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

CSI/CSSS/22/508

**DÉLIBÉRATION N° 22/282 DU 8 NOVEMBRE 2022 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LE SPF SANTÉ PUBLIQUE À LA PLATE-FORME EHEALTH DANS LE CADRE DE LA CRÉATION D'UNE BANQUE DE DONNÉES DE CONTACT DPO AU SEIN DE LA PLATE-FORME EHEALTH.**

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

Vu le Règlement (UE) n° 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 RGPD);

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*, en particulier 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*, en particulier l'article 5 , 1°, 2°, 9° ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 28 octobre 2022;

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la décision suivante, le 8 novembre 2022 :

## A. OBJET DE LA DEMANDE

**1.** En vertu de l'article 4 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, la plate-forme eHealth vise à optimaliser la qualité et la continuité des soins de santé et la sécurité du patient, à simplifier les formalités administratives pour tous les acteurs des soins de santé et à soutenir la politique en matière de soins de santé et ce à travers une prestation de services et un échange d'information électroniques entre tous les acteurs des soins de santé organisés avec les garanties nécessaires sur le plan de la sécurité de l'information et de la protection de la vie privée.

**2.** Un aspect principal lors de l'échange de données est la disponibilité des services des différents acteurs. En effet, une indisponibilité des informations relatives à un patient peut donner lieu à une perturbation de la prestation de services à ce patient.

**3.** La disponibilité des données échangées est susceptible de faire l'objet de plusieurs menaces. Un incident technique sur l'infrastructure pourra ainsi donner lieu à une interruption des échanges.

**4.** Depuis le début de la crise Covid, il s'avère que non seulement les incidents techniques, mais aussi les cybermenaces peuvent avoir un impact sérieux sur la disponibilité des systèmes. Lorsque ce type de menace se concrétise, cette dernière peut impacter les systèmes concernés, mais éventuellement aussi s'étendre rapidement à d'autres parties.

**5.** Tant pour les incidents techniques que pour les cybermenaces, il est d'une importance capitale que les différentes parties puissent être contactées rapidement, de sorte que celles-ci puissent prendre des mesures afin de parer, de manière adéquate, à un danger éventuel ou prendre des mesures appropriées afin de limiter l'impact d'un incident sur la prestation de services.

**6.** Au cours des 2 dernières années, le service de sécurité de la Plate-forme eHealth a, en collaboration avec le CCB, régulièrement envoyé un avertissement aux hôpitaux concernant les cybermenaces qui sont susceptibles de compromettre le fonctionnement des systèmes hospitaliers. Les informations relatives aux menaces ont été envoyées aux DPO des hôpitaux qui les ont fait traiter par les services informatiques ou le service de sécurité de l'information des hôpitaux.

**7.** Les informations relatives aux menaces se sont avérées utiles pour les hôpitaux et les listes de contact ont été élargies, à la demande des DPO et des services informatiques, au personnel des services informatiques, pour faire en sorte que les messages arrivent plus rapidement chez les personnes concernées et pour éviter que l'indisponibilité du DPO ne donne pas lieu à un retard inutile.

**8.** Afin d'encore mieux informer les hôpitaux, la Plate-forme eHealth demande un accès aux données de contact du personnel dirigeant des hôpitaux. Ces données de contact seront uniquement utilisées pour informer les hôpitaux sur les cybermenaces ou les incidents en cours qui constituent une menace potentielle pour les services de l'hôpital et qui requièrent une attention immédiate. Les données concernées sont les suivantes:

- Le nom de l'hôpital
- Le nom du dirigeant
- Le rôle du dirigeant
- Le numéro de téléphone
- Le numéro de GSM
- L'adresse électronique

## II. COMPÉTENCE

**9.** Selon l'article 4, 1) du RGPD, on entend par données à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

**10.** 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.

**11.** 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

**12.** 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 du RGPD est remplie. C'est notamment le cas, lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[1].

**13.** En vertu de l'arrêté royal du 12 février 2008 déterminant les règles suivant lesquelles le gestionnaire des hôpitaux doit communiquer au Ministre qui a la Santé publique dans ses attributions, l'identité des personnes chargées de la communication des données se rapportant à l'établissement, modifié par l'arrêté royal du 9 décembre 2021, suivant lequel le gestionnaire de l'hôpital est obligé de communiquer l'identité (nom, prénom et numéro de registre national) et les données de contact (numéro de téléphone fixe et/ou mobile (GSM) et l'adresse électronique) des personnes responsables de la communication des données se rapportant à l'hôpital.

[1] Art. 6, §1er, e) du RGPD.

- le directeur général.
- le médecin-chef,
- le chef du département infirmier de l'hôpital,
- la ou les personne(s) responsable(s) de la communication de la situation financière et des résultats d'exploitation de l'hôpital;
- la ou les personne(s) responsable(s) de la communication des données statistiques concernant l'hôpital;
- le délégué à la protection des données visé à l'article 37 du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

**14.** En vertu de l'article 5, 1°, 2° et 9° de la loi eHealth[2], la plate-forme eHealth est chargée en vue de l'exécution de son objectif, de développer une vision et une stratégie pour une prestation de services et un échange d'informations électroniques dans les soins de santé efficaces, effectifs et dûment sécurisés, tout en respectant la protection de la vie privée et en concertation étroite avec les divers acteurs publics et privés des soins de santé, de déterminer des normes, des standards et des spécifications TIC fonctionnels et techniques ainsi qu'une architecture de base utiles pour la mise en œuvre des TIC à l'appui de cette vision et de cette stratégie et de promouvoir le respect de la vision, de la stratégie, des normes, standards et spécifications fonctionnels et techniques, de l'architecture de base, ainsi que l'utilisation de la plate-forme électronique de collaboration pour l'échange de données électronique sécurisé et des services de base et la réalisation des projets par un maximum d'acteurs des soins de santé. En exécution de cela, des normes de sécurité minimales ont été définies qui prévoient notamment des systèmes d'avertissement et de communication d'informations en matière de protection des données et de sécurité de l'information. Des données de contact s'avèrent nécessaires à cet effet.

**15.** 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 DES DONNÉES À CARACTÈRE PERSONNEL

**16.** 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).

**17.** En vertu de l'article 5, 5° de la loi eHealth précitée, la plate-forme eHealth peut créer une base de données regroupant des données à caractère personnel en vue d'apporter un soutien à une initiative dans le domaine de la santé.

[2] 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.** Selon l'article 5 du RGPD, 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 (minimisation des données).

**19.** La base de données hébergée par la plate-forme eHealth contient les données d'identification et de contact qui sont strictement nécessaires pour identifier et contacter les responsables d'un hôpital.

**20.** Le Comité fait observer que la plate-forme eHealth ne conservera aucune donnée à caractère personnel relative à la santé concernant les personnes de contact.

**21.** En vertu de l'article 5 du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

**22.** Cette banque de données doit permettre à eHealth de contacter la direction d'un hôpital lorsqu'un incident technique ou une cybermenace risque de compromettre le fonctionnement de l'hôpital.

**23.** En vertu de l'article 5 du RGPD, 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). À cet effet, le SPF Santé publique enverra régulièrement des mises à jour des listes de contact à la plate-forme eHealth.

**24.** Compte tenu de la finalité du traitement, le Comité estime que la communication envisagée est adéquate, pertinente et non excessive.

## C. PRINCIPE DE TRANSPARENCE

**25.** 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 certaines 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.

**26.** En vertu des obligations découlant du RGPD, la plate-forme eHealth publiera ces traitements sur son site web où sont aussi publiés les autres traitements.

**27.** Le Comité est d'avis que les mesures de transparence actuelles sont suffisantes.

## D. MESURES DE SÉCURITÉ

**28.** En vertu de 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.

**29.** 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 conseiller en sécurité de l'information; 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.

**30.** Le Comité constate que la plate-forme eHealth dispose d'un délégué à la protection des données et satisfait à ces exigences de sécurité de l'information.

Par ces motifs,

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

accorde, en vertu l'article 5, 1°, 2°, 9° de la loi du 21 août 2008 *relative à la création et à l'organisation de la plate-forme eHealth*, une autorisation pour la création d'une base de données à caractère personnel relatives au personnel dirigeant des hôpitaux au sein de la plate-forme eHealth,

autorise, 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
Président