

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

CSI/CSSS/25/366

BONNES PRATIQUES (N° 25/212 DU 2 DÉCEMBRE 2025) À APPLIQUER LORS DU DÉVELOPPEMENT D'APPLICATIONS D'AGENDA 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 2 décembre 2025:

I. OBJET DE LA DEMANDE

1. Une application d'agenda permet à un usager de soins de fixer (enregistrer) un rendez-vous chez un prestataire de soins en mode en ligne ou via une application mobile ou de gérer les rendez-vous existants. De son côté, le prestataire de soins peut gérer les rendez-vous qui ont été pris chez lui.
2. Lors de l'enregistrement de rendez-vous, l'usager de soins a la possibilité d'ajouter des données à caractère personnel relatives à sa santé, telles que le motif de sa consultation (p.ex. description des symptômes ou rapport d'un examen). Le type de prestataire de soins chez qui un rendez-vous est pris permet parfois aussi de déduire des données à caractère personnel relatives à la santé (p.ex. consultation chez un psychiatre ou un oncologue). L'enregistrement d'un rendez-vous implique dès lors une combinaison de différents types de données à caractère personnel:

- des données administratives telles que le nom, des données de contact, la date et l'heure du rendez-vous;
 - des données à caractère personnel relatives à la santé qui ont explicitement trait à l'état de santé telles les symptômes, la nature de la demande de soins ou des remarques complémentaires en lien avec le rendez-vous;
 - des données à caractère personnel relatives à la santé qui ont implicitement trait à l'état de santé telles la spécialité du prestataire de soins consulté.
3. Un fournisseur d'une application d'agenda a indiqué qu'il souhaite aussi conserver les données à caractère personnel relatives à la santé dans l'application d'agenda après que le rendez-vous a eu lieu. Il souhaite à cet égard intervenir comme sous-traitant des prestataires de soins concernés.
 4. Le Comité de sécurité de l'information est invité à se prononcer sur la question quant à savoir si des données à caractère personnel relatives à la santé peuvent être conservées dans une application d'agenda après que le rendez-vous a eu lieu.

II. COMPÉTENCE

5. En vertu de l'article 46, § 1^{er}, 1^o, 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.
6. Le Comité de sécurité de l'information estime par conséquent qu'il est compétent.

III. BONNES PRATIQUES

7. Compte tenu des principes du Règlement général sur la protection des données (RGPD), 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* et de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé*, la chambre sécurité sociale et santé du Comité de sécurité de l'information formule les bonnes pratiques suivantes qui doivent être respectées par les applications d'agenda. Celles-ci ont exclusivement trait au traitement de données à caractère personnel relatives à la santé dans une application d'agenda, à l'exclusion des données administratives qui sont également enregistrées à cette occasion.
8. Eu égard au principe de proportionnalité et de minimalisation des données, l'enregistrement permanent de données à caractère personnel relatives à la santé dans l'application d'agenda, lorsque celles-ci sont déjà disponibles dans le DPI, n'est pas conforme aux principes des articles 5, alinéa 1^{er} b) et c) et 9 du RGPD.
9. Une application d'agenda a pour finalité de créer et de gérer des rendez-vous. Le traitement de données à caractère personnel relatives à la santé dans l'application d'agenda doit donc se limiter à ce qui est strictement nécessaire pour la création et la gestion des rendez-vous. La conservation de données à caractère personnel relatives à la santé après que le rendez-vous a eu lieu, ne fait pas partie de cette finalité et doit donc avoir lieu dans le DPI. En

vertu de l'article 9 du RGPD, le traitement de données à caractère personnel relatives à la santé est interdit, sauf s'il est satisfait à une exception spécifique.

Lorsqu'un patient introduit des informations relatives à son état de santé dans l'application d'agenda et qu'une consultation a effectivement lieu, le prestataire de soins doit, dans les limites de sa compétence, obligatoirement enregistrer des informations dans le DPI, conformément à l'article 33 de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé*.

10. En ce qui concerne les prestataires de soins qui sont actifs dans un secteur dans lequel il existe une procédure d'enregistrement de logiciels (médecins, infirmiers et kinésithérapeutes) et pour les hôpitaux, il est garanti que ces informations peuvent effectivement être enregistrées dans le DPI et que le DPI demeure par conséquent la source authentique, conformément à l'article 33 de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé*. Dans le souci de la qualité et de la continuité des soins, le rapport de la consultation et les données à caractère personnel relatives à la santé pertinentes doivent, en effet, être repris dans le dossier de patient informatisé, qui est intégré dans le réseau d'échange de données sécurisé et les coffres-forts de santé. L'offreur d'une application logicielle intervient, le cas échéant, comme le sous-traitant des prestataires de soins concernés, qui sont les responsables du traitement, et supprime les données à caractère personnel relatives à la santé dans l'application d'agenda dès que le rendez-vous a eu lieu.
11. En ce qui concerne les prestataires de soins qui sont actifs en dehors de l'hôpital dans un secteur dans lequel il n'existe pas de procédure d'enregistrement de logiciel, les données à caractère personnel relatives à la santé peuvent être conservées dans l'application d'agenda, pendant un délai raisonnable, et doivent se limiter à ce qui est strictement nécessaire pour les finalités pour lesquelles ces données sont traitées, si le patient a donné son consentement éclairé à cet effet et que ceci intervient conformément aux dispositions de la RGPD. À cet égard, l'offreur de l'application d'agenda intervient aussi comme le sous-traitant des prestataires de soins concernés, qui sont les responsables du traitement.
12. Il est loisible à tout fournisseur de logiciel de commercialiser des logiciels de soutien des dossiers patients informatisés et les critères d'enregistrement et l'usage des services de base de la Plate-forme eHealth permettent de garantir la qualité et la sécurité de l'information. En vue du respect de la réglementation relative à la protection des données, le Comité recommande fortement l'enregistrement et l'usage de ces services de base.
13. 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 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.

Ces bonnes pratiques entrent en vigueur le 17 décembre 2025.

Michel DENEYER
Président

Le siège de la chambre sécurité sociale et santé 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).