

<p>Comité de sécurité de l'information Chambre sécurité sociale et santé</p>
--

CSI/CSSS/20/180

DÉLIBÉRATION N° 20/098 DU 7 AVRIL 2020 RELATIVE AUX BONNES PRATIQUES À METTRE ŒUVRE PAR LES PLATE-FORMES POUR LES SOINS À DISTANCE DANS LE CADRE DE LA PANDÉMIE DE 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 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale*, en particulier l'article 46 ;

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

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la délibération suivante, le 7 avril 2020 :

I. OBJET DE LA DEMANDE

1. Dans le contexte COVID-19, des directives ont été établies pour les plateformes de soins à distance. Il s'agit d'un mécanisme global qui permet à différents types de soignants de dispenser des soins à leurs patients sans contact physique, de facturer ces prestations à l'assurance soins de santé, et aux patients de bénéficier de l'intervention financière de l'assurance soins de santé.

II. COMPÉTENCE

2. En vue de l'article 46, §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 peut formuler les bonnes pratiques qu'elle juge utiles pour l'application et le respect de la présente 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.
3. Le Comité s'estime dès lors compétent.

III. BONNES PRATIQUES

4. Compte tenu des principes du 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 formule les pratiques suivantes à respecter par les plateformes de soins à distance.
5. Ces plateformes ICT de soutien doivent répondre aux conditions minimales suivantes :
 - consentement du patient ;
 - communication vidéo via un outil permettant un cryptage « de bout en bout » ;
 - la communication vidéo ou audio n'est pas enregistrée sur la plateforme utilisée ;
 - si l'outil propose d'autres fonctions, outre la possibilité de communication vidéo ou audio, celles-ci sont proposées de telle sorte que les utilisateurs sont en mesure de respecter les règles d'utilisation ci-après ;
 - les documents qui contiennent des données à caractère personnel peuvent uniquement être échangés via un système qui prévoit un chiffrement de bout en bout et qui inclut un système fiable d'authentification de l'identité des utilisateurs ; les moyens d'authentification avec une authentification à deux facteurs (possession et connaissance) qui sont intégrés dans le Federal Authentication Service (FAS), tels que la carte d'identité électronique, Itsme ou, pour les patients, l'authentification générée dans le cadre de la plateforme Helena, sont considérés comme des systèmes fiables d'authentification de l'identité des utilisateurs ;
 - le patient est physiquement et mentalement en mesure d'utiliser un ordinateur.

6. 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.
7. Les règles d'utilisation sont les suivantes :
- la communication vidéo ou audio n'est pas enregistrée par les participants à la communication ;
 - les prescriptions de médicaments sont établies par la voie électronique sur Recip-e et sont consultables par le patient via le Personal Health Viewer ; le numéro unique de la prescription électronique (ou RID), qui ne contient pas de données à caractère personnel, peut être transmis au patient¹ ;
 - les documents que le prestataire de soins et/ou le patient peuvent consulter via le portail eSanté ou le Personal Health Viewer sont en principe consultés à cet endroit.
8. Le Comité rappelle qu'en vertu de l'article 9 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, le responsable du traitement 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.

Bart VIAENE

Le siège du Comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante : Quai de Willebroeck, 38 - 1000 Bruxelles (tél. 32-2-741 83 11).

¹ Voyez à ce sujet https://www.riziv.fgov.be/fr/themes/cout-remboursement/par-mutualite/medicament-produits-sante/prescrire_medicaments/Pages/prescription-medicale.aspx