.

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 à la protection des données.

Sur les destinataires

Les clients visés par la société CGM sont des industriels du secteur de la santé ou des organismes publics de recherche.

La Commission relève que les clients de CGM ne seront destinataires d'aucune donnée individuelle relative aux patients des professionnels de santé. Seule CGM sera en mesure d'analyser ces données sous la forme pseudonymisée et n'envisage une communication de résultats que sous la forme anonymisée au sens des critères de l'avis du G29.

Ont accès aux données pseudonymisées de l'entrepôt, le personnel habilité de CGM et la société sous-traitante de CGM.

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

Sur l'information et le droit d'accès S'agissant des patients :

Les professionnels de santé seront chargés contractuellement d'informer leurs patients du traitement des données les concernant dans le cadre de l'entrepôt, ainsi que de permettre l'exercice des droits d'accès, de rectification et d'opposition qui leur sont reconnus.

Il est prévu que les personnes soient informées individuellement par la remise à chacun des patients concernés d'un dépliant et par l'affichage d'un document dans la salle d'attente ou d'accueil du cabinet médical.

La Commission prend acte que l'exercice des droits d'accès, de rectification et

d'opposition du patient s'exercera auprès du professionnel de santé en charge de leur suivi ou auprès de la société Compugroup. Elle prend acte de la suppression de l'ensemble des données collectées en cas d'exercice du droit d'opposition.

S'agissant des professionnels de santé :

Les logiciels édités par CGM prévoient l'information préalable et le recueil du consentement du professionnel de santé avant l'installation du module permettant la pseudonymisation et le transfert des données vers l'entrepôt.

Les droits des personnes concernées s'exercent auprès du délégué à la protection des données du responsable de traitement par l'envoi d'un courriel ou d'un courrier.

La Commission rappelle que l'information des personnes devra être conforme aux articles 12, 13 et 14 du RGPD. Sous cette réserve, elle considère les modalités d'information et d'exercice des droits satisfaisantes.

Sur les mesures de sécurité

Les données recueillies par les professionnels de santé sont remontées vers l'entrepôt depuis un module spécifiquement développé en lien avec le logiciel des praticiens.

Les données qui sont extraites et envoyées dans la base de données centralisée sur le serveur CGM Data sont pseudonymisées.

Un identifiant unique associé au patient a été construit à partir de plusieurs champs ajoutés à un aléa avec une méthode de hachage de type SHA 256.

La base de données pseudonymisées est centralisée et hébergée par une filiale du responsable de traitement dont l'infrastructure a obtenu un agrément HDS.

Les données sont transmises dans l'entrepôt via un canal de communication chiffré (HTTPS).

Les données font ensuite l'objet d'une anonymisation (technique de généralisation par agrégation et k-anonymat). La Commission rappelle que, pour se prévaloir de l'anonymat d'un jeu de données, le responsable de traitement doit respecter les trois critères de l'avis n°05/2014 sur les techniques d'anonymisation adoptés par le groupe de l'Article 29 (G 29) le 10 avril 2014. Cette conformité nécessite d'être revues régulièrement au vu des évolutions des techniques d'anonymisation et de réidentification.

En outre, la Commission appelle le responsable de traitement à une vigilance quant à la présence de données permettant l'identification pouvant se trouver dans des documents conservés dans des formats non textuels.

Les utilisateurs sont authentifiés au moyen d'un mot de passe.

La Commission rappelle que, conformément à sa délibération n°2017-190 du 22 juin 2017 portant modification de la recommandation relative aux mots de passe, elle demande que ces derniers fassent une longueur minimale de douze caractères et soient composés de lettres majuscules, minuscules, chiffres et symboles ou qu'ils fassent entre huit et onze caractères, soient composés de trois des quatre possibilités précitées et associés à une restriction d'accès en cas d'erreurs successives (blocage temporaire de compte,

possibilité de nouvelles tentatives après une durée d'attente incrémentielle, etc.).

Ils doivent en outre être définis, ou modifiés dès la première connexion, par l'utilisateur, puis régulièrement renouvelés et ne doivent pas être stockés en clair.

Les actions des utilisateurs accédant à l'entrepôt font l'objet de mesures de traçabilité.

Un cloisonnement du traitement est réalisé notamment au moyen d'une séparation des communications réseaux.

Une politique de sauvegarde est mise en œuvre.

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

Les données sont conservées pendant les 6 mois suivant la fin du projet de recherche réalisé puis archivées pendant 10 ans.

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, la société Compugroup Medical Solutions à mettre en œuvre le traitement décrit ci-dessus, et rappelle que les traitements de données à caractère personnel qui seront mis en œuvre ultérieurement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé sont des traitements distincts qui doivent faire l'objet de formalités propres prévues à la section 2 du chapitre IX de la loi.

Pour la Présidente Le Vice-Président délégué

Marie-France MAZARS

Nature de la délibération: Autorisation