Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/19/300

DÉLIBÉRATION N° 19/166 DU 1ER OCTOBRE 2019 RELATIVE AU RÈGLEMENT FIXANT LES CRITÈRES EN VUE DE L'APPLICATION D'UN CERCLE DE CONFIANCE PAR UNE ORGANISATION DANS LE CADRE DE L'ÉCHANGE DES DONNÉES DE SANTÉ

Le Comité de sécurité de l'information,

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

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 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018 ;

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

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la décision suivante, le 1er octobre 2019 :

I. OBJET

1. Dans le cadre du règlement relatif aux relations thérapeutiques (« note relative aux preuves électroniques d'une relation thérapeutique et d'une relation de soins », règlement approuvé par le Comité de gestion de la plate-forme eHealth le 13 novembre 2018 et le Comité de sécurité de l'information le 4 décembre 2018), il est fait référence au « cercle de confiance ». Pour rappel, un cercle de confiance peut être défini comme « un groupe d'utilisateurs d'une organisation pour lequel l'organisation même prend, à plusieurs niveaux, des mesures relatives à la sécurité de l'information et en surveille le respect correct, de sorte que d'autres organisations puissent raisonnablement avoir confiance que ces mesures de sécurité de l'information sont respectées et qu'elles ne doivent pas les organiser ou les contrôler elles-mêmes ».

2. Il est apparu qu'en fonction des régions mais aussi en fonction du type d'organisation, les règles d'application de ce principe de cercle de confiance pouvaient différer. La Plate-forme eHealth a donc pris l'initiative de concrétiser ce principe afin d'assurer la cohérence à l'ensemble du secteur. Il est en effet essentiel que soient établies des règles minimales aux organisations qui appliquent le cercle de confiance. Cette concrétisation du principe est essentielle au maintien de la confiance des différents acteurs dans le système.

3. Lors de la réunion du 4 septembre 2019, le Comité de gestion de la plate-forme eHealth a approuvé, en deuxième lecture, la note relative au règlement fixant les critères en vue de l'application d'un cercle de confiance par une organisation dans le cadre de l'échange des données de santé. Ce règlement est disponible en annexe ainsi que sur le site web de la plateforme eHealth[1].

4. Les cercles de confiance peuvent être organisés par de nombreuses organisations telles les hôpitaux, les instances chargées de l'évaluation des besoins dans le cadre de BelRAI, les mutualités, etc. Pour que des organisations autres que l'organisation qui met en place un cercle de confiance, puissent légitiment y faire confiance, des critères sont fixés auxquels doit satisfaire toute organisation qui souhaite organiser ce type de cercle de confiance. Ces critères renvoient, dans toute la mesure du possible, à la législation belge et européenne actuelle telle le Règlement général sur la protection des données (RGPD). Ils ne portent pas préjudice à cette réglementation qui reste pleinement en vigueur, mais ils précisent dans certains cas comment il y a lieu de satisfaire à cette réglementation.

5. Après avis du Comité de gestion de la plate-forme eHealth le 11 juin 2019, ainsi que du Groupe de travail « Accès » du Comité de concertation des utilisateurs de la plate-forme eHealth, le 27 août 2019, une liste de 13 critères a été établie :

1° registre des activités de traitement ;
2° précision des fondements pour le traitement de catégories spécifiques de données à caractère personnel ;
3° limitation de traitement ;
4° authentification de l'identité de l'utilisation ;
5° vérification des caractéristiques pertinentes et des relations de l'utilisateurs ;

[1] https://www.ehealth.fgov.be/ehealthplatform/fr/reglements.

6° logging interne ;
7° audit trail ;
8° information, formation et sensibilisation ;
9° contrôle interne ;
10° respect des délibérations du Comité de sécurité de l'information ;
11° enregistrement dans la source authentique Cobrha en tant qu'organisation mettant en place un cercle de confiance ;
12° documentation publique ;
13° contrôle externe.

II. COMPÉTENCE

6. 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*, 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.

7. En effet, par la délibération n°09/008 du 20 janvier 2009, dernièrement modifiée le 15 juin 2010, le Comité s'est, en particulier, prononcé sur l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth lors de l'échange de données à caractère personnel. Un système fiable de gestion des utilisateurs et des accès détermine quel utilisateur peut avoir accès, en quelle qualité et dans quelles circonstances, à quels types de données à caractère personnel relatives à quelles personnes et à quelle période.

8. Le Comité de sécurité de l'information estime par conséquent qu'il est compétent.

III. EXAMEN

9. Le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes et le traitement de données à caractère personnel relatives à la santé est en principe interdit.

10. L'interdiction ne s'applique cependant pas lorsque le traitement est nécessaire à des fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé.

11. Le traitement de données à caractère personnel, en particulier de données à caractère personnel relatives à la santé, doit intervenir dans le respect des mesures relatives à la sécurité de l'information et à la protection de la vie privée. Un aspect essentiel dans ce contexte est la garantie que les données à caractère personnel sont uniquement traitées pour des finalités légitimes et par des personnes qui, pour pouvoir réaliser ces finalités, ont besoin de traiter des données à caractère personnel relatives à la personne concernée. Dans un système de traitement mutualisé de données à caractère personnel par de nombreux acteurs, l'offre de ce type de garantie requiert que les responsabilités de chacun

soient clairement définies. Le règlement entend y contribuer en précisant le concept des 'cercles de confiance'.

12. Le Comité ajoute, au-delà des règles fixées par la délibération n°09/008 précitée, qu'il est très important qu'il y ait des règles fixes sur l'application d'un « cercle de confiance ».

13. Le Comité rappelle que l'appartenance à un « cercle de confiance » ne dispense pas le groupe d'utilisateurs d'une organisation et l'organisation elle-même du respect des dispositions du règlement 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) ainsi que de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

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

approuve le règlement, en annexe, fixant les critères en vue de l'application d'un cercle de confiance par une organisation dans le cadre de l'échange des données de santé.

Bart VIAENE