Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/24/414

DÉLIBÉRATION N° 24/202 DU 3 DÉCEMBRE 2024 RELATIVE AUX BONNES PRATIQUES À APPLIQUER LORS DU DÉVELOPPEMENT D'APPLICATIONS « PATIENT CHANNEL » CONFORMÉMENT AUX CRITÈRES ÉTABLIS PAR LA PLATE-FORME EHEALTH

Le Comité de sécurité de l'information,

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

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 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant dispositions diverses*;

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

Vu le rapport de monsieur Michel Deneyer;

Émet, après délibération, la décision suivante, le 3 décembre 2024:

I. OBJET DE LA DEMANDE

1. Une « application patient channel » est une application (application web, application mobile, fat client, ...) qui vise à fournir aux usagers de soins un moyen sécurisé d'accès à leurs données à caractère personnel relatives à la santé sur la base de sources authentiques reconnues par la Plate-forme eHealth.

2. La Plate-forme eHealth préconise les 6 principes de base suivants pour les applications « patient channel » (selon la définition précitée) en ce qui concerne le traitement de données à caractère personnel relatives à la santé:

a. les données à caractère personnel peuvent être traitées par un prestataire de soins, une équipe de soins ou un établissement de soins qui a une relation de soins avec l'usager de soins;

b. la logique de traitement qui requiert l'accès à des données à caractère personnel relatives à la santé doit donc être localisée dans le logiciel utilisé par le prestataire de soins, l'équipe de soins ou l'établissement de soins;
c. les données à caractère personnel sont échangées entre le prestataire de soins, l'équipe de soins ou l'établissement de soins d'une part et l'usager de soins d'autre part moyennant un chiffrement end-to-end;
d. il n'est pas permis à d'autres instances que le prestataire de soins, l'équipe de soins ou l'établissement de soins d'avoir accès aux données à caractère personnel relatives à la santé échangées;
e. la source authentique peut proposer un composant de visualisation avec une possibilité d'extraction des données à caractère personnel par l'usager de soins;
f. le traitement ultérieur des données à caractère personnel extraites s'effectue sous la responsabilité de l'usager de soins.

II. COMPÉTENCE

3. En vertu de l'article 46, § 1er, 1°, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est chargée, dans une optique de protection de la vie privée, de formuler les bonnes pratiques qu'elle juge utiles pour l'application et le respect de cette loi et de ses mesures d'exécution et des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la santé.

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

III. BONNES PRATIQUES

5. Compte tenu des principes du Règlement général sur la protection des données (RGPD) et des dispositions 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 les les principes de base précités, qui doivent être respectés par les applications « patient channel ».

6. Ces principes de base précités doivent être respectés de manière cumulative par le gestionnaire d'applications.

7. La présente délibération entre en vigueur le 18 décembre 2024.

Michel DENEYER
Président