Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire

(demande d'avis n° 20006669)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ;

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 ;

Vu le code de la santé publique, notamment ses articles L. 1461-1, L. 1462-1, L. 3131- 16 et L. 6113-8 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I-2-e ;

Vu la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, notamment son article 4 ;

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 décret n° 2020-293 du 23 mars 2020 modifié prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ;

Vu l'arrêté du 23 décembre 2016 modifié relatif au recueil et au traitement des données d'activité médicale et des données de facturation correspondantes, produites par les établissements de santé publics ou privés ayant une activité en médecine, chirurgie, obstétrique et odontologie, et à la transmission d'informations issues de ce traitement dans les conditions définies à l'article L. 6113-8 du code de la santé publique ;

Vu l'arrêté du 23 mars 2020 modifié prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ;

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

Émet l'avis suivant :

La Commission a été saisie le 15 avril 2020 pour avis, sur le fondement de l'article 8.I.2°-e) de la loi n° 78-17 du 6 janvier 1978 modifiée (ci-après la loi « Informatique et Libertés »), d'un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire, pris en application des dispositions de l'article L. 3131-16 du code de la santé publique (ci-après le projet).

En application de ces dispositions introduites par la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19 le ministre de la santé peut prescrire, par arrêté motivé, toute mesure réglementaire relative à l'organisation et au fonctionnement du dispositif de santé visant à mettre fin à la catastrophe sanitaire, à l'exception des mesures prévues par l'article L. 3131-15 du code de la santé publique, relevant d'un décret.

Le projet d'arrêté a pour objet, dans le contexte d'urgence lié à la gestion de la crise sanitaire actuelle, d'organiser le regroupement de certaines données à caractère personnel, comprenant des données de santé, afin de permettre leur utilisation en vue de suivre et projeter les évolutions de l'épidémie, de prévenir, de diagnostiquer et de traiter au mieux la pathologie et d'organiser le système de santé pour combattre l'épidémie et en atténuer les impacts. Il prévoit pour ce faire l'ajout dans l'arrêté du 23 mars 2020 d'un chapitre relatif aux mesures concernant le traitement des données à caractère personnel du système de santé.

Ainsi, le projet prévoit, à titre temporaire et dans le cadre spécifique de la gestion de l'urgence sanitaire :

- d'une part, d'ajouter une remontée hebdomadaire au circuit de remontée des informations d'activité médicale et des données de facturation correspondantes, produites par les établissements de santé publics ou privés ayant une activité en médecine, chirurgie, obstétrique et odontologie, prévu à l'article L. 6113-8 du code de la santé publique et par l'arrêté du 23 décembre 2016 modifié (programme de médicalisation des systèmes d'information ou PMSI) ;
- d'autre part, la centralisation au sein du groupement d'intérêt public dénommé Plateforme des données de santé, prévu par l'article L. 1462-1 du code de la santé publique (également dénommé « Health Data Hub ») de données provenant de différentes sources en vue de leur mise à disposition afin de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le COVID-19.

Tout en reconnaissant la légitimité des objectifs poursuivis par le projet, la Commission tient à rappeler, au vu de l'urgence, que quel que soit le contexte, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être mises en œuvre. Ainsi, elle estime que des mesures juridiques et techniques adaptées devront être prévues afin d'assurer un haut niveau de protection des données.

La Commission indique par ailleurs que cet avis rendu dans un délai très bref et dans un contexte de crise sanitaire mondiale exceptionnelle, ne préjuge en rien de l'analyse qu'elle produira au fond tant sur les plans juridique que technique, s'agissant de la mise en œuvre de manière pérenne de la Plateforme des données de santé, notamment à des

fins de mise à disposition des données du Système national des données de santé (SNDS), ainsi que sur le décret d'application prévu à l'article L. 1461-7 du code de la santé publique, qui sera modifié suite à l'adoption de la loi du 24 juillet 2019.

Sur la constitution d'un entrepôt de données au sein de la plateforme des données de santé

La Commission relève que la centralisation des données au sein de la Plateforme des données de santé implique la création d'un entrepôt de données de santé en vue de leur mise à disposition auprès d'autres responsables de traitements.

Les opérations de traitement liées à ce projet sont soumises au règlement (UE) n° 2016/679 du Parlement européen et du conseil du 27 avril 2016 (ci-après le RGPD) et aux dispositions pertinentes de la loi « informatique et libertés ».

La Commission prend acte du choix du ministère de créer ce traitement par la voie d'un arrêté pris dans le cadre de l'état d'urgence sanitaire. Elle rappelle toutefois que la constitution de cette base, qui s'inscrit dans un contexte particulier d'urgence et de gestion d'une crise sanitaire en cours, ne saurait être encadrée par cet arrêté que pour la période d'état d'urgence sanitaire déclaré à l'article 4 de la loi du 23 mars 2020. Au-delà, ce traitement ne disposerait plus de base légale.

Elle rappelle que des éléments essentiels concernant le fonctionnement de la plateforme en dehors du contexte de l'état d'urgence sanitaire seront précisés dans le décret en Conseil d'Etat prévu à l'article L. 1461-7 du code de la santé publique et que la centralisation de données au sein du « catalogue » de la Plateforme, qui constitue un entrepôt de données, sera soumise à autorisation préalable de la Commission, en application des dispositions des articles 44-3° et 66 de la loi « informatique et libertés ».

Sur la responsabilité de traitement

La Commission prend acte de ce que la Plateforme des données de santé et la Caisse nationale d'assurance maladie (CNAM) seront conjointement responsables des traitements décrits dans le projet. A ce titre, le projet mentionne que la Plateforme des données de santé est responsable du stockage et de la mise à disposition des données et qu'elle est autorisée à opérer des croisements de données. Le projet mentionne par ailleurs que la CNAM est responsable des opérations de pseudonymisation dans le cadre du croisement des données et peut traiter le numéro d'inscription au répertoire national d'identification des personnes physiques à cette fin.

La Commission relève cependant que le projet prévoit que les données peuvent être traitées dans la solution technique de la Plateforme des données de santé, ainsi que dans celle de la CNAM. Il en résulte que la CNAM pourrait également être amenée à stocker et à mettre à disposition des données dans le cadre du traitement envisagé.

A cet égard, la Commission prend acte de l'engagement du ministère de préciser dans le projet que la CNAM est :

- également autorisée à recevoir les données énumérées,
- responsable du stockage et de la mise à disposition des données,
- autorisée à croiser les données,
- et à mettre en œuvre des traitements répondant à ses missions au titre du 3° de l'article 65 de loi « informatique et libertés ».

Le ministère s'est par ailleurs engagé à ce qu'un accord définissant de manière transparente les obligations respectives de la Plateforme des données de santé et de la CNAM soit conclu, conformément aux dispositions de l'article 26 du Règlement général sur la protection des données. Cet accord précisera notamment les modalités de transfert des données entre la Plateforme des données de santé et la CNAM. La Commission en prend acte.

Sur la mise en œuvre de traitements ultérieurs

Le projet prévoit que seuls peuvent traiter les données ainsi rassemblées par la Plateforme des données de santé les acteurs suivants : des responsables de traitement autorisés dans les conditions prévues aux articles 66 et 76 de la loi « informatique et libertés », l'Etat mettant en œuvre des traitements mentionnés au 6° de l'article 65 ou les organismes et les services chargés d'une mission de service public mentionnés à l'article 67.

A cet égard, la Commission a été informée de ce que le ministère envisageait de prendre l'arrêté prévu par l'article 67, afin de déterminer les listes des organismes et services chargés d'une mission de service public en lien avec l'alerte sanitaire.

Elle rappelle donc qu'en dehors des organismes et services figurant sur cette liste, ainsi que l'Etat, pour les traitements prévus à l'article 65-6° de la loi « informatique et libertés », les traitements mis en œuvre à partir des données contenues dans cet entrepôt devront faire l'objet d'une demande d'autorisation auprès d'elle, qui ne pourra intervenir, s'agissant des recherches, études et évaluations dans le domaine de la santé, qu'après avis du comité compétent.

La conformité de ces traitements à la méthodologie de référence MR-004 est de fait exclue, dans la mesure où les personnes concernées ne seront informées individuellement ni de la constitution de cet entrepôt, ni des traitements ultérieurs mis en œuvre à partir des données qu'il contient.

Sur les finalités poursuivies par le traitement et les traitements ultérieurs

La constitution de l'entrepôt de données a pour objet de permettre leur mise à disposition pour la réalisation de traitements ultérieurs. La Commission relève à ce titre que le projet mentionne que les données contenues dans cet entrepôt ne pourront être traitées que pour des projets poursuivant une finalité d'intérêt public en lien avec l'épidémie actuelle de COVID-19.

La Commission prend acte de ce que cette finalité, très générale, sera interprétée au regard des finalités de constitution de l'entrepôt indiquées à l'article 1er et des considérants du projet, qui précisent notamment que « *la capacité à mobiliser les données de santé est un axe essentiel de la lutte contre l'épidémie de covid-19 et qu'il est nécessaire de poursuivre et anticiper les évolutions de l'épidémie, prévenir, diagnostiquer et traiter au mieux la pathologie et adapter l'organisation de notre système de santé pour combattre l'épidémie et en atténuer les impacts* ».

Elle relève par ailleurs que le projet d'arrêté ne fait, sinon à travers la mention de sa base légale, référence ni à l'urgence qui s'attache la production des résultats des analyses réalisées dans le cadre de ces traitements, ni à la durée de leur mise en œuvre. S'agissant d'une solution temporaire et déployée spécifiquement afin de faire face à l'épidémie de -COVID19 dans le cadre de l'état d'urgence sanitaire, la Commission prend acte de l'engagement du ministère de préciser dans l'arrêté que les traitements

mis en œuvre à partir des données de l'entrepôt n'ont pas vocation à s'inscrire dans la durée et ne pourront, en dehors de la réalisation de nouvelles formalités, être mis en œuvre au-delà de l'état d'urgence sanitaire déclaré à l'article 4 de la loi du 23 mars 2020.

Sur les données dont le traitement est envisagé

Le projet dresse la liste des catégories de données susceptibles d'être transmises à la Plateforme des données de santé en vue de leur mise à disposition.

La Commission relève, au-delà du caractère très générique des catégories décrites, qu'il n'est fait mention ni de la profondeur historique des données, ni de leur nature exacte, notamment au regard de l'intérêt que peut présenter leur analyse dans le cadre de l'épidémie de COVID-19. A titre d'exemple, le projet mentionne, sans plus de détail, la remontée possible de données issues du SNDS ou de « données de pharmacie ».

Elle rappelle qu'en application du principe de minimisation des données prévu par l'article 5-1-c du RGPD, les données devront être adéquates, pertinentes et limitées à ce qui est nécessaire au vu de la finalité poursuivie, tant s'agissant des données figurant dans l'entrepôt au sein de la Plateforme des données de santé, que des données mises à disposition pour la réalisation de traitements ultérieurs.

A cet égard, la Commission prend acte de l'engagement du ministère de compléter le projet afin qu'il précise clairement que la Plateforme des données de santé et la CNAM ne peuvent, dans le cadre de l'arrêté examiné, collecter que les données nécessaires à la réalisation des traitements mis en œuvre dans le cadre des projets poursuivant une finalité d'intérêt public en lien avec l'épidémie actuelle de COVID-19.

Elle rappelle que l'arrêté ne doit pas permettre une remontée systématique et exhaustive de l'ensemble des données dont la liste figure dans le projet, indépendamment des besoins de ces projets.

La Commission rappelle par ailleurs, concernant chacun des traitements qui viendrait alimenter l'entrepôt ainsi constitué, qu'il devra préalablement avoir été créé et mis en œuvre conformément aux dispositions du RGPD et de la loi « informatique et libertés », notamment s'agissant des formalités prévues par cette dernière le cas échéant.

Enfin, elle relève que le projet prévoit que les solutions techniques de mise à disposition des données ne peuvent contenir ni les nom et prénoms des personnes, ni leur numéro d'inscription au répertoire d'identification des personnes physiques (NIR), ni leur adresse.

Sur la durée de conservation des données

Le projet ne mentionne pas de durée de conservation précise, s'agissant des données contenues dans l'entrepôt. Cependant, le projet s'inscrivant dans le cadre de l'état d'urgence sanitaire déclaré à l'article 4 de la loi du 23 mars 2020, la Commission en déduit que les données ne devront être conservées dans celui-ci que pour la durée de l'état d'urgence sanitaire.

S'agissant de ces données, le ministère a précisé que celles dont la conservation sera prévue par le décret mentionné à l'article L. 1461-7 du code de la santé publique, ainsi que par l'arrêté qui viendra préciser les bases de données figurant au « catalogue » de

la Plateforme des données, seront conservées en application des règles de droit commun, tandis que les autres catégories de données seront détruites.

La Commission en prend acte. Elle considère cependant que dans l'hypothèse où l'adoption du cadre juridique de droit commun applicable à la plateforme des données de santé n'aurait pas pu être finalisé à l'issue de l'état d'urgence sanitaire, l'ensemble des données collectées pendant cette période devra être détruit.

Sur les modalités d'information des personnes et d'exercice des droits

La Commission relève qu'en dehors de la constitution, au sein de la Plateforme des données de santé, d'un répertoire public recensant la liste et les caractéristiques de tous les projets portant sur les données de l'entrepôt, le projet ne prévoit aucune modalité d'information ou d'exercice des droits particulière quant à la constitution de l'entrepôt ou aux traitements mis en œuvre ultérieurement.

La Commission rappelle cependant que les personnes concernées devront être informées, s'agissant du traitement de données visant à la constitution de l'entrepôt, puis de chaque projet de recherche menée à partir des données qu'il contient, dans les conditions prévues par l'article 14 du RGPD. A ce titre, en application des dispositions de l'article 14-5-b) du RGPD, 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 révèlerait impossible, exigerait des efforts disproportionnés ou compromettrait gravement la réalisation des objectifs du traitement. En pareils cas, il appartient au responsable de traitement de prendre des mesures appropriées pour protéger les droits et libertés, ainsi que les intérêts légitimes des personnes concernées, y compris en rendant les informations publiquement disponibles.

Elle demande donc, en prenant en considération le contexte de crise sanitaire actuel ne permettant pas de procéder à une information individuelle de l'ensemble des personnes concernées, que des mesures appropriées soient prises et que l'information relative au traitement de données visant à la constitution de l'entrepôt et à chaque projet de recherche mené à partir des données qu'il contient soit rendue publique, notamment en faisait figurer dans le répertoire public mentionné dans le projet, l'ensemble des informations prévues à l'article 14 du RGPD.

Elle rappelle notamment que cette information devra détailler les modalités d'exercice des droits des personnes concernées et que les responsables de traitement devront prévoir les mesures nécessaires pour faire droit à ces demandes.

Sur les transferts de données vers des pays tiers et les divulgations non autorisées par le droit de l'Union

La Commission relève que les contrats qui lui ont été fournis ne prévoient eux-mêmes ni la localisation des données ni l'ensemble des garanties relatives aux modalités d'accès aux données par les administrateurs de l'hébergeur. Le contrat permet cependant à la Plateforme, à travers les « Conditions des services en ligne » de choisir le lieu d'hébergement des données. En outre, les informations fournies par la Plateforme des données de santé mentionnent explicitement le recours à un hébergeur certifié « hébergeur de données de santé ». A cet égard, la Commission prend acte de ce que le ministère s'est engagé à ce que la Plateforme des données de santé exige de son hébergeur que les données « au repos » soient hébergées au sein de l'Union européenne.

La Commission souligne toutefois que cette localisation ne s'applique qu'aux données « au repos », alors même que le contrat mentionne l'existence de transferts de données en dehors de l'Union européenne dans le cadre du fonctionnement courant de la plateforme, notamment pour les opérations de maintenance ou de résolution d'incident.

A cet égard, les dispositions contractuelles de sous-traitance conclues entre la Plateforme des données de santé et le prestataire chargé de l'hébergement des données, stipulent que les données traitées peuvent être transférées vers les États-Unis pour y être stockées et traitées, ainsi que dans tout autre pays dans lequel le sous-traitant ou ses sous-traitants ultérieurs sont implantés. Ces transferts font l'objet d'un encadrement conformément au Chapitre V du RGPD, étant régis en l'espèce par des clauses contractuelles types, conformément à l'article 46-2-c de ce règlement.

La Commission rappelle, dans ce contexte, les inquiétudes soulevées à plusieurs reprises par le Comité européen de la protection des données (CEPD) concernant l'accès par les autorités des Etats-Unis aux données transférées aux Etats-Unis, plus particulièrement la collecte et l'accès aux données personnelles à des fins de sécurité nationale en vertu de l'article 702 de la loi américaine FISA et du décret (« *Executive Order* ») 12 333. Ces problématiques sont actuellement soumises à la Cour de justice de l'Union européenne dans le cadre d'une demande de décision préjudicielle formée par la *High Court of Ireland* concernant la validité de la décision 2010/87/UE, par laquelle la Commission européenne a établi des clauses contractuelles types pour certaines catégories de transferts. Un arrêt de la Cour dans cette affaire (C-311/18) est attendu dans les mois qui viennent.

La Commission rappelle également que les traitements mis en œuvre par le sous-traitant sont soumis aux dispositions du RGPD, et notamment aux restrictions relatives aux transferts et divulgations non autorisées par le droit de l'Union. Toute demande d'accès d'une juridiction ou d'une autorité administrative d'un pays tiers, adressée au sous-traitant, en dehors d'un accord international applicable ou, selon l'interprétation du CEPD, de l'application d'une dérogation relative à l'intérêt vital de la personne concernée, ne pourrait donc être considérée comme licite.

Elle relève également que les dispositions contractuelles de sous-traitance prévoient une obligation de notification au responsable du traitement de toute demande de divulgation des données traitées adressée au sous-traitant en France, sauf interdiction légale, qui ne saurait être fondée qu'en droit de l'Union ou national.

Au vu de ce contexte et de la sensibilité des données dont le traitement est envisagé, pour lesquelles une protection plus élevée doit être assurée, ainsi que des éventuels risques matériels et juridiques en matière d'accès direct par les autorités de pays tiers, la Commission demande qu'une vigilance particulière soit accordée, dans la mise en œuvre de l'arrêté, aux conditions de conservation et aux modalités d'accès aux données, et recommande que la Plateforme des données de santé assure un hébergement et un traitement des données sur le territoire de l'Union européenne. A plus long terme, elle prend acte de ce qu'il lui a été indiqué que l'entrepôt appelé à être constitué au sein de la Plateforme des données de santé n'est pas lié aux services d'un unique prestataire et souhaiterait, eu égard à la sensibilité des données en cause, que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne.

Sur la sécurité

A titre liminaire, La Commission se doit de souligner que la mise en œuvre effective de la solution technique de conservation et de mise à disposition des données de la Plateforme des données de santé, ainsi que la constitution de son « catalogue » de données, ne devaient initialement intervenir que postérieurement à l'entrée en vigueur d'un cadre juridique précis accompagné de la mise en œuvre de l'ensemble d'un plan d'action. En effet, la Commission relève que la solution technique a fait l'objet d'une analyse globale des risques et des impacts sur la vie privée, suivie d'une homologation le 16 décembre 2019 selon le référentiel de sécurité du SNDS, avec un plan d'action conséquent de mise en œuvre de mesures de sécurité s'étalant sur une période de plusieurs mois. Elle relève en outre que l'homologation des espaces projets par les responsables de traitement des projets pourrait faire l'objet d'une procédure dérogatoire dans le cadre de la crise sanitaire.
La Commission s'interroge donc sur les conditions de démarrage anticipé de la solution technique dans un contexte où la Plateforme de données de santé a dû accomplir en quelques semaines des opérations, dont certaines structurantes, pour garantir la sécurité des données traitées étaient prévues pour s'étaler sur plusieurs mois.

La Commission souligne en conséquence que la Plateforme des données de santé devra s'assurer que cette mise en œuvre anticipée n'engendre pas de risque supplémentaire pour les personnes concernées.

Par ailleurs, la Commission rappelle l'importance de la mise en place d'une gouvernance centralisée de la sécurité informatique de la solution technique, qui doit être assurée avec un niveau d'indépendance suffisant vis-à-vis de la direction de la Plateforme des données de santé. Elle relève que cette exigence ne semble actuellement pas remplie, alors que le contexte de mise en place en urgence de la solution technique rend cette exigence d'autant plus d'actualité. Bien que la situation actuelle ne soit que transitoire, la Commission appelle la Plateforme des données de santé à mettre en place dans les plus brefs délais une gouvernance dédiée et indépendante chargée de la sécurité.

La Commission relève par ailleurs que la Plateforme des données de santé a réalisé une analyse d'impact relative à la protection des données consacrée à la solution technique dans sa version dédiée aux projets en lien avec le COVID-19, ainsi qu'une analyse actualisée de conformité au référentiel de sécurité du SNDS. Elle relève que cette analyse permet d'appréhender correctement l'ensemble des mesures mises en place par la Plateforme des données de santé dans sa démarche de conformité aux principes de la protection des données personnelles, et souligne que cette analyse a été réalisée en conformité avec les principes du RGPD.

Concernant la transmission des données des producteurs de données vers la Plateforme, la Commission prend acte que la procédure qui sera appliquée a fait l'objet d'échanges avec l'Agence nationale de sécurité des systèmes d'information. Les données seront chiffrées avec des clés de chiffrement renouvelées à chaque échange et transmises à travers un canal sécurisé mis en place à l'initiative des opérateurs projets, assurant notamment l'authentification de la source et du destinataire et le chiffrement du flux. Etant donné la diversité des sources possibles, des discussions au cas par cas sur les modalités de transferts sont également envisagées. La Commission rappelle que si les modalités opérationnelles de transfert peuvent en effet être adaptées à des cas particuliers, cela ne devra en aucun cas affaiblir le niveau de sécurité des données.

A cet égard, une convention de transfert des données devra être signée entre la Plateforme des données de santé et chaque fournisseur de données afin d'encadrer la transmission des informations, en précisant notamment la fréquence des mises à jour et les conditions de sécurité du transfert.

La Commission prend acte de ce que la Plateforme des données de santé recevra uniquement des données préalablement pseudonymisées par les producteurs de données, selon les modalités également précisées dans la convention de transfert des données.

Suite à des échanges avec le ministère, il a été indiqué à la Commission que dans le cas particulier d'un appariement déterministe au moyen du NIR des personnes concernées, *via* le circuit CNAM, un pseudonyme obtenu à partir d'une fonction cryptographique irréversible appliquée au NIR est également fourni à la Plateforme des données de santé. Pour autant, la Commission relève que ces modalités de pseudonymisation ne semblent pas détaillées dans l'analyse d'impact relative à la protection des données et que les conséquences en termes de risques de ré identification pour les personnes ne semblent pas clairement établies à ce stade. Elle relève également que le projet d'arrêté ne prévoit pas la transmission du NIR à la Plateforme des données de santé. Compte tenu du contexte de la saisine et des informations transmises, la Commission n'est pas en capacité d'appréhender pleinement les conséquences du recours à un tel pseudonyme et ne saurait se prononcer sur ce point.

Après réception des données, les pseudonymes utilisés pour la transmission seront remplacés par des pseudonymes aléatoires dans l'espace opérateur de la solution technique. La Commission relève qu'une table de correspondance entre les pseudonymes initiaux et ceux générés par la Plateforme sera conservée. La Commission prend acte que cette table de correspondance sera conservée dans une sous-partie isolée de l'espace opérateur, qu'elle sera chiffrée avec une clé dédiée et dont l'utilisation nécessitera l'action conjointe de deux employés de la Plateforme des données de santé ayant des rôles distincts. Afin d'améliorer encore le niveau de sécurité et dans la mesure où l'accès à ces clés ne semble pas nécessaire dans le cadre du fonctionnement courant des projets, la Commission recommande que ces clés soient stockées dans une base distincte gérée par la Plateforme de données de santé elle-même ou bien par un autre sous-traitant.

Lors de la mise à disposition des données au sein des espaces projets, de nouveaux pseudonymes seront générés, assurant ainsi l'utilisation d'identifiants différents au sein de chaque projet pour un même individu. La Commission s'interroge toutefois sur les modalités pratiques de pseudonymisation mise en œuvre par la Plateforme des données de santé pour cette mise à disposition, notamment en cas de mise à jour des données au sein de ces espaces projets. Elle attire donc l'attention du ministère sur la nécessité de prévoir des modalités de pseudonymisation des données précisant, le cas échéant, le choix de l'opération cryptographique irréversible utilisée ainsi que la procédure de gestion des secrets associés ou encore la sécurité renforcée appliquée en conséquence à la table de correspondance.

La Commission prend acte de ce que l'ensemble des échanges de données ayant lieu lors de l'utilisation des espaces projets de la solution technique seront réalisés *via* des canaux de communication chiffrés et assurant l'authentification de la source et du destinataire.

La Commission prend également acte de ce que les données stockées seront chiffrées avec des algorithmes à l'état de l'art à partir de clés générées par les responsables de la Plateforme sur un boîtier chiffrant maitrisé par la Plateforme des données de santé.

La Commission relève toutefois qu'afin de bénéficier de toutes les capacités de la solution technique de l'hébergeur ces clés devront lui être confiées. Elles seront conservées par l'hébergeur au sein d'un boîtier chiffrant, ce qui a pour conséquence de permettre techniquement à ce dernier d'accéder aux données.

La Commission relève que des mesures techniques sont mises en place afin de maitriser les accès des administrateurs des sous-traitants en charge de la solution technique. Une fonctionnalité d'autorisation préalable des accès administrateurs est activée selon l'analyse d'impact relative à la protection des données réalisée. Néanmoins, la Commission relève que cette fonctionnalité ne semble pas mentionnée dans les contrats fournis. En outre, la Commission s'interroge sur l'effectivité de cette mesure qui ne semble pas couvrir la totalité des accès possibles.

La Commission relève que le projet prévoit que les données ne peuvent être traitées que dans les solutions techniques de la Plateforme des données de santé et de la CNAM, et ne peuvent pas en être extraites. Les fonctionnalités d'exportation automatique ne seront pas utilisables par les entités accédant aux données dans les espaces projets. La Commission s'interroge toutefois sur l'effectivité du blocage de toute possibilité d'exportation. Les pièces du dossier indiquent que les procédures d'audits systématiques des exportations par les opérateurs de données sont maintenues, ainsi que l'obligation, pour les utilisateurs de s'engager à ne pas exporter de données à caractère personnel et à mettre en place des mécanismes de traçabilité des opérations d'exportation.
En conséquence la Commission appelle le ministère à indiquer explicitement que toutes les fonctionnalités d'exportation des données seront totalement désactivées et inaccessibles aux utilisateurs, soit en indiquant que les données à caractère personnel hébergées sur la plateforme ne pourront faire l'objet d'aucune exportation, que seules des données ayant fait l'objet d'une procédure d'anonymisation dans les règles de l'art pourront être exportées et que ces exports seront préalablement et systématiquement audités afin de s'assurer du caractère anonyme des données exportées. La Commission rappelle en effet que seules des données anonymes peuvent être exportées hors d'un environnement homologué conformément à l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au SNDS.

Le ministère s'est engagé à ce que la Plateforme des données de santé tienne à sa disposition un registre incluant notamment l'ensemble des projets mis en œuvre et détaillant tous les accès ouverts pour et par les responsables de traitement des projets. La Commission en prend acte.

La Commission prend également acte qu'une procédure de gestion des identités et des habilitations est définie par le responsable de la sécurité des systèmes d'information (RSSI) de la Plateforme des données de santé et mise en œuvre sous la responsabilité du directeur technique.

Sur le circuit de remontée hebdomadaire des données du PMSI

L'article1-II du projet prévoit que, sans préjudice du circuit prévu par l'arrêté du 23 décembre 2016 modifié, les établissements de santé mentionnés à l'article 1er du même arrêté transmettent, selon une périodicité hebdomadaire, les fichiers anonymes mentionnés au I de l'article 5 du même arrêté directement à l'Agence technique de

l'information sur l'hospitalisation (ATIH). Ces données seront ensuite transmises sans délai à la CNAM afin d'alimenter le SNDS.

La Commission relève cependant que le projet ne précise pas, à l'inverse du courrier de saisine l'accompagnant, que cette remontée d'informations « *n'a pas vocation, dans le contexte de forte mobilisation des établissements, à faire réaliser par ceux-ci des remontées exhaustives d'activité de façon hebdomadaire mais d'ouvrir une remontée hebdomadaire permettant d'intégrer en priorité l'activité liée à l'épidémie* ». Elle demande donc que cette précision soit ajoutée dans le projet.

La Commission prend toutefois acte de l'engagement du ministère de mentionner dans le projet que les données remontées dans ce cadre ne pourront pas être utilisées pour les finalités pour lesquelles elles sont habituellement collectées, détaillées à l'article L. 6113-8 du code de la santé publique, sauf s'agissant de la veille et la vigilance sanitaires.

La Commission rappelle que les données auxquelles il est fait référence, qui sont des données pseudonymisées, ne sauraient être considérées comme anonymes au sens du RGPD, tel qu'éclairé par l'avis du G29 n° 05/2014 du 10 avril 2014 relatif aux techniques d'anonymisation.

Elle prend acte de l'engagement du ministère de modifier le projet sur ce point, afin qu'il ne soit plus fait référence à des données « anonymes ». Tout traitement de ces données devra donc intervenir dans le respect des dispositions du RGPD et de la loi « informatique et libertés », s'agissant de données à caractère personnel.

Les autres dispositions du projet n'appellent pas d'observation de la Commission.

La Présidente

Marie-Laure DENIS