Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/20/100

DÉLIBÉRATION N° 20/056 DU 3 MARS 2020 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL ISSUES DE LA BASE DE DONNÉES COBRHA PAR LA PLATE-FORME EHEALTH À DES INSTANCES NON COMMERCIALES EN VUE D'OFFRIR AUX PATIENTS ET AUX PRESTATAIRES DE SOINS DES OUTILS DE RECHERCHE D'AUTRES PRESTATAIRES DE SOINS À PROXIMITÉ AFIN D'AMÉLIORER LA PRISE EN CHARGE DES PATIENTS

Le Comité de sécurité de l'information, chambre sécurité sociale et santé (dénommé ci-après « le Comité »),

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 relatif à la protection des données ou GDPR) ;

Vu la loi du 3 décembre 2017 *relative à la création de l'Autorité de protection des données*, en particulier l'article 114, modifié par la loi du 25 mai 2018 ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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*, notamment l'article 97;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la Plate-forme eHealth*, en particulier l'article 11;

Vu le rapport d'auditorat de la Plate-forme eHealth ;

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la décision suivante, le 3 mars 2020 :

I. OBJET DE LA DEMANDE

1. CoBRHA (*Common Base Register For Healthcare Actor*) est une base de données contenant des données d'identification de base des prestataires de soins et des institutions de soins agréés. Cette base de données est une source authentique consolidée qui permet de répondre à 3 questions concernant un acteur de soins de santé :

1) Qui est-il ? Cet acteur peut être un professionnel de soins de santé (ex : médecins, infirmière, ...) ou une institution de soins de santé (ex : hôpital, maison de repos, ...)
2) Qu'est-il autorisé à faire ? Pour une institution de soins de santé, cela correspond aux activités reconnues de cette institution (ex: hôpital général, soins intensifs, SMUR/MUG, ...). Pour un professionnel, cela correspond aux professions et spécialités reconnues de cette individu (diplôme, visa, ...).
3) Quelles sont ces responsabilités ? Ceci correspond aux rôles joués par les acteurs de soins de santé, éventuellement vis à vis d'un autre acteur de soin de santé (ex : médecin en chef d'un hôpital)

2. La base de données est gérée par la Plate-forme eHealth et alimentée par les institutions publiques suivantes : le Service public fédéral Santé publique, l'INAMI, l'Agence fédérale des médicaments et des produits de santé (AFMPS), le Collège intermutualiste national, les Régions, les Communautés, le Registre national, la Banque Carrefour de la Sécurité Sociale et la Banque Carrefour des entreprises.

3. Chaque source authentique doit veiller à alimenter et à mettre jour CoBRHA selon les procédures définies avec la plate-forme eHealth. La disponibilité, la qualité et l'actualisation des données transmises à la plate-forme eHealth sont définies en concertation avec chaque source authentique.

4. CoBRHA contient des données communiquées issues de bases de données gérées par les institutions elles-mêmes, à savoir :

- le fichier des prestataires de soins pour remboursement par l'assurance maladie (INAMI) ;
- le cadastre des professions de santé tel que défini par la loi du 29 janvier 2003 portant création de la banque de données fédérale des professionnels de soins de santé (SPF Santé publique) ;
- des données relatives à l'agrément de différentes institutions publiques (hôpitaux, maisons de repos, soins à domicile, …) communiquées par les Régions ;
- des données relatives à l'enregistrement des officines ouvertes au public et de leur pharmacien titulaire (AFMPS) ;
- des données communiquées par le CIN ;
- le numéro BCE-KBO (Banque Carrefour des Entreprises).

5. Certaines données contenues dans la base de données CoBRHA sont publiques et publiées directement sur le site web des sources authentiques. C'est, notamment, le cas des données communiquées par l'INAMI. Selon l'article 218, §2 de la loi coordonnée du 14 juillet 1994

relative à l'assurance obligatoire soins de santé et indemnités[1], l'INAMI met à disposition du public, sur son site internet, la liste des dispensateurs de soins disposant d'un numéro attribué par cet Institut. Cette liste comprend les noms, prénoms, numéro INAMI, adresse(s) de travail et situation d'adhésion aux accords et conventions. Il en va de même pour la liste des officines ouvertes au public[2] et de leur pharmacien titulaire publiée sur le site web de l'AFMPS.

6. Par contre, l'accès aux données contenues dans le cadastre des professions de santé est régi par l'article 100 de la loi coordonnée du 10 mai 2015[3]. Selon cet article, le droit d'accès aux données enregistrées dans la banque de données fédérale permanente des professionnels des soins de santé est limité comme suit :

1° tout professionnel des soins de santé, enregistré dans la banque de données, a accès aux données qui le concernent; conformément à l'article 12 de la loi du 8 décembre 1992 sur la vie privée, il a en outre le droit d'obtenir sans frais la rectification de ces données;

2° pour autant qu'ils n'aient pas un autre accès direct à ces données et pour autant qu'ils soient habilités, par une loi ou en vertu de celle-ci, à connaître les informations concernées, les établissements publics de sécurité sociale et les autorités publiques ont accès à toutes les données d'identification;

3° les Ordres compétents, les mutualités visées dans la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et les compagnies d'assurances ont accès aux données d'identification, sans toutefois avoir accès au numéro d'identification du registre national des personnes physiques.

Les mutualités et les compagnies d'assurances ont en outre accès aux données relatives à l'agrément des pratiques;

4° le public a accès aux nom et prénoms, au(x) titre(s) professionnel(s) et qualifications professionnelles particulières et aux informations sur le droit d'un praticien déterminé de prester des services ou sur toute restriction éventuelle à sa pratique et, sauf opposition du praticien, à son adresse professionnelle principale; un praticien qui n'exerce plus de manière substantielle la profession pour laquelle il a été enregistré peut demander que son enregistrement ne soit plus accessible au public;

5° les professionnels de soins de santé visés à l'article 97, § 1er, ont accès aux nom et prénoms, au(x) titre(s) professionnel(s) et qualifications professionnelles particulières et à l'adresse professionnelle principale ainsi qu'aux données volontairement mises à disposition visées à l'article 98, 4°;

6° la Direction générale des Professions de la santé, de la Vigilance sanitaire et du Bien-être au travail du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement et l'Institut national d'Assurance Maladie et Invalidité ont accès aux données relatives à l'agrément;

7° la plate-forme eHealth, instituée par la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, a accès à toutes les données d'identification, aux

---

[1] Loi du 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994, *M.B.* du 27 août 1994, p. 21524.

[2] Article 20 de l'arrêté royal du 25 septembre 1974 concernant l'ouverture, le transfert et la fusion d'officines pharmaceutiques ouvertes au public, *M.B.* du 5 octobre 1974, p. 12267.

[3] Article 100, 7° de la loi du 10 mai 2015 loi coordonnée relative à l'exercice des professions de santé, *M.B.* du 18 juin 2015, p. 35172.

données relatives à l'agrément, ainsi qu'à celles relatives à l'autorisation d'exercice mais pas, en cas de retrait de l'autorisation d'exercice, aux données relatives aux raisons ayant causé le retrait;
8° Les autorités d'autres États membres ont accès aux données enregistrées dans la banque de données fédérale permanente des professionnels des soins de santé, dans le contexte de soins de santé transfrontaliers, conformément aux chapitres II et III et aux mesures nationales d'exécution des dispositions de l'Union relatives à la protection des données à caractère personnel, en particulier des Directives 95/46/CE et 2002/58/CE, et dans le respect du principe de la présomption d'innocence. Les échanges d'informations se font dans le cadre du Système d'information du marché intérieur créé en application de la Décision 2008/49/CE de la Commission du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du Système d'information du marché intérieur (IMI).

7. En vue de l'exécution des missions réglementaires qui leur sont confiées, les services publics fédéraux et régionaux doivent pouvoir consulter la base de données CoBRHA et accéder aux données autorisées en fonction de leurs missions réglementaires respectives.

8. Les instances non marchandes qui soutiennent des demandeurs de soins dans leur recherche de soins ou des prestataires de soins dans leur prestation de soins peuvent se voir communiquer la qualification professionnelle et les données de contact professionnelles des prestataires de soins compétents qui sont disponibles dans CoBRHA afin de permettre à ces instances de proposer au demandeur de soins ou au prestataire de soins un ou plusieurs prestataires de soins qualifiés exerçant à proximité.

II. COMPÉTENCE

9. L'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la Plate-forme eHealth* dispose que toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

10. Le Comité s'estime dès lors compétent pour se prononcer sur la demande d'autorisation, et ce, même si les données concernées ne sont pas des données à caractère personnel relatives à la santé.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

11. Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à l'article 6, §1er du RGDP est remplie. C'est, notamment, le cas lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis[4] ou lorsque le traitement est nécessaire à

[4] Art. 6, §1, c) du RGPD.

l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[5].

12. Selon l'article 5, 5° de la loi eHealth[6], la plate-forme eHealth est chargée, en vue de l'exécution de son objectif, de s'accorder sur une répartition des tâches en ce qui concerne la collecte, la validation, l'enregistrement et la mise à disposition de données échangées au moyen de la plate-forme de collaboration et sur les normes de qualité auxquelles ces données doivent répondre, et contrôler le respect de ces normes de qualité.

B. PRINCIPE DE FINALITÉ

13. L'article 5 du RGPD n'autorise le traitement de données à caractère personnel que pour des finalités déterminées, explicites et légitimes.

14. Les services publics fédéraux et régionaux, les établissements publics de sécurité sociale, les administrations publiques et les organismes d'intérêt public désignés doivent pouvoir accéder aux données contenues dans la base de données CoBRHA en vue de permettre l'exécution de leurs missions réglementaires respectives. Cette consultation ne peut se faire que pour les données autorisées en fonction de leurs missions réglementaires respectives.

15. Les instances non marchandes qui soutiennent des demandeurs de soins dans leur recherche de soins ou des prestataires de soins dans leur prestation de soins peuvent se voir communiquer la qualification professionnelle et les données de contact professionnelles des prestataires de soins compétents qui sont disponibles dans CoBRHA afin de permettre à ces instances de proposer au demandeur de soins ou au prestataire de soins un ou plusieurs prestataires de soins qualifiés exerçant à proximité.

16. A cet égard, le Comité constate que l'article 101 de la loi du 10 mai 2015 stipule que la commercialisation du contenu des données contenues dans le cadastre des professions de santé, par la vente, la location, la distribution ou toute autre forme de mise à disposition à des tiers est interdite. Plus généralement, toute utilisation autre que purement interne comme support de l'activité de l'utilisateur légitime est expressément interdite. Par conséquent, la communication de ces mêmes données via CoBRHA dans un but lucratif est également interdite.

17. Au vu des objectifs du traitement tels que décrits ci-dessus, le Comité sectoriel considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

B. PRINCIPE DE PROPORTIONALITÉ

[5] Art. 6, §1, e) du RGPD.
[6] Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, *M.B.* du 13 octobre 2008, p. 54454.

18. L'article 5 du RGDP dispose que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

19. Les données consultées par les services publics fédéraux et régionaux, les établissements publics de sécurité sociales, les administrations publiques et les organismes d'intérêt publics désignés sont les données strictement autorisées pour l'exécution de leurs missions réglementaires respectives.

20. Les instances non marchandes qui soutiennent des demandeurs de soins dans leur recherche de soins ou des prestataires de soins dans leur prestation de soins peuvent se voir communiquer la qualification professionnelle et les données de contact professionnelles des prestataires de soins compétents qui sont disponibles dans CoBRHA afin de permettre à ces instances de proposer au demandeur de soins ou au prestataire de soins un ou plusieurs prestataires de soins qualifiés exerçant à proximité. Ces données sont utilisées par l'instance non marchande en question uniquement pour la finalité précitée et ne sont pas conservées au-delà du délai nécessaire à la réalisation de cette finalité. Il s'agit plus précisément de la qualification professionnelle et des données de contact professionnelles suivantes : les nom et prénom(s), l'adresse professionnelle, le numéro de téléphone professionnel et le numéro INAMI.

21. L'instance non marchande qui offre le soutien en question veille à ce que les informations concernant tous les prestataires de soins compétents qui satisfont à des critères de sélection objectifs soient communiquées et évite donc une anti-sélection.

22. En ce qui concerne le délai de conservation des données, le Comité rappelle que les données ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation). Le Comité est d'avis qu'une fois que le dossier est clôturé au regard de cette finalité, les données relatives au(x) prestataire(s) de soins sélectionné(s) communiquées au patient doivent être effacées.

23. Compte tenu des finalités de la base de données CoBRHA, le Comité estime que la communication envisagée est adéquate, pertinente et non excessive.

C. PRINCIPE DE TRANSPARENCE

24. Conformément à l'article 14 du RGPD, lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit fournir plusieurs informations à la personne concernée. Cette disposition ne s'applique pas, notamment, lorsque l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée.

25. Vu que la mise à disposition des données concernées est prévue par l'article 100 de la loi du 10 mai 2015 précité ainsi que le caractère publique des autres données contenues dans CoBRHA, le Comité constate que le responsable du traitement est dispensé.

D. MESURES DE SÉCURITÉ

26. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). Ces mesures devront assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraînent l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

27. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un délégué à la protection des données; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, information et formations régulières du personnel sur le thème de la protection de la vie privée et sur les règles de sécurité); sécurité physique et de l'environnement; sécurisation des réseaux; sécurisation logique des accès et des réseaux; journalisation, traçage et analyse des accès; surveillance, revue et maintenance; système de gestion des incidents de sécurité et de la continuité (systèmes de tolérance de panne, de sauvegarde, …); respect et documentation[7].

[7] « Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel », document rédigé par la Commission de la protection de la vie privée disponible à l'adresse:http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que:

la communication des données à caractère personnel telle que décrite dans la présente délibération est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE