Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Legifrance.gouv.fr
LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT

Commission Nationale de l'Informatique et des Libertés

Délibération n°2017-013 du 19 janvier 2017

Délibération n° 2017-013 du 19 janvier 2017 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé « EDS ». (demande d'autorisation n° 1980120)

Etat: VIGUEUR

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 un entrepôt de données, dénommé EDS ;

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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative 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 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-IV et 25-I-1° ;

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 ;

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

Formule les observations suivantes :

L'Assistance publique - Hôpitaux de Paris (AP-HP) souhaite disposer d'un système d'information commun, sous la forme d'un entrepôt de données, dénommé Entrepôt de données de santé (EDS). L'EDS vise à faciliter la réalisation de recherches dans le domaine de la santé et d'études relatives au pilotage hospitalier en regroupant dans une base unique l'ensemble des données de soins recueillies auprès des patients hospitalisés dans l'un des 39 établissements, répartis au sein de 12 groupes hospitaliers.

Pour l'année 2015, l'AP-HP indique que près de 100 000 professionnels (dont 12 500 médecins, 4 920 internes, 56 820 personnels soignants) ont pris en charge 8 millions de patients en son sein.

La constitution de cet entrepôt, impliquant adhésion de la Direction générale, de la Commission médicale d'établissement et du Directoire de l'AP-HP, représente donc l'opportunité de fournir aux professionnels impliqués dans la recherche un outil d'investigation unique au niveau national et favorisant les partenariats. La Commission relève par ailleurs qu'un Comité scientifique et éthique de l'AP-HP sera en charge de l'évaluation de projets de recherche et autorisera l'accès aux données de l'EDS dans ce cadre, avant la réalisation des formalités préalables nécessaires auprès d'elle.

L'EDS permettra la réalisation :

· de recherches non interventionnelles sur données, réalisées par les professionnels de santé AP-HP des équipes de soins et portant sur des données des patients qu'ils prennent directement en charge ;

· de recherches non interventionnelles sur données, réalisées par des personnels de l'AP-HP et éventuellement des tiers hors AP-HP et portant sur les données de patients pris en charge sur un périmètre de plusieurs services ou hôpitaux, voire des patients de l'ensemble de l'AP-HP (études multicentriques). Les recherches non interventionnelles multicentriques sur les données de l'EDS feront l'objet d'une demande d'autorisation au Comité scientifique et éthique de l'AP-HP, avant la réalisation des formalités préalables nécessaires auprès de la Commission. ;

· d'études réalisées par les personnels AP-HP des départements d'information médicale (DIM) dans le cadre de leurs missions (articles L. 6113-7, L. 6111-8 et R. 6113-1 et suivants du Code de la santé publique) ;

· d'études de faisabilité d'essais cliniques réalisées par un nombre limité de personnels de l'AP-HP suivant le périmètre géographique (ex : personnel du DIM siège ou du groupe hospitalier). Il s'agit des études de détermination du nombre de patients pris en charge dans les hôpitaux de l'AP-HP et susceptibles de remplir des critères d'inclusion et de non inclusion d'une étude de recherche biomédicale interventionnelle ou non interventionnelle (suivi de cohorte). Le résultat est un nombre de patients correspondant à l'étude de faisabilité (données agrégées). Ces études feront l'objet d'une demande d'autorisation au Comité scientifique et éthique de l'AP-HP, avant la réalisation des formalités préalables nécessaires auprès de la Commission.

Sur la finalité du traitement :

Le traitement envisagé a pour finalité de constituer un entrepôt de données à caractère personnel, comprenant notamment des données de santé, afin de permettre ultérieurement la réalisation :

· de recherches dans le domaine de la santé non interventionnelles par les personnels de l'AP-HP (professionnels de santé, chercheurs) éventuellement associés à des partenaires extérieurs à l'AP-HP ;

· la réalisation d'études de faisabilité d'essai cliniques ;

· la réalisation d'études relatives au pilotage médical et stratégique visant à optimiser l'organisation des soins, réalisées par les médecins des DIM de l'AP-HP dans le cadre de leurs missions.

La Commission considère que les finalités poursuivies sont déterminées, légitimes et explicites, conformément aux dispositions de l'article 6-2° de la loi du 6 janvier 1978 modifiée (loi Informatique et Libertés).

Elle estime qu'il y a lieu de faire application des dispositions combinées des articles 8-IV et 25-I-1° de la loi Informatique et Libertés, qui soumettent à autorisation les traitements comportant des données relatives à la santé et justifiés 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 d'études/recherches dans le domaine de la santé, sont des traitements distincts qui doivent faire l'objet de formalités propres au titre du chapitre IX de la loi Informatique et Libertés.

Enfin, la Commission observe que l'AP-HP envisage d'utiliser ultérieurement l'EDS pour d'autres finalités que celles décrites ci-dessus (notamment en tant qu'outil d'aide à la décision médicale, de maîtrise des vigilances et des risques, ou de codage PMSI (Programme de médicalisation des systèmes d'information)). La Commission rappelle que de telles utilisations constitueraient des modifications substantielles de la finalité du traitement qui devraient lui être soumises préalablement.

Sur la nature des données traitées :

Les données dont le traitement est envisagé sont relatives aux patients hospitalisés à l'AP-HP, comprenant également les patients hospitalisés antérieurement à la constitution de l'EDS, ainsi qu'aux professionnels de santé.

S'agissant des données relatives aux patients :

· Données d'identification accessibles uniquement à l'équipe de soins telle que définie par les dispositions de l'article L. 1110-4 du code de la santé publique et au médecin du DIM du groupe hospitalier : nom, prénom, adresse, date et lieu de naissance. Ces données ne pourront être utilisées qu'afin :

o d'avertir une personne d'un risque sanitaire grave auquel elle est exposée ;

o de proposer à la personne concernée de participer à une recherche ;

o de réaliser un traitement à des fins de recherche, d'étude ou d'évaluation, si le recours à ces données est nécessaire à la finalité du traitement, sans solution alternative.

· Données dont le traitement est autorisé par la méthodologie de référence 003, homologuée par la Commission dans la délibération n° 2016-263 du 21 juillet 2016. Ces données seront accessibles à l'équipe de soins et aux professionnels n'appartenant pas à l'équipe de soins, dans le cadre de projets de recherche ou d'études, dans la limite des données strictement nécessaires et pertinentes au regard des objectifs de la recherche ou de l'étude :

o numéro d'ordre ou code alphanumérique ;

o santé : les données strictement nécessaires à la réalisation de la recherche et relatives à la santé de la personne qui s'y prête, par exemple : poids, taille, thérapie suivie dans le cadre de la recherche et concomitante, résultats d'examens, suivi et traitement des données relatives aux effets et événements indésirables survenant au cours de la recherche, antécédents personnels ou familiaux, maladies ou événements associés ;

o informations signalétiques : âge ou date de naissance (mois et année de naissance, voire jour de naissance si ce dernier est nécessaire à la réalisation d'une recherche impliquant des personnes âgées de moins de deux ans), lieu de naissance, sexe ;

o images : photographie et/ou vidéo ne permettant pas l'identification des personnes se prêtant à la recherche (par exemple avec masquage du visage, des signes distinctifs) et recueillies dans des conditions conformes aux dispositions applicables en matière de droit à l'image et de droit à la voix ;

o dates relatives à la conduite de la recherche (notamment la date d'inclusion et les dates de visites) ;

o origine ethnique ;

o données génétiques strictement nécessaires pour répondre aux objectifs ou finalités de la recherche, ne permettant pas par elles-mêmes une identification directe ou indirecte de la personne. Ces données ne pourront en aucun cas être utilisées aux fins d'identification ou de réidentification des personnes ;

o situation familiale ;

o niveau de formation (par exemple, primaire, secondaire, supérieur) ;

o catégorie socioprofessionnelle (par exemple, les catégories INSEE) ;

o vie professionnelle : profession actuelle, historique, chômage, trajets et déplacements professionnels ;

o régime d'affiliation à la sécurité sociale à l'exclusion du numéro d'inscription au Répertoire national d'identification des personnes physiques, assurance complémentaire (mutuelle, assurance privée) ;

o participation à d'autres recherches ou études (oui ou non) ;

o déplacements (vers le lieu de soin : mode, durée, distance) ;

o consommation de tabac, alcool, drogues ;

o habitudes de vie et comportements, par exemple : dépendance (seul, en institution, autonome, grabataire), assistance (aide-ménagère, familiale), exercice physique (intensité, fréquence, durée), régime et comportement alimentaire ;

o mode de vie : par exemple urbain, semi-urbain, nomade, sédentaire ; habitat (maison particulière ou immeuble, étage, ascenseur, etc.) ;

o vie sexuelle ;

o statut vital, lorsque cette information figure dans le document source ;

o montant annuel des indemnités perçues ;

o échelle de qualité de vie.

La Commission relève que différents niveaux de présentation des données sont envisagés, en fonction des habilitations des professionnels susceptibles d'accéder aux données de l'EDS : données agrégées, données anonymisées, données pseudonymisées, données directement identifiantes. Le niveau d'habilitation variera en fonction de l'appartenance à l'équipe de soins, ou encore de la qualité de membre du personnel de l'AP-HP et sera défini par le responsable de traitement s'agissant des données agrégées, des données anonymisées et des données pseudonymisées.

En application de l'article 6-4° de la loi Informatique et Libertés, la Commission souligne l'importance de la mise à jour des données et par conséquent de la synchronisation des données conservées dans l'EDS avec celles issues des bases de données opérationnelles l'alimentant.

S'agissant des professionnels de santé :

Seul le matricule fera l'objet d'un traitement, en tant qu'identifiant de connexion.

La Commission considère que les données dont le traitement est envisagé sont adéquates, pertinentes et non excessives au regard des finalités du traitement, conformément à l'article 6-3° de la loi du 6 janvier 1978 modifiée.

Sur la durée de conservation des données :

Les données seront conservées dans l'entrepôt pendant la durée prévue par les dispositions légales et règlementaires applicables en matière de conservation des dossiers médicaux.

Par ailleurs, les données à caractère personnel extraites de l'EDS pour être traitées dans le cadre de projets de recherche ne pourront être conservées que jusqu'à la publication des résultats de la recherche.

La Commission estime que cette durée de conservation des données n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, conformément aux dispositions de l'article 6-5° de la loi Informatique et Libertés.

Sur les destinataires des données :

Les membres de l'équipe de soins, telle que définie par les dispositions de l'article L. 1110-4 du code de la santé publique, auront accès à l'ensemble des données contenues dans l'EDS concernant les patients qu'ils prennent en charge.

Les professionnels membres du DIM auront accès aux données nécessaires à l'exercice de leurs missions concernant les patients pris en charge au sein du ou des établissements dans lesquels ces missions s'exercent.

Par ailleurs, des chercheurs (personnels de l'AP-HP éventuellement associés à des partenaires extérieurs à l'AP-HP) auront accès aux données de l'EDS, à l'exclusion des données directement identifiantes lorsqu'ils ne sont pas membres de l'équipe de soins, dans la limite des données strictement nécessaires et pertinentes au regard des objectifs de la recherche ou de l'étude.

Ces destinataires n'appellent pas d'observation de la Commission.

Sur l'information et les droits des personnes concernées :

S'agissant des patients :

Les personnes concernées sont informées du traitement de données les concernant réalisé dans le cadre de la constitution de l'EDS, au moyen du livret d'accueil et par voie d'affichage dans les locaux des établissements.

Le responsable de traitement envisage la publication d'une information sur son site web afin d'annoncer la constitution de l'EDS et précisant que tout patient pris en charge à l'AP-HP, comprenant également les patients pris en charge antérieurement, peut s'opposer à l'utilisation de ses données dans le cadre de recherches. L'existence et les modalités d'exercice des droits des personnes seront également détaillées.

Les patients admis postérieurement à la constitution de l'EDS seront informés lors de la préadmission ou de l'admission dans un établissement de l'AP-HP par la remise d'un document écrit.

La Commission relève que les supports d'information qui lui ont été remis à l'appui de la demande de l'AP-HP ne font pas explicitement mention de la constitution de l'EDS et des finalités spécifiques de la constitution de ce dernier, du droit des personnes de définir des directives relatives au sort des données à caractère personnel après leur mort et de la durée de conservation des catégories de données traitées ou des critères permettant de déterminer cette durée.

Elle demande que les supports d'information soient complétés sur ces points, conformément aux dispositions de l'article 32 de la loi Informatique et Libertés.

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 57 de la loi Informatique et Libertés et qui devra être réalisée pour chaque projet de recherche.

Elle rappelle en outre que, dans le cas où la réalisation d'une recherche nécessiterait qu'il soit dérogé à l'obligation d'information individuelle de la personne concernée, la recherche ne pourra être réalisée dans le cadre d'une méthodologie de référence et devra faire l'objet d'une demande d'autorisation spécifique auprès de la Commission.

S'agissant des droits d'accès, de rectification et d'opposition des personnes concernées, dont l'existence est rappelée dans les documents d'information, ils 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 56 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.

S'agissant des professionnels de santé :

L'information leur sera délivrée par une mention figurant 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.

Sous réserve de la modification des documents d'information, la Commission considère que ces modalités d'information et de recueil du consentement sont satisfaisantes.

Sur la sécurité des données et la traçabilité des actions :

S'agissant des professionnels utilisateurs de l'EDS, la Commission observe que la politique d'authentification repose sur un identifiant individuel et un mot de passe d'une longueur minimum de huit caractères. A cet égard, elle rappelle qu'une politique satisfaisante de mot de passe implique que ceux-ci soient composés de huit caractères minimum, comprenant au moins trois des quatre types de caractères suivants : majuscules, minuscules, chiffres et caractères spéciaux.

S'agissant des administrateurs techniques et fonctionnels de l'AP-HP chargés de la mise en œuvre et du bon fonctionnement de l'EDS, la Commission rappelle que la composition des mots de passe doit respecter les mêmes exigences de complexité que pour les professionnels utilisateurs et de surcroît, présenter une longueur minimum de dix caractères.

Des mesures d'audit de la complexité des mots de passe sont mises en œuvre afin d'identifier les mots de passe faibles et de demander leur modification. Pour limiter les possibilités d'accès frauduleux, les utilisateurs sont invités à renouveler leurs mots de passe tous les six mois et un blocage du compte d'un utilisateur est réalisé après un nombre fixé de tentatives. De plus, un outil d'analyse des erreurs d'authentification sera déployé.

La Commission observe que des profils d'habilitation définissent les accès, rôles et informations disponibles aux différents utilisateurs de l'EDS. Les permissions d'accès sont supprimées pour tout utilisateur n'étant plus habilité et une revue globale des habilitations est opérée tous les six mois.

La Commission relève qu'en fonction des habilitations délivrées, quatre niveaux d'accès aux données sont proposés : données agrégées, données anonymisées, données pseudonymisées et données directement identifiantes. La Commission prend note que le processus d'anonymisation des données n'est pas encore défini. Elle n'est donc pas en mesure de se prononcer sur la validité de ce dernier et demande à être saisie d'une demande d'autorisation pour la mise en œuvre du traitement de données à caractère personnel ayant pour finalité l'anonymisation.

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.

Des procédures d'export sont définies pour extraire des données de l'EDS. Des règles d'encadrement strictes de ces pratiques et des mesures de traçabilité sont mises en œuvre. La Commission relève que les données éligibles pour des procédures d'export sont les données pseudonymisées et directement identifiantes, soit les données les plus identifiantes (directement ou indirectement). Elle invite par conséquent l'AP-HP à la plus grande vigilance sur cet aspect et l'encourage à la mise en place d'outils techniques centralisés permettant de mener des travaux de recherche sans avoir à extraire les données de leur environnement, réduisant ainsi l'intérêt de réaliser des exports.

Les actions des professionnels de santé accédant à l'EDS font l'objet de mesures de traçabilité. Ils sont informés de celles-ci. En particulier, sont tracées les connexions à l'EDS (identifiant, date et heure), la configuration de l'outil et les requêtes réalisées. Une analyse des traces est réalisée mensuellement, permettant un suivi de l'activité.

La Commission observe que l'EDS est accessible uniquement sur le réseau interne de l'AP-HP à partir d'un navigateur web. L'accès est sécurisé au moyen du protocole HTTPS. Concernant le recours à ce protocole, la Commission recommande d'utiliser la version de TLS la plus à jour possible. Il n'y a pas d'accès possible en dehors du réseau interne de l'AP-HP, sauf pour les agents techniques en astreinte qui peuvent bénéficier d'un accès distant à des fin de télémaintenance.

Des mesures sont prévues pour assurer le cloisonnement du traitement. Le réseau de l'entreprise fait l'objet de mesure de filtrage ayant pour but de restreindre l'émission et la réception des flux réseau aux machines identifiées et autorisées.

Les accès distants sont sécurisés via un VPN chiffré. 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.

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 l'article 34 de la loi du 6 janvier 1978 modifiée.

La Commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Dans ces conditions, la Commission autorise l'Assistance publique - Hôpitaux de Paris à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité un entrepôt de données, dénommé EDS .

La Présidente

I. FALQUE-PIERROTIN

Nature de la délibération: AUTORISATION
Date de la publication sur legifrance: 4 mars 2017