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

CSI/CSSS/20/236

DÉLIBÉRATION N° 20/140 DU 6 MAI 2020 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LE COLLÈGE INTERMUTUALISTE NATIONAL (CIN) À LA PLATE-FORME TECHNIQUE DE LABORATOIRES MIPS, DANS LE CADRE DE LA LUTE CONTRE LE COVID-19

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 et portant diverses dispositions* ;

Vu la délibération n°17/041 du 21 février 2017, modifiée le 18 juillet 2017, le 19 septembre 2017 et le 5 juin 2018, relative à la communication de données à caractère personnel par la plate-forme eHealth et cette dernière, dans le cadre de la création d'un annuaire de routage pour un échange électronique sécurisé de données ;

Vu la délibération n°12/033 du 17 avril 2012 relative à la mise à disposition d'une boite aux lettres électronique sécurisée comme service de base de la plate-forme eHealth (eHealthBox) ;

Vu la décision n°17/2020 du Service Public Fédéral Intérieur d'extension temporaire de la délibération du Comité sectoriel RN n°35/2010 du 6 octobre 2010 ;

Vu la délibération n°10/078 du 9 novembre 2010, modifiée le 27 mars 2020 et le 7 avril 2020, relative à l'accès aux registres Banque Carrefour dans le chef des laboratoires agrées de biologie clinique, en vue de la vérification et de l'actualisation des données d'identification de leurs patients, de leur identification univoque dans les dossiers des laboratoires ainsi que de la gestion de la facturation ;

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

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la délibération suivante, le 6 mai 2020 :

I. OBJET DE LA DEMANDE

1. Dans le cadre de la crise sanitaire et de la lutte contre la propagation du COVID-19 et vu la multiplication du nombre de tests de dépistage à effectuer, il a été décidé d'étendre la possibilité de procéder à des tests de dépistage relatifs au COVID-19 par des laboratoires de biologie clinique non agréés désignés par la Ministre fédérale en charge de la Santé publique.

2. Tous les résultats de ces tests sont disponibles sur un serveur central de la société MIPS, en tant que sous-traitant technique des laboratoires. Ce serveur de résultats est accessible à chaque prestataire de soins de santé qui a une relation de soins avec le patient concerné via le système hub&metahub.

3. Dans un certain nombre de cas, l'échantillon et la demande de test ne sont pas réalisés par le médecin détenteur du dossier médical global du patient (DMG), mais par un médecin coordinateur d'un centre d'accueil et de soins ou par un poste de triage. C'est pourquoi, les médecins détenteurs du DMG souhaitent également recevoir, via leur eHealthBox, le résultat du test quand bien même ce test n'aurait pas été prescrit par eux, ceci afin qu'ils puissent suivre leur patient.

4. A cet effet, il faudrait rapidement mettre en place un système permettant, pour les résultats disponibles sur le serveur de résultats de MIPS, qui sont liés au NISS du patient, d'envoyer un message vers l'eHealthBox du titulaire du DMG du patient tel que connu auprès du Collège intermutualiste national (CIN).

5. Pour cette raison, il a été décidé de faire appel au webservice DAAS mis en place dans le cadre de l'annuaire de routage[1].

6. Compte tenu du caractère très urgent de cette communication, il est proposé d'accorder une utilisation temporaire du service DAAS à MIPS pour pouvoir envoyer le résultat du test au détenteur du DMG du patient. L'accès à l'information relative à l'identité du détenteur du

[1] Voyez la délibération n°17/041 du 21 février 2017, modifiée le 18 juillet 2017, le 19 septembre 2017 et le 5 juin 2018, relative à la communication de données à caractère personnel par la plate-forme eHealth et cette dernière, dans le cadre de la création d'un annuaire de routage pour un échange électronique sécurisé de données

DMG détenue par le CIN prendra fin dès la publication au Moniteur belge de l'arrêté royal déclarant la fin de l'épidémie de COVID-19 en Belgique.

II. COMPÉTENCE

7. Conformément à l'article 42, §2, 3° de la loi du 13 décembre 2006, toute communication de données à caractère personnel relatives à la santé doit faire l'objet d'une délibération de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information, sauf dans les cas d'exception prévus dans la loi.

8. En vertu de l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, 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, sauf dans les cas prévus par la loi.

9. Le Comité s'estime dès lors compétent pour se prononcer sur cette communication de données à caractère personnel.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

10. Selon l'article 9, §1er du RGPD, le traitement de données à caractère personnel relatives à la santé est interdit. Cette interdiction ne s'applique pas lorsque l'une des conditions mentionnées à l'article 9, §2 est remplie. C'est notamment le cas, lorsque le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail ou de diagnostics médicaux[2].

11. Dans le cadre de la lutte contre le COVID-19, il est nécessaire que le médecin détenteur du dossier médical global (DMG) d'un patient concerné par un test effectué dans un centre de triage ou un centre de soins soit informé des résultats de ce test afin de suivre ce patient et de mettre à jour les informations médicales contenues dans le dossier médical de ce patient.

12. Le Comité de sécurité est par conséquent d'avis qu'il existe un fondement acceptable au traitement de données à caractère personnel envisagé.

B. PRINCIPES RELATIFS AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

13. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence). Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées

[2] Article 9, §2, h) du RGPD.

(minimisation des données). Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude).

14. Selon l'article 5 du RGPD, les données à caractère personnel doivent être ccollectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

15. L'information relative à l'identité du médecin détenteur du DMG est détenue par le Collège Intermutualiste National qui est la source authentique de cette donnée.

16. Selon l'article 5 du RGPD, les données à caractère personnel doivent 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).

17. L'information relative à détenteur du DMG du patient ne sera pas conservée par MIPS, cette information sera uniquement consultée en vue d'envoyer les résultats du test de dépistage du COVID-19 effectué par un laboratoire non agréé d'une firme pharmaceutique au médecin détenteur du DMG via l'eHealthBox.

18. Le Comité prend acte que l'accès à l'information relative à l'identité du détenteur du DMG détenue par le CIN prendra fin dès la publication au Moniteur belge de l'arrêté royal déclarant la fin de l'épidémie de COVID-19 en Belgique.

19. Compte tenu de la finalité de la communication de données, le Comité estime que la communication envisagée est adéquate, pertinente et non excessive.

C. PRINICIPE DE TRANSPARENCE

20. Conformément à l'article 14 du RGPD, le responsable du traitement fournit à la personne concernée les informations nécessaires lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Cependant, cette disposition ne s'applique pas notamment lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

21. Le Comité est d'avis que les mesures de transparence envisagées sont suffisantes.

D. MESURES DE SÉCURITÉ

22. 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.

23. 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, …); documentation.

24. Le Comité de sécurité de l'information tient à rappeler les dispositions de l'article 9 de la loi du 30 juillet 2018 r*elative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, selon lesquelles le responsable du traitement (et ses sous-traitants) prend les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Par ces motifs,

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

autorise temporairement, la communication des données à caractère personnel telle que décrite dans la présente délibération, 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