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

CSI/CSSS/21/376

DÉLIBÉRATION N° 10/085 DU 21 DÉCEMBRE 2010, MODIFIÉE EN DERNIER LIEU LE 7 DÉCEMBRE 2021, RELATIVE À L'ORGANISATION DE LA COMMUNICATION DE PRESCRIPTIONS ÉLECTRONIQUES AMBULATOIRES DANS LE CADRE DE RECIP-E ET DE L'APPLICATION PARIS

Le Comité de sécurité de l'information,
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 sur 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 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale* ;

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 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 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*, en particulier l'article 97 ;

Vu la délibération n° 12/047 du 19 juin 2012, modifiée en dernier lieu le 18 avril 2017 et le 18 juillet 2017, relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement ;

Vu l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* ;

Vu la délibération n° 10/085 du 21 décembre 2010 et les versions modifiées du 15 décembre 2015, du 16 janvier 2018 et du 7 décembre 2021 ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 1er décembre 2021 ;

Emet, après délibération, la décision suivante, le 7 décembre 2021 :

I. OBJET DE LA DEMANDE

i. RECIP-E

1. L'Institut national d'assurance maladie-invalidité (dénommé ci-après : « l'INAMI ») implémente au moyen du projet Recip-e l'utilisation de la prescription électronique ambulatoire. Dans la première phase, l'objectif du projet était de mettre en pratique le modèle de la prescription électronique ambulatoire développé en Belgique, de tester ce modèle dans plusieurs régions et de préparer sa mise en œuvre nationale à l'aide de ces expériences. Actuellement, le déploiement national de Recip-e est en cours pour les médecins et les pharmaciens. Par ailleurs, la prescription électronique ambulatoire est implémentée dans les hôpitaux. Finalement, Recip-e est également disponible pour les dentistes et les sages-femmes d'une part et pour les kinésithérapeutes et les infirmiers d'autre part, respectivement en tant que prescripteurs et en tant qu'exécutants d'une prescription.

2. Compte tenu du cadre juridique de la prescription électronique ambulatoire, tel que prévu à l'article 42 de la loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé, les prescriptions électroniques ambulatoires doivent pouvoir être échangées de manière électronique entre le prestataire de soins qui a créé la prescription et le prestataire de soins choisi par le patient pour exécuter la prescription.

3. Afin d'organiser l'architecture nécessaire pour l'échange des prescriptions électroniques ambulatoires, le Comité de l'assurance soins de santé de l'INAMI a lancé en 2009 un appel public à un partenaire technique. Il a été répondu à l'appel par l'asbl Recip-e, dont les membres sont diverses associations professionnelles représentatives de dispensateurs de soins reconnues par la loi[1]. Conformément à ses statuts, cette asbl a pour objectifs:
   - d'intervenir en tant que partenaire contractuel pour le projet pilote « Prescription électronique ambulatoire »;
   - d'accompagner, de réaliser et de gérer le système Recip-e pour la prescription électronique pour les diverses professions des soins de santé;
   - d'intervenir comme organe de concertation dans le but d'adopter, autant que possible, des positions communes sur la prescription électronique, dans le contexte plus large des TIC dans les soins de santé, et de développer des concepts et des modèles.

[1] Algemene Pharmaceutische Bond / Association Pharmaceutique Belge, Belgische vereniging van artsensyndicaten / Association Belge des Syndicats Médicaux, Vereniging der Coöperatieve Apotheken van België / Office des Pharmacies coopératives de Belgique, KARTEL (ASGB – GBO – SBGS/SBMS) / CARTEL (ASGB – GBO – SBGS/SBMS), AADM, AXXON, Nationaal Verbond van Katholieke Vlaamse Verpleegkundigen en Vroedvrouwen, Verbond der Vlaamse Tandartsen.

4. Dans le cadre du projet précité, l'asbl Recip-e a développé l'architecture suivante pour l'échange de prescriptions électroniques ambulatoires entre les acteurs concernés, plus précisément entre un prescripteur *en dehors* d'un hôpital et le prestataire des soins prescrits ou entre un prescripteur *dans* un hôpital et un prestataire des soins prescrits.

5. Concrètement, le flux de données électronique Recip-e pour l'échange de prescriptions électroniques ambulatoires comprend quatre flux différents:
   - du prescripteur vers le stockage temporaire Recip-e;
   - du stockage temporaire vers le prestataire des soins prescrits;
   - feedback éventuel du prestataire de soins au prescripteur;
   - si le patient le souhaite, avertissement éventuel, par le prescripteur à un prestataire de soins, de l'arrivée d'une prescription.

6. Pendant une période limitée, un flux papier continue à exister pendant la mise en œuvre nationale. Les prescriptions actuelles, imprimées sur papier, pourvues d'un numéro d'identification unique par prescription (en format code-barre et en texte lisible), sont remises par le prescripteur au patient qui, à son tour, fournit la prescription au prestataire de soins de son choix et possédant la compétence correcte (pharmacien pour les prescriptions médicamenteuses, kinésithérapeutes pour les prescriptions kiné et infirmiers pour les prescriptions infirmières). Par ailleurs, il existe aussi une alternative dématérialisée. Le prescripteur n'imprime pas la prescription. A l'aide de l'eID / du numéro de registre national, le pharmacien peut obtenir toutes les prescriptions ouvertes. Il existe également une appli permettant d'obtenir la prescription spécifique de manière analogue à la prescription papier.

7. La prescription sera créée de manière électronique par le prescripteur, à savoir un médecin, un dentiste ou une sage-femme, au moyen de son logiciel. Dans la mesure où le prescripteur n'établit pas la prescription ambulatoire dans son cabinet mais dans un hôpital, le logiciel employé pour la créer sera le logiciel DMI de l'hôpital. La prescription doit être conforme aux dispositions légales en vigueur. Le Comité souligne que la présente délibération se limite à l'évaluation du traitement de données à caractère personnel dans le cadre de la communication électronique de la prescription et que la composition de la prescription électronique ambulatoire ne fera pas l'objet de cette délibération.

8.1 Pour l'authentification du prescripteur, le logiciel du prescripteur demande via la plate-forme eHealth un token SAML pour une session. La durée de validité de la session est limitée dans le temps. Ce token SAML sert de preuve aux systèmes que l'utilisateur est un prescripteur valide. L'information d'identification est obtenue d'une part via le certificat 'Holder-of-Key'[2] qui authentifie l'utilisateur de l'application et qui est délivré par eHealth. Ce certificat contient l'identité du responsable de la gestion de l'application. D'autre part, l'information d'identification est obtenue via l'identification (NISS) du prescripteur même qui a ouvert la session.

[2] Holder of Key : certificat technique qui permet la délégation de l'identité au certificat installé en local.

9. Il y a lieu d'opérer une distinction entre, d'une part, une prescription médicale ambulatoire créée sur le système d'un prescripteur individuel et, d'autre part, une prescription médicale ambulatoire créée dans un hôpital à partir d'un système hospitalier (DMI).

9.1. Dans le premier cas, l'information d'identification du prescripteur est obtenue au moyen du logiciel du médecin sur la base de son identification (NISS), soit via son eID (avec introduction du code PIN), soit au moyen d'un certificat de cryptage personnel (certificat eHealth) et de la clé privée y associée (qui fait office en l'occurrence de moyen d'authentification de l'identité du titulaire), délivré par la plate-forme eHealth. Pour cette dernière méthode, l'utilisateur doit introduire une phrase de passe pour sa clé privée.

9.2. Dans le cas d'une prescription médicale ambulatoire créée dans un hôpital pour être exécutée en dehors de l'hôpital (par exemple dans une officine publique), l'hôpital est garant de la traçabilité de l'identification correcte et univoque du prescripteur pour chaque prescription établie au sein de l'hôpital. L'hôpital qui est responsable, via le certificat 'Holder-of-Key', de la gestion de l'application (de prescription), garantit à tout moment qu'il conserve l'information d'identification correcte du prescripteur d'une prescription déterminée et qu'il est en mesure d'en fournir la preuve en cas de demande. L'identification du prescripteur de toute prescription unique est garantie selon le concept des cercles de confiance[3] et par la combinaison des informations d'identification disponibles, d'une part, dans le certificat 'Holder-of-Key' qui authentifie le propriétaire de l'application et, d'autre part, dans la gestion des accès et des loggings de la part de l'hôpital et de l'identité du prescripteur (personne physique) présente dans la partie chiffrée de la prescription qui peut être déchiffrée par l'hôpital.

Le logging au sein de l'hôpital doit comporter le numéro d'identification Recip-e unique (RID) de chaque prescription ambulatoire envoyée. En regroupant périodiquement les prescriptions Recip-e (par analogie avec les prescriptions intra-muros), après avoir appliqué une fonction de hachage, dans un 'timestamp bag' avant de proposer celui-ci au service de timestamping de la Plate-forme eHealth, il est garanti que la prescription ne pourra pas être modifiée de manière inaperçue après l'application du timestamping.

Tant l'hôpital que les instances de contrôle ont la possibilité de procéder ensuite à un nouveau hachage des prescriptions électroniques et de vérifier si le résultat correspond au résultat de hachage qui a fait l'objet d'un timestamp et d'une signature électroniques de la Plate-forme eHealth. Ceci permet d'avoir la certitude que la prescription n'a pas été modifiée.

9.3. L'authentification de l'identité du prescripteur d'une prescription ambulatoire au sein d'un hôpital doit s'effectuer selon les méthodes d'authentification décrites dans le « Protocole portant les conditions et les modalités selon lesquelles un document électronique peut être associé, de manière précise, à une date de référence et une heure de référence et ne peut

[3] Cercles de confiance (« circles of trust ») : une série d'accords méthodologiques et techniques entre des parties de confiance qui protègent l'information de manière irréfutable.

plus être modifié de manière inaperçue, dans le cadre de la prescription hospitalière électronique ». Ce protocole a fait l'objet d'un avis positif[4] du Comité sectoriel[5].

Ceci signifie que chaque hôpital doit établir les procédures nécessaires pour garantir une identification et authentification correctes du prescripteur. Seuls deux types de procédures d'authentification peuvent être prévues à cet égard, à savoir une authentification au moyen du nom d'utilisateur et d'un mot de passe ou une authentification au moyen du certificat d'authentification sur la carte d'identité électronique ou d'un autre certificat répondant aux dispositions de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

En ce qui concerne l'authentification au moyen d'un nom d'utilisateur et d'un mot de passe, le protocole spécifie que ce nom d'utilisateur et le mot de passe sont strictement personnels et ne sont pas transférables. Le mot de passe peut être soit utilisable une seule fois, soit utilisable de nombreuses fois. En cas de mot de passe utilisable plusieurs fois, le prescripteur est tenu de modifier le mot de passe le plus rapidement possible après réception ou du moins au moment de la première utilisation. Si le mot de passe peut être utilisé plusieurs fois, le prescripteur doit ensuite régulièrement modifier ce mot de passe.

Le protocole précise qu'un mot de passe sûr est idéalement composé de 15 caractères et d'au moins 8 caractères. Un mot de passe peut soit être utilisable une seule fois sur base d'un "challenge" chiffré pour chaque utilisation (mot de passe dynamique), soit être utilisable plusieurs fois (mot de passe statique). Un mot de passe utilisable plusieurs fois contient des symboles et des caractères alphanumériques placés dans un ordre qui se laisse difficilement deviner. Chaque prescripteur doit veiller à ce que le mot de passe choisi réponde à ces conditions. La responsabilité d'un prescripteur est engagée lorsqu'un mot de passe est décelé et/ou utilisé de manière illicite.

Il appartient à chaque prescripteur de faire un usage judicieux de son nom d'utilisateur et mot de passe et d'assurer le secret en ce domaine. Chaque prescripteur assume la responsabilité de tout usage approprié ou non de son nom d'utilisateur et mot de passe, en ce compris l'usage par des tiers.

Lorsqu'un prescripteur est au courant de la perte de son nom d'utilisateur et/ou mot de passe ou d'une quelconque utilisation inappropriée de son nom d'utilisateur et/ou mot de passe par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée, il doit prendre immédiatement toutes les mesures nécessaires et en informer le conseiller en sécurité de l'information de l'hôpital.

Dès la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour éviter tout abus.

[4] Avis du Comité sectoriel de la sécurité sociale et de la santé n° 11/01 du 15 février 2011.

[5] Actuellement la chambre sécurité sociale et santé du Comité de sécurité de l'information.

Jusqu'à l'inactivation du nom d'utilisateur et du mot de passe, chaque prescripteur reste responsable de tout usage légitime de son nom d'utilisateur et/ou mot de passe et de tout usage illégitime suite à la négligence de son nom d'utilisateur et/ou mot de passe.

10. Une fois la prescription électronique créée, elle est, après authentification du logiciel du prescripteur activé et après authentification du médecin prescripteur même, préparée par le logiciel local avant qu'elle ne puisse être envoyée au système central de Recip-e.

11. La préparation de la prescription électronique s'effectue comme suit. La prescription électronique est chiffrée par le module du logiciel du prescripteur au moyen du service de base de cryptage de la plate-forme eHealth, de sorte qu'elle ne puisse être ouverte et lue que par une personne habilitée, à savoir le prescripteur de la prescription, le patient ou un prestataire de soins compétent choisi par le patient pour exécuter la prescription. Ensuite, les informations administratives suivantes sont ajoutées à la prescription chiffrée:
    - la référence de la clé utilisée lors du chiffrement, afin de pouvoir récupérer la clé auprès du dépôt de clés;
    - le code du type de document, à savoir un code indiquant s'il s'agit ou non d'une prescription médicamenteuse, un code indiquant si la prescription médicamenteuse requiert des informations sur l'assurabilité, et un code indiquant si la prescription médicamenteuse requiert des informations sur la présence d'une autorisation préalable d'un médecin- conseil;
    - le numéro national d'identification de la sécurité sociale (NISS) du patient et le numéro d'identification du prescripteur. A cet égard, une distinction est opérée entre la prescription ambulatoire créée par a) un prescripteur individuel et b) un prescripteur dans un hôpital :
        a) en cas de prescription ambulatoire créée par un prescripteur individuel, le numéro d'identification du prescripteur est soit le NISS, soit le numéro INAMI du prescripteur ;
        b) en cas de prescription ambulatoire créée par un prescripteur dans un hôpital, le numéro d'identification du prescripteur est le numéro d'identification de l'hôpital. L'hôpital doit pouvoir prouver à tout moment et de manière univoque (au moyen de sa gestion interne des utilisateurs) l'identité du prescripteur associé à cette prescription.

12. Avant que la prescription chiffrée et les informations administratives ne soient transmises au système central de Recip-e, l'ensemble est chiffré à nouveau de sorte que seul le système central de Recip-e puisse déchiffrer les deux composants (sans évidemment ne pouvoir déchiffrer la prescription chiffrée en tant que telle). Ensuite, plusieurs contrôles de sécurité sont effectués afin de garantir que la prescription provienne effectivement du prescripteur concerné. Lorsqu'un de ces contrôles est négatif, un message d'erreur est renvoyé au logiciel du prescripteur. Lorsque les contrôles de sécurité connaissent un résultat positif, le message est traité et pourvu d'un numéro d'identification unique pour chaque prescription. Le message résultant est ensuite envoyé au système central de Recip-e.

13. Le système central de Recip-e peut ensuite traiter le message:
    - la partie destinée à Recip-e, à savoir la prescription chiffrée ainsi que les informations administratives à nouveau chiffrées, peut être déchiffrée par le système central de Recip-

e, ce qui permet au système Recip-e de lire (uniquement) les informations administratives;
- la prescription chiffrée est sauvegardée et soumise à un horodatage au moyen du service de base de la plate-forme eHealth 6 et un logging de sécurité est effectué;
- dans la mesure où la prescription peut être enregistrée correctement dans le système central de Recip-e, le numéro d'identification du document devient le numéro d'identification unique Recip-e. Ceci est requis pour une impression d'une prescription électronique correctement sauvegardée;
- la plate-forme eHealth conserve des loggings contenant une indication de quelle personne (sur base du numéro INAMI des intéressés) a effectué une transaction à quel moment et pour quelle partie administrative, ainsi que les éventuels messages d'erreur. La plate-forme eHealth ne conserve, en aucun cas, des traces de la prescription chiffrée en tant que telle.

14. Pour extraire ensuite la prescription médicale électronique du système central Recip-e, les procédures suivantes ont été développées.

15. Au cours de la phase actuelle du projet Recip-e, l'exécuteur d'une prescription est toujours un pharmacien. A l'avenir, un infirmier ou un kinésithérapeute pourra également extraire une prescription qui lui est destinée. Lorsque le patient présente son eID / numéro NISS, une relation thérapeutique est créée avec le patient / l'existence d'une relation thérapeutique est consultée auprès de l'exécuteur.

    En cas d'urgence, il est possible d'obtenir accès aux données sur le serveur central de Recip-e sans validation de la relation thérapeutique ou relation de soins ou des exclusions. Il s'agit de la procédure dite « break the glass ». Recip-e prévoira les « cas d'urgence » (motifs pour « break the glass ») possibles dans les spécifications à l'attention des fournisseurs de logiciels et le prestataire de soins devra lui-même indiquer dans quel cas d'urgence il se trouve. Dans ce cas, le prestataire de soins devra lui-même, par la suite, créer la relation thérapeutique si elle n'existait pas encore. Le prestataire de soins doit déclarer formellement que la procédure est uniquement utilisée dans un cas d'urgence et qu'il en assume la responsabilité. L'accès est immédiatement accordé au prestataire de soins sans que la relation thérapeutique ou la relation de soins ne soit vérifiée et sans contrôler les exclusions. Le nombre de fois où la procédure « break the glass » est appliquée, à quels moments et les raisons de son application feront l'objet d'un logging spécifique dans les loggings de sécurité. Ceci pourra être contrôlé. Cette possibilité est uniquement proposée aux prestataires de soins qui peuvent accéder au serveur central de Recip-e au moyen du certificat d'authentification délivré par eHealth.

    Cette procédure d'exception peut être appliquée moyennant certaines garanties : le prestataire de soins doit indiquer la raison pour laquelle la procédure d'urgence est appliquée, de sorte à permettre un contrôle a posteriori par toute partie concernée. Le prestataire de soins doit en outre créer par la suite la relation thérapeutique de façon manuelle et, dès que le service est à nouveau disponible, il devra synchroniser cette relation thérapeutique créée de manière asynchrone.

[6] Voir la délibération n° 10/045 du 15 juin 2010 de la section Santé du Comité sectoriel de la sécurité sociale et de la santé relative à l'application du service de base d'horodatage électronique par la plate-forme eHealth.

Un monitoring des relations thérapeutiques créées de manière asynchrone dans le cadre de la procédure « break the glass » est implémenté. Le nombre d'applications manuelles de l'action « break the glass » pourra être vérifié a posteriori auprès de l'organisation qui gère la banque de données des relations thérapeutiques. Par ailleurs, Recip-e vérifiera, via monitoring, auprès de tous les fournisseurs de services concernés dans la chaîne (CIN, Registre national, Plate-forme eHealth, BCSS, fournisseur réseau) si le motif de la procédure d'urgence « break the glass » était justifié, c'est-à-dire s'il y avait effectivement une interruption de la disponibilité au sein de la chaîne au moment de l'exécution de la prescription, y compris de la création de la relation thérapeutique.

16. Lors du démarrage du système de la pharmacie, le module logiciel de la pharmacie est authentifié au moyen d'un certificat système eHealth. Ce certificat authentifie la pharmacie et a un responsable (titulaire de l'officine) qui peut être lié à ce certificat au moyen de sources authentiques. Cette personne est notamment responsable de l'utilisation correcte du certificat et de la gestion de la clé privée, ainsi que des actions exécutées lors de l'utilisation de ce certificat.

17. La session peut être démarrée par chaque pharmacien qui travaille dans l'officine sous la responsabilité du titulaire. Afin de pouvoir démarrer une session, le pharmacien doit s'authentifier au moyen de la carte d'identité électronique (avec introduction du code PIN), soit - dans une première phase - au moyen du certificat d'encryptage personnel et de la clé privée y associée (qui fait office en occurrence de moyen d'authentification de l'identité du pharmacien), délivré par la plate-forme eHealth.

18. Sur base du numéro d'identification unique Recip-e de la prescription électronique, lue via le code-barre figurant sur la prescription imprimée que le patient délivre dans la pharmacie, le logiciel du pharmacien peut envoyer une demande chiffrée au système central de Recip-e afin d'obtenir la prescription électronique associée à ce numéro d'identification unique. La plate-forme eHealth valide si cette demande provient d'une pharmacie valide et agréée, après quoi le système Recip-e peut déchiffrer la demande et valider les droits d'accès sur base (1) du rôle précis de l'exécuteur de la prescription (transmis avec la demande) et (2) du type de prescription.

    L'exécuteur de la prescription vérifie en outre dans le traitement numérique de la prescription électronique si le patient est encore en vie ou décédé (via le système MyCareNet). Ce contrôle est effectué en dehors de Recip-e mais préalablement à la délivrance d'un produit. Le prescripteur de son côté vérifie également, lors de la création de la prescription, si le patient est encore en vie ou décédé (via son logiciel). Ce contrôle est également réalisé en dehors de Recip-e, mais préalablement à la prescription du produit à l'attention de la personne.

19. Lorsque la procédure d'autorisation s'est déroulée correctement, Recip-e renverra la prescription chiffrée à la pharmacie concernée. La clé pour déchiffrer la prescription chiffrée est ensuite demandée auprès du dépôt de clés de la plate-forme eHealth. Si le demandeur peut effectivement être autorisé à obtenir accès à la clé, la clé est envoyée au module logiciel de l'exécuteur, après quoi la prescription électronique pourra être déchiffrée à l'aide de la clé reçue.

20. Après avoir exécuté la prescription, l'exécuteur archive la prescription ainsi que la clé et l'enregistrement du temps effectué. Le système central Recip-e est ensuite averti par le logiciel de l'exécuteur que la prescription a été exécutée et archivée.

21. Une fonction est prévue sur le système central Recip-e afin de permettre au patient de consulter ses propres prescriptions médicales via des plateformes externes (p.ex. masanté.be). Lorsque le patient s'authentifie à l'aide de son eID ou d'un système équivalent approuvé, il peut consulter la liste des prescriptions pourvues de numéros d'identification uniques Recip-e. Le patient a la possibilité de gérer une prescription (révoquer, …) et d'appliquer des mesures de protection de la vie privée sur ses prescriptions (« VISI Flag ») de sorte que le pharmacien, lorsque le patient présente son eID / numéro NISS, puisse uniquement voir les prescriptions auxquelles le patient n'a pas appliqué ces mesures. Le patient peut lui-même activer le « VISI Flag » ou demander au prescripteur de l'activer avec son consentement. Le patient (ou le mandataire) peut également réserver une prescription auprès d'un pharmacien spécifique et fournir ses propres données de contact.

22. La validité des prescriptions est gérée par Recip-e: seules les prescriptions valides sont présentées au pharmacien. Il est par ailleurs prévu que les prescripteurs puissent consulter entre eux leurs prescriptions, moyennant l'existence d'une relation thérapeutique avec le patient et d'un consentement éclairé du patient accordé via le formulaire de consentement éclairé relatif à l'échange électronique de données à caractère personnel relatives à la santé, tel qu'approuvé par la section santé du Comité sectoriel de la sécurité sociale et de la santé[7]par la délibération n° 12/047 du 19 juin 2012.

23. Les prescriptions sont conservées sur le serveur Recip-e pendant maximum 1 an à compter de la création de la prescription. Toutefois, dès qu'une prescription (valide) est extraite par un prestataire de soins ou révoquée par le patient en question ou le prestataire de soins, la prescription en question est supprimée du serveur. Seules des métadonnées (sans le contenu de la prescription) sont conservées pour des raisons de logging.

24. L'infirmier pourra également consulter les prescriptions électroniques. Le patient a par ailleurs accès à ses propres prescriptions. Le mandataire (après octroi de ce rôle par la voie électronique par le patient) peut également obtenir accès aux prescriptions du patient, mais le patient a la possibilité de limiter certains accès.

ii. **PARIS**

25. Afin de permettre à chaque prescripteur de générer des prescriptions électroniques en dehors du dossier médical informatisé (dans l'attente de l'utilisation généralisée du DMI), les pouvoirs publics mettent gratuitement une application (web) à la disposition qui offre un service minimal: "PARIS" (Prescription & Autorisation Requesting Information System).

PARIS est mis à la disposition de prescripteurs occasionnels ou de prescripteurs qui se trouvent dans une situation où ils n'ont (temporairement) pas accès à leur logiciel de

[7] Actuellement la chambre sécurité sociale et santé du comité de sécurité de l'information.

gestion du dossier de patient ou au système informatique de l'hôpital, ou qui ne disposent pas (encore) d'un dossier médical informatisé (c'est-à-dire d'un logiciel de gestion du dossier de patient). PARIS offrira à ce groupe cible aussi la possibilité de générer des prescriptions électroniques en dehors du dossier médical informatisé (DMI).

L'application est donc utile pour les médecins généralistes, les spécialistes, les dentistes et les sages-femmes qui se trouvent dans une situation où ils n'ont (temporairement) pas accès à leur logiciel de gestion du dossier de patient ou au système informatique de l'hôpital, par exemple pendant les visites à domicile, les visites dans les centres de services de soins, pendant une consultation à l'hôpital, ou qui ne disposent pas (encore) d'un dossier médical informatisé, à savoir d'un logiciel de gestion du dossier de patient, ou qui n'en ont pas besoin. Il s'agit par exemple de certaines catégories de spécialistes, de prescripteurs qui n'ont plus qu'une pratique limitée ou qui n'exercent plus la profession au sens classique du terme (qui sont actifs auprès des mutualités, dans l'administration, dans l'enseignement, les biologistes cliniques, les anatomopathologistes, etc.) et de prescripteurs âgés à la fin d'une pratique active.

26. Le prescripteur peut utiliser les fonctionnalités suivantes du système Recip-e:
- créer une prescription;
- consulter la liste des prescriptions générées par le prescripteur qui n'ont pas encore été délivrées;
- annuler une prescription qui n'a pas encore été délivrée;
- envoyer une notification au pharmacien individuel;
- consulter le feedback de pharmaciens concernant les prescriptions à délivrer.

27. PARIS n'offre pas de service minimal pour les demandes d'autorisation électroniques de médicaments pour lesquelles l'application CIVARS est déjà opérationnelle.

II. COMPÉTENCE DU COMITÉ

28. L'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* dispose que toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information, sauf dans quelques cas exceptionnels.

29. Par ailleurs, en vertu de l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est en principe compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé, sauf les exceptions prévues.

30. L'article 46, § 2, alinéa 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* dispose en outre que la chambre sécurité sociale et santé du Comité de sécurité de l'information est chargée de veiller au respect 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. À

cet effet, elle peut formuler toutes recommandations qu'elle juge utiles et aider à la solution de tout problème de principe ou de tout litige.

31. Le Comité constate par ailleurs que le demandeur prévoit, lors de la communication de la prescription électronique ambulatoire, l'utilisation du NISS du prescripteur et du patient, ce qui implique l'utilisation du numéro de registre national ou du numéro d'identification attribué par la Banque Carrefour de la sécurité sociale.

En vertu de l'article 15, § 3, de la loi précitée du 15 janvier 1990, la chambre sécurité sociale et santé du Comité de sécurité de l'information peut, dans la mesure où elle doit rendre une délibération pour une communication de données à caractère personnel, éventuellement rendre également une délibération pour l'utilisation du numéro de registre national par les instances concernées si cela est nécessaire dans le cadre de la communication envisagée.

Conformément à l'article 5, § 1er, de la loi du 5 mai 2014 *garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier*, le Comité peut également se prononcer sur l'utilisation du numéro du registre national chaque fois qu'une décision est prise à propos d'un flux de données à caractère personnel ou d'un traitement de données à caractère personnel.

Pour autant que le numéro d'identification de la sécurité sociale ait été attribué par la Banque Carrefour de la sécurité sociale, son utilisation est libre en vertu de l'article 8, § 2, de la loi précitée du 15 janvier 1990.

32. L'article 42 de la loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé fixe les critères auxquels doit répondre une prescription valable. Il est notamment stipulé que la prescription doit être datée sur papier ou de manière électronique au moyen d'une procédure approuvée par le Comité sectoriel de la sécurité sociale et de la santé. Par ailleurs, la prescription doit être signée ou bien l'identité du prescripteur doit être authentifiée au moyen d'une procédure approuvée par le Comité sectoriel de la sécurité sociale et de la santé[8]. Le Comité doit dès lors se prononcer sur la procédure permettant de dater la prescription de manière électronique et sur la procédure d'authentification de l'identité du prescripteur.

33. Le Comité estime qu'il est compétent pour se prononcer sur le traitement de données à caractère personnel dans le cadre du projet Recip-e de l'application web PARIS.

III. EXAMEN DE FOND

A. ADMISSIBILITÉ

[8] Actuellement la chambre sécurité sociale et santé du Comité de sécurité de l'information.

34. Le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes et le traitement de données à caractère personnel relatives à la santé est en principe interdit.[9]

35. L'interdiction n'est pas d'application lorsque le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3[10].

36. Le Comité constate que la communication des prescriptions électroniques cryptées par le prescripteur au système central de Recip-e répond aux conditions de l'exception à l'interdiction précitée prévue à l'article 9, alinéa 2, h) du RGPD.

B. FINALITÉ

37. Conformément à l'article 5, b), du RGPD, le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.

38. Grâce au traitement de données à caractère personnel visé dans le cadre des projets Recip-e et PARIS, l'INAMI souhaite permettre l'utilisation de la prescription électronique ambulatoire, telle que décrite aux points 1, 2, 3, 25 et 26. L'INAMI, en tant qu'institution publique de sécurité sociale, a pour mission légale d'organiser, de gérer et de contrôler l' « assurance obligatoire »[11]. Ceci implique notamment qu'il élabore les règles pour le remboursement de prestations de santé et de médicaments et qu'il en détermine les tarifs. Plus spécifiquement, il entre dans les compétences du service des soins de santé de fixer les conditions selon lesquelles les prestations de santé peuvent être remboursées.

39. Le Comité estime qu'il est effectivement légitime dans le chef de l'INAMI et de l'asbl Recip-e de développer l'infrastructure requise pour l'utilisation de la prescription électronique ambulatoire et constate à cet égard que le traitement visé poursuit des finalités déterminées et explicites.

C. PRINCIPE DE PROPORTIONNALITÉ

40. Conformément à l'article 5, b) et c), les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

---

[9] Art. 9, alinéa 1er du RGPD.
[10] Art. 9, alinéa 2, h) du RGPD.
[11] Loi du 14 juillet 1994 *relative à l'assurance obligatoire soins de santé et indemnités*, coordonnée le 14 juillet 1994, *M.B.* 27 août 1994.

41. Les données à caractère personnel suivantes seront traitées lors de la communication de la prescription électronique ambulatoire : d'une part, la prescription électronique ambulatoire en tant que telle, contenant le nom et le prénom du patient, les coordinats du prescripteur et les informations concernant les prestations ou les médications prescrites, et, d'autre part, la partie administrative qui contient le NISS du patient ainsi que le NISS ou le numéro INAMI du prescripteur.

42. La prescription électronique est chiffrée à l'aide du service de base de cryptage pour un destinataire inconnu de la plate-forme eHealth. Ceci signifie que dès que la prescription électronique est créée, le message est chiffré de sorte qu'uniquement un nombre très restreint de personnes puissent la déchiffrer et puissent lire la prescription, à savoir le prescripteur même, les autres prescripteurs, l'intéressé au nom duquel la prescription a été créée, le mandataire et le prestataire de soins auquel l'intéressé a demandé d'exécuter ou de consulter la prescription. Le système central de Recip-e qui conserve les prescriptions chiffrées après qu'elles ont été correctement créées, ne peut dès lors, d'aucune façon, prendre connaissance du contenu de la prescription.

43. Étant donné que l'identification univoque du patient et du prescripteur est primordiale, il est prévu que dans la partie administrative qui accompagne la prescription chiffrée, le patient est identifié à l'aide de son NISS et le prescripteur est identifié à l'aide de son NISS ou de son numéro INAMI.

44. Le demandeur souligne que l'utilisation des numéros d'identification précédents est nécessaire, d'une part, pour permettre aux patients de consulter les prescriptions prescrites à leur nom dans le système central de Recip-e et de les annuler, et d'autre part, pour exécuter correctement les loggings de sécurité requis.

45. De manière générale, le Comité estime qu'il est en effet indiqué d'utiliser des numéros d'identification uniques tels que le NISS afin d'identifier le patient et le prescripteur dans la partie administrative lors de la communication de tels messages chiffrés. Le Comité constate que bien que des données à caractère personnel relatives à la santé puissent être déduites de la combinaison entre les numéros d'identification du patient et du prescripteur, ce traitement de données à caractère personnel est également nécessaire pour pouvoir satisfaire à plusieurs obligations spécifiques. Ainsi, le traitement de ces numéros d'identification est nécessaire en vue de l'exécution obligatoire de loggings de sécurité, de l'envoi des messages aux destinataires corrects (routage) et du développement pratique de certains droits des intéressés prévus par la loi, tels que le droit de consultation. Ce traitement de données à caractère personnel requiert toutefois que les mesures de sécurité, telles que décrites ci-après, offrent une garantie que les données en question seront traitées avec la plus grande confidentialité. Par ailleurs, le traitement des numéros d'identification n'est autorisé que pour les finalités précitées, à savoir la gestion de loggings de sécurité, le routage et l'organisation des droits des intéressés prévus par la loi, tels que le droit de consultation.

46. Le Comité estime que les données à caractère personnel qui seront traitées dans le cadre du projet Recip-e et du projet PARIS sont pertinentes, proportionnelles et non excessives.

47. Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

48. Les prescriptions chiffrées sont conservées pendant maximum un an dans le système central de Recip-e dans la mesure où elles ne sont pas demandées par un prestataire de soins (et sont toujours valides) ou qu'elles n'ont pas été révoquées par le patient concerné ou le prestataire de soins.

49. Il est prévu que les prescriptions électroniques sont, après qu'elles ont été délivrées à l'exécuteur, conservées par ce dernier conformément aux dispositions légales. Après qu'une prescription électronique a été demandée et exécutée, la prescription électronique chiffrée sauvegardée dans le système central de Recip-e est supprimée. Les loggings de sécurité sont conservés par le système central de Recip-e pendant une période de 30 ans.

50. Si le système central de Recip-e est utilisé pour envoyer un message chiffré (feedback) entre l'exécuteur de la prescription et le prescripteur, il est prévu que le message chiffré n'est conservé que jusqu'au moment où un prescripteur ouvre une session et où le message peut être délivré. Dès qu'ils sont délivrés, les messages de feedback sont supprimés immédiatement et définitivement du système central de Recip-e.

51. Vu ce qui précède, le Comité estime que les délais de conservation prévus sont acceptables.

C. PROTECTION ET CONFIDENTIALITÉ

52. Conformément à l'article 9, alinéa 3, du RGPD, les données à caractère personnel relatives à la santé peuvent uniquement être traitées sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si ce n'est pas strictement requis, le Comité sectoriel estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin[12], ce qui est le cas en l'espèce.

53. Conformément à l'article 5, f), du RGPD, le demandeur doit prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

54. Conformément aux mesures de référence en matière de protection de tout traitement de données à caractère personnel telles qu'elles ont été établies par la Commission de la protection de la vie privée, tout responsable du traitement doit, en fonction de la nature et de l'ampleur du traitement, dans le cadre de cette obligation, prendre des mesures spécifiques, plus précisément rédiger un plan de sécurité, désigner un conseiller en sécurité,

[12] Le Comité a formulé cette préférence dans le paragraphe 61 de la délibération n° 07/034 du 4 septembre 2007 relative à la communication de données à caractère personnel au Centre fédéral d'expertise des soins de santé en vue de l'étude 2007-16-HSR « étude des mécanismes de financement possibles pour l'hôpital de jour gériatrique », www.privacycommission.be.

garantir la protection physique des données à caractère personnel et la protection des réseaux, prévoir une gestion adéquate des utilisateurs et des accès, mettre en place des mécanismes de journalisation et de traçage, valider et vérifier régulièrement les mesures de sécurité techniques ou organisationnelles, posséder un plan de gestion des incidents de sécurité et disposer d'une documentation complète, centralisée et mise à jour[13].

55. Il est prévu en l'espèce que le service de base de gestion des accès et des utilisateurs de la plate-forme eHealth est utilisé pour l'authentification et l'autorisation des différents utilisateurs du projet Recip-e et du projet PARIS, plus précisément le prescripteur, l'exécuteur et l'intéressé même. Le traitement de données à caractère personnel par la plate-forme eHealth dans le cadre de la gestion des utilisateurs et des accès a déjà fait l'objet d'une autorisation du Comité[14]. Dans le cas de prescriptions ambulatoires créées dans un hôpital, l'hôpital réalise un logging univoque de l'identité du médecin qui a rédigé une prescription ambulatoire spécifique.

56. Compte tenu de l'article 42 de la loi coordonnée du 10 mai 2015, le Comité approuve explicitement les méthodes d'authentification prévues, ainsi que l'utilisation du service de base « timestamping » de la Plate-forme eHealth pour la datation des prescriptions électroniques ambulatoires.

57. Pour le chiffrement de la prescription électronique en vue de la communication entre le prescripteur et l'exécuteur, d'une part, et le chiffrement du message chiffré et des informations administratives en vue de la communication entre le prescripteur et le système central de Recip-e, d'autre part, il sera fait usage du service de base de cryptage pour un destinataire inconnu de la plate-forme eHealth. Le chiffrement d'éventuels messages de feedback sera effectué à l'aide d'un système de cryptage pour un destinataire connu.

58. Le projet Recip-e et le projet PARIS prévoient aussi l'exécution des loggings de sécurité requis, également en utilisant les services de base de la plate-forme eHealth. Dans ces loggings, les données suivantes sont conservées : quelle action a été réalisée (communication de la personne qui a réalisé l'action (à l'aide du NISS), relative à quelle personne (aussi à l'aide du NISS) et quand l'action a-t-elle été réalisée.

59. Finalement, le Comité prend acte du fait qu'un conseiller en sécurité individuel a été désigné pour les deux projets. Le Comité a pu prendre connaissance de leur identité.

[13] http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf
[14] Délibération du Comité sectoriel de la sécurité sociale et de la santé n° 09/008 du 20 janvier 2009, modifiée le 16 mars 2010 et le 15 juin 2010 relative à l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth lors de l'échange de données à caractère personnel, www.privacycommission.be.

Par ces motifs,

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

conclut que la communication des données à caractère personnel, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection des données qui ont été définies en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la conservation et de sécurité de l'information.

autorise le traitement de données à caractère personnel pour l'échange électronique de la prescription ambulatoire électronique dans le cadre du projet Recip-e et de l'application web PARIS ainsi que l'utilisation du numéro national pour ces finalités.

Compte tenu de l'article 42 de la loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé, le Comité approuve explicitement les méthodes d'authentification prévues, ainsi que l'utilisation du service de base « timestamping » de la Plate-forme eHealth pour la datation des prescriptions électroniques ambulatoires.

Bart VIAENE
Président