Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/26/034

DÉLIBÉRATION N° 26/018 DU 3 MARS 2026 RELATIVE AUX BONNES PRATIQUES À METTRE EN ŒUVRE PAR LES PRESTATAIRES DE SERVICES DANS LES SOINS DANS LE CADRE DU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ

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 de monsieur Michel Deneyer ;

Émet, après délibération, la décision suivante, le 3 mars 2026 :

I. OBJET DE LA DEMANDE

1. L'offre existante de prestataires de services proposant notamment des services d'imagerie médicale et de tests de la capacité physique, constitue une offre complémentaire à laquelle les usagers de soins peuvent de plus en plus souvent faire appel. Ceci n'a pas toujours lieu dans le cadre des prestations de soins reconnues, mais ces activités présentent clairement des points communs avec les soins de santé classiques.

2. Le Comité de sécurité de l'information a été prié d'établir une série de directives pour le traitement de données à caractère personnel relatives à la santé afin de promouvoir le respect des droits des usagers 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 formule les pratiques suivantes à respecter par les prestataires de services dans les soins qu'ils soient commerciaux ou non.

6. Ces prestataires de services doivent répondre aux conditions minimales suivantes :

I. Dispositions préalables:

1. L'usager de soins dispose du libre choix du médecin traitant pour l'examen et le suivi de son dossier et doit être dûment informé à ce sujet. Cela implique au minimum
   - i. qu'il doit être clair quels sont les médecins traitants. Cette information est clairement renseignée dans les locaux du prestataire de services et sur son site web. L'usager de soins doit en être explicitement informé par le prestataire de services.
   - ii. que l'usager de soins doit avoir la possibilité de choisir un ou plusieurs médecins traitants parmi cette liste. Ce choix doit être respecté.
2. La prestation de soins s'effectue sous la surveillance de personnel qualifié.
   - i. Une organisation qui propose des actes médicaux (tels que l'imagerie médicale) doit le faire sous la surveillance d'un professionnel des soins de santé tel que défini dans la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé.
   - ii. Lors de la prestation du service, une relations de soins (de santé) doit être créée avec au moins un des médecins indiqués comme médecins traitants possibles ou avec le cabinet de médecine qui assure la surveillance de la prestation de services et du traitement des données à caractère personnel, compte tenu du choix éventuel effectué par l'usager de soins.
   - iii. Une relation de soins (de santé) peut uniquement être créée en utilisant ou présentant la carte eID de l'usager de soins et en communiquant le numéro de l'eID. Il n'est pas autorisé d'utiliser le numéro eID pour d'autres finalités que la création d'une relation de soins (de santé) ou de conserver le numéro de l'eID dans le système d'information du médecin, du prestataire de services ou d'un

fournisseur d'un prestataire de services après la création de la relation de soins (de santé) ou au-delà de 168 heures. Il n'est pas autorisé de créer une relation de soins (de santé) à l'issue du délai de 168 heures en ayant simplement recours à des données stockées dans les systèmes d'information du médecin, du prestataire de services ou d'un fournisseur de ce prestataire de services.

iv. Secret professionnel et confidentialité : les collaborateurs du prestataire de services sont tenus, en vertu d'une obligation légale, statutaire ou contractuelle équivalente, de respecter le caractère confidentiel des données.
v. Les catégories de personnes qui ont accès aux données de santé doivent être décrites avec précision. Ces listes sont tenues à la disposition de l'autorité de contrôle compétente[1].
vi. Contrôle interne : l'organisation doit prévoir des mesures de contrôle interne afin de contrôler les loggings et de garantir que les rôles attribués aux collaborateurs répondent aux principes de base de limitation de la finalité et de proportionnalité.

II. Traitement de données à caractère personnel
    1. Dans les locaux et sur le site web du prestataire de services, il y a lieu d'indiquer clairement qui sont les médecins traitants, comment les données sont traitées, de quelle façon l'usager de soins peut exercer ses droits, quelles sont les possibilités en matière d'envoi du dossier, la procédure en matière de plaintes ainsi que les coordonnées du DPO.

III. Exigences techniques et organisationnelles.
    1. Les loggings de sécurité doivent être conservés.
        i. Tout(e tentative de) traitement de données à caractère personnel doit faire l'objet d'un enregistrement dans les loggings.
        ii. Le logging doit être effectué d'une manière non-répudiable, de sorte qu'il soit enregistré quel collaborateur a eu accès aux données de quel usager de soins, à quel moment et pour quelles finalités.
        iii. Le traitement de données à caractère personnel doit être effectué de manière conforme au RGPD.
    2. Échange de données et enregistrement
        i. Chiffrement et communication : les documents qui contiennent des données à caractère personnel (tels les images de body mapping 3D ou le rapport) sont de préférence échangés via le système hub/metahub ou au moyen d'un système avec un chiffrement end-to-end qui prête suffisamment attention à l'identification du destinataire de l'information.

[1] Article 9 du la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

7. Le Comité de sécurité de l'information 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 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 à caractère personnel visées;

2° la liste des catégories de 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.

Par ces motifs,

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

conclut que

le traitement de données à caractère personnel relatives à la santé doit être effectué selon les dispositions de cette délibération.

Cette délibération constitue un cadre général à respecter lorsque des données à caractère personnel relatives à la santé sont traitées. Elle ne porte nullement atteinte à la compétence du Comité de sécurité de l'information de se prononcer au cas par cas sur ce type de communication de données.

La présente délibération entre en vigueur le 18 mars 2026.

Michel DENEYER
Président