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

CSI/CSSS/22/206

DÉLIBÉRATION N° 20/098 DU 7 AVRIL 2020, MODIFIÉE LE 24 MAI 2022, RELATIVE AUX BONNES PRATIQUES À METTRE ŒUVRE PAR LES PLATE-FORMES POUR LES SOINS À DISTANCE

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 24 mai 2022 :

I. OBJET DE LA DEMANDE

1. Pendant la pandémie de 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 prestataires de soins de dispenser des soins à leurs utilisateurs de soins sans contact physique, de facturer ces prestations à l'assurance soins de santé, et aux utilisateurs de soins 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 de sécurité de l'information 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.

Les conditions minimales et règles d'utilisation mentionnées ci-après sont applicables aux applications et plateformes de communication vidéo et audio et d'échange de données qui sont utilisées pour les consultations à distance. Le dossier de patient informatisé, qui est géré par le prestataire de soins ou l'établissement de soins, ne fait pas partie de ces applications et plateformes de communication. La gestion du dossier de patient informatisé et la communication de données du dossier de patient informatisé sont régies par la réglementation et les bonnes pratiques existantes.

5. Ces plateformes ICT de soutien doivent répondre aux conditions minimales suivantes :

- consentement de l'utilisateur de soins ;
- libre choix de l'utilisateur de soins ;
- l'utilisateur de soins est clairement informé avant l'utilisation de la plateforme des facteurs de succès critiques et des limites d'une consultation à distance ;
- les utilisateurs de la plateforme de soutien utilisent un système fiable pour l'authentification de leur identité ; les moyens d'authentification avec authentification à deux facteurs (possession et connaissance) qui sont intégrés dans le Federal Authentification Service (FAS) tels la carte d'identité électronique, Itsme ou, pour les utilisateurs de soins, l'authentification générée dans le cadre de la plateforme Helena, sont déjà considérés comme des systèmes fiables d'authentification de l'identité des

utilisateurs ; l'usage dans le secteur de la santé des moyens d'authentification intégrés dans le FAS est déjà intégralement remboursé par les pouvoirs publics de sorte que leur usage est gratuit pour l'utilisateur de soins et ne peut pas être facturé à l'assurance maladie ou au prestataire de soins ; ceci est valable quelles que soient les modalités d'utilisation de ces moyens d'authentification (via CSAM ou d'application à application) ;

- la communication vidéo, audio et de données à caractère personnel et l'échange de documents contenant des données à caractère personnel s'effectuent moyennant un cryptage « de bout en bout » ; le fournisseur de la plateforme utilisée ne peut à aucun moment prendre connaissance du contenu de cette communication ou de ces documents; seuls l'utilisateur de soins et le(s) prestataire(s) de soins qui participent à la communication peuvent prendre connaissance de leur contenu ;
- la communication vidéo, audio et les données à caractère personnel ne sont pas enregistrées sur la plateforme utilisée avant ou après la consultation à distance; les métadonnées relatives à la consultation à distance peuvent être transmises aux organismes assureurs et utilisées par ces derniers à des fins de facturation ;
- si l'outil propose d'autres fonctions, outre la possibilité de communication vidéo, audio et de données à caractère personnel, celles-ci sont proposées de telle sorte que les utilisateurs sont en mesure de respecter les règles d'utilisation ci-après ;
- l'utilisateur de soins est capable d'exprimer sa volonté et est physiquement et mentalement en mesure d'utiliser un dispositif lui permettant de participer à la consultation à distance.

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 :

- préalablement à la consultation à distance, une relation thérapeutique ou une relation de soins doit exister entre l'utilisateur de soins et le prestataire de soins et celle-ci doit être prouvée conformément au règlement relatif aux preuves électroniques d'une relation thérapeutique et d'une relation de soins (voir https://www.ehealth.fgov.be/ehealthplatform/fr/reglements) ;
- si la relation thérapeutique ou la relation de soins entre l'utilisateur de soins et le prestataire de soins est établie juste avant le début de la consultation à distance, l'utilisateur de soins est dûment informé au préalable des conséquences de l'établissement de cette relation thérapeutique ou relation de soins et il est mis fin à cette relation thérapeutique ou relation de soins à l'issue de la consultation à distance, à moins que l'utilisateur de soins ne formule explicitement le souhait de maintenir cette relation thérapeutique ou relation de soins ;

- la communication vidéo ou audio n'est pas enregistrée par les participants à la communication ;
- la consultation à distance a une certaine durée et a lieu dans des circonstances qui sont suffisantes pour garantir une prestation de soins de qualité ;
- les données à caractère personnel et les documents échangés lors de la consultation peuvent être mis à la disposition des participants à la communication à l'issue de la consultation ;
- les prescriptions de médicaments sont établies par la voie électronique sur Recip-e et sont consultables par l'utilisateur de soins 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 utilisateur de soins[1] ;
- les documents que le prestataire de soins et/ou l'utilisateur de soins peuvent consulter via le portail eSanté ou le Personal Health Viewer sont en principe consultés à cet endroit ;
- en vue de l'appui de la prestation de soins, le prestataire de soins a de préférence recours à un logiciel enregistré auprès de la Plate-forme eHealth et enregistre, en toute hypothèse, les données pertinentes relatives à la prestation de soins dans un dossier de patient (électronique) ;
- si le prestataire de soins n'est pas le détenteur du dossier médical global (DMG) du patient, il envoie, sauf opposition de l'utilisateur de soins, un feedback (électronique) relatif aux soins fournis au détenteur (éventuel) du DMG et actualise, si cela s'avère utile, le SumEHR et le schéma de médication dans le coffre-fort de l'utilisateur de soins.

[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

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
Président