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

CSI/CSSS/19/278

DÉLIBÉRATION N° 19/152 DU 3 SEPTEMBRE 2019 RELATIVE À L'UTILISATION DE MOYENS D'IDENTIFICATION ÉLECTRONIQUE OFFERTS PAR DES ORGANISATIONS PRIVÉES DANS LE CADRE DU SERVICE DE BASE 'GESTION INTÉGRÉE DES UTILISATEURS ET DES ACCÈS' DE LA PLATE-FORME EHEALTH EN COLLABORATION AVEC LE SERVICE D'AUTHENTIFICATION FÉDÉRAL DU SPF BOSA

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 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 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*;

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

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

Vu le rapport de monsieur Bart Viaene;

Émet, après délibération, la décision suivante, le 3 septembre 2019:

I. OBJET

1. Conformément à ses missions légales, la Plate-forme eHealth offre plusieurs services de base, dont le service 'Gestion intégrée des utilisateurs et des accès'.

2. Le service 'Gestion intégrée des utilisateurs et des accès' de la Plate-forme eHealth a pour objet de faciliter l'identification, l'authentification, la vérification de qualités et de relations et la gestion d'autorisations d'acteurs des soins de santé.

3. Ce service se compose de différents composants qui collaborent afin de permettre l'identification (unique), l'authentification et la vérification de qualités et de relations, et le partage des résultats des contrôles réalisés, toutes applications en matière d'eSanté confondues. Les utilisateurs des soins de santé qui demandent un accès aux services (hébergés auprès des instances des soins de santé et de la Plate-forme eHealth) disposent donc d'un single sign on.

4. Ces composants sont conformes aux normes internationales pour les communications entre organisations afin de garantir la sécurité et la stabilité et de simplifier l'intégration.

5. Pour autant qu'il soit satisfait aux conditions décrites dans la présente délibération, la Plate-forme eHealth souhaite autoriser l'utilisation de moyens d'identification électronique offerts par des organisations privées lorsque ceux-ci sont offerts en collaboration avec le Service d'authentification fédéral (« FAS »), en vue de l'accès aux applications offertes dans le secteur de la santé. Le FAS est un service offert par le Service public fédéral Stratégie et Appui, DG Transformation digitale (ci-après « SPF BOSA »), qui offre différents moyens d'identification électronique pour l'authentification des citoyens en vue de l'accès aux applications des services publics.

6. Au sein de la collaboration, il est fait appel au FAS pour le mécanisme d'authentification qui permet à une personne d'utiliser le moyen d'identification électronique pour confirmer son identité vis-à-vis d'une partie de confiance.

II. EXAMEN

7. L'organisation qui offre un moyen d'identification électronique peut offrir son moyen d'identification dans le secteur de la santé en vue de l'accès de patients à leur dossier médical à condition qu'elle satisfasse aux conditions suivantes:

8. Cette authentification intervient par un système d'authentification propre à l'organisation
- à condition que le moyen d'authentification propre à l'organisation satisfasse aux conditions d'un niveau de garantie « substantiel », tel que précisé dans les points 2.1., 2.2.1 élément 2, 2.2.3., 2.2.4., 2.3.1. (à l'exception de l'élément 1) de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et
- à condition que le moyen d'authentification utilisé dans le système d'authentification propre à l'organisation et que son processus d'activation satisfassent aux conditions d'un niveau de garantie « faible », tel que précisé dans les points 2.2.1. élément 1, et 2.2.2.de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et qu'il ait été conçu de la sorte que l'on peut présumer qu'il ne sera utilisé que par la personne à laquelle il appartient.

9. L'organisation dispose de méthodes documentées et d'une politique de gestion de la sécurité de l'information, d'approches de gestion des risques et d'autres méthodes de contrôle reconnues de sorte qu'elle puisse offrir les garanties utiles pour le moyen d'authentification électronique.

10. L'organisation dispose d'un plan de cessation d'activités efficace. Ce plan comporte des mesures concernant le transfert de la prestation de service à la Plate-forme eHealth ou à une autre autorité désignée par la Plate-forme eHealth.

11. L'organisation qui offre le moyen d'identification électronique ne pourra, en aucune hypothèse et concernant aucun aspect de l'utilisation du moyen d'identification électronique, facturer des frais à la Plate-forme eHealth ou au SPF BOSA.

12. L'organisation satisfait aux exigences en matière de protection des données à caractère personnel.

L'organisation qui offre le moyen d'identification électronique traite des données à caractère personnel et intervient à cet égard comme responsable du traitement tel que défini dans le Règlement général relatif à la protection des données 2016/679 pour tous les traitements de données à caractère personnel liés à la prestation de service qu'elle fournit et respecte toutes les obligations pertinentes.

En cette qualité, elle doit prendre les mesures techniques et organisationnelles appropriées qui sont nécessaires à la protection des données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent être conformes à l'état de la technique au niveau de la sécurité.

L'organisation désigne un délégué à la protection des données.

L'organisation ne prend pas connaissance des applications auxquelles l'utilisateur demande un accès au moyen du moyen d'identification électronique.

L'organisation installe une piste de vérification sécurisée (*audit trail*) de sorte que les données, par transaction spécifique, puissent être reconstituées en vue de la protection des données et de la protection de la vie privée. L'organisation conserve, à cet effet, pour toute connexion et tentative de connexion les informations suivantes pendant un délai de dix ans à compter du moment de la connexion ou de la tentative de connexion en question:

1. le numéro d'identification unique de l'utilisateur;

2. le service d'identification électronique de l'organisation avec lequel l'utilisateur se connecte ou essaie de se connecter; et

3. la date et l'heure de la connexion ou de la tentative de connexion.

13. L'organisation satisfait aux exigences suivantes en ce qui concerne l'échange d'informations avec le FAS.

L'organisation du moyen d'identification électronique envoie au FAS, lors de toute connexion, le numéro d'identification de la sécurité sociale (NISS) de l'utilisateur sur la base duquel le FAS constate l'identité de l'utilisateur.

L’échange d’informations entre l’organisation et le FAS intervient conformément aux protocoles techniques tels que précisés dans les spécifications techniques.

Lors de tout échange d’informations entre le FAS et l’organisation et entre l’organisation et l’utilisateur, le service d’identification électronique réalise des contrôles afin d’au moins prévenir les abus suivants:

1. Un nouvel envoi d’un même message ou d’une même tentative de connexion;

2. Une modification du contenu des informations échangées; et

3. Une tierce partie qui se présente comme l’organisation offrant le moyen.

Ces abus sont détectés et donnent lieu à l’échec de la connexion.

L’organisation qui offre le moyen d’identification électronique prévoit suffisamment de mécanismes de contrôle afin de détecter, de manière proactive, des risques de sécurité éventuels.

14. L'organisation satisfait aux conditions suivantes en ce qui concerne la gestion de la prestation de service.

La prestation de service est disponible, sur base mensuelle, pendant 99,9 % du temps.

Lors de la connexion d’un utilisateur, le temps de réaction n’est pas supérieur à:

1 seconde pour 95 % des connexions;

2 secondes pour 98 % des connexions; et

5 secondes pour 99,5 % des connexions.

L’organisation introduit des mécanismes permettant de garantir la continuité de la prestation de service jusqu’à la fin de la collaboration.

15. L’organisation offre des services d’appui, se charge de traiter les plaintes, de réaliser des enquêtes de sécurité, gère les problèmes et incidents relatifs au moyen et assure la communication relative au moyen à l’utilisateur.

16. Le SPF BOSA et la Plate-forme eHealth ne peuvent en aucun cas être tenus pour responsables des dommages qui résultent directement du non-respect par l’organisation des spécifications techniques et des procédures liées au moyen d’identification électronique telles que décrites dans l’annexe du Règlement d'exécution (UE) n° 2015/1502:

- demande et enregistrement,
- preuve et vérification de l’identité de la personne concernée,
- conception et fonctionnement du moyen d’identification électronique,
- délivrance, mise à disposition et activation du moyen d’identification électronique,
- suspension, révocation et réactivation du moyen d’identification électronique,
- renouvellement et remplacement du moyen d’identification électronique,
- mécanisme d’authentification.

17. Chaque utilisateur final est responsable de la préservation, de la sécurité, de la confidentialité et de la gestion appropriées de ses codes numériques et des données qui y sont associées. L'utilisateur final est responsable du choix d'un code secret sécurisé.

18. Conformément à l'article 5 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 est compétent pour autoriser l'utilisation 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. Le Comité constate que le moyen d'identification électronique, à condition que l'organisation satisfasse aux conditions de la présente délibération, sera disponible via le service de base 'gestion intégrée des utilisateurs et des accès' de la Plate-forme eHealth. L'article 8 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions* dispose que lors de la communication de données à caractère personnel non pseudonymisées à ou par la Plate-forme eHealth, seuls les numéros d'identification visés à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (soit le numéro de registre national, soit le numéro d'identification de la Banque Carrefour de la sécurité sociale) sont utilisés. Le Comité autorise dès lors l'organisation offrant le moyen d'identification électronique qui satisfait aux conditions de la présente délibération, à utiliser le numéro de registre national de l'intéressé identifié avec le moyen.

19. L'utilisation du moyen d'identification électronique doit être inscrite dans le 'Règlement à l'usage des utilisateurs en vue de l'accès et de l'utilisation du système informatique de l'Etat fédéral et des institutions publiques de sécurité sociale par les citoyens et leurs mandataires' après approbation par le Comité de gestion de la Banque Carrefour de la sécurité sociale, en exécution de l'article 3, § 2, 1°, et § 4, de la loi du 24 février 2003 *concernant la modernisation de la gestion de la sécurité sociale et concernant la communication électronique entre des entreprises et l'autorité fédérale* et l'arrêté royal du 21 novembre 2006 *portant extension de l'application de l'article 3 de la loi du 24 février 2003 concernant la modernisation de la gestion de la sécurité sociale et concernant la communication électronique entre des entreprises et l'autorité fédérale aux citoyen*.

20. Grâce à cette collaboration, le *single sign on* sera possible entre les connexions basées sur ces moyens d'identification électronique et les connexions au sein du FAS du même niveau pour les applications dans le secteur de la santé.

21. Avant que le SPF BOSA ne puisse mettre l'usage du moyen électronique en production via le FAS, l'organisation qui offre le moyen d'identification électronique doit prouver à la Plate-forme eHealth qu'elle satisfait aux conditions fixées dans la présente délibération. La Plate-forme eHealth détermine, de manière autonome, le mode de vérification quant à la conformité aux conditions reprises dans la présente délibération.

22. Conformément aux modalités définies par le SPF BOSA, une concertation est organisée entre l'organisation offrant le moyen d'identification électronique et le SPF BOSA (service

meetings) au cours de laquelle tous les aspects possibles de l'utilisation du moyen d'identification électronique et la collaboration avec le FAS sont examinés.

23. En cas d'incidents majeurs, l'organisation offrant le moyen d'identification électronique est tenue de les signaler, dans les meilleurs délais et au plus tard dans les 72 heures après l'incident, à la Plate-forme eHealth et en copie au SPF BOSA et de transmettre un rapport détaillé relatif aux incidents, à leur impact et au suivi de ces incidents, en ce compris un avis circonstancié du délégué à la protection des données de l'organisation offrant le moyen d'identification électronique concernant ces incidents.

24. Lorsque le SPF BOSA constate que l'organisation qui offre le moyen électronique ne satisfait plus aux conditions prévues dans la présente délibération, il peut demander des explications détaillées et imposer, si nécessaire, un contrôle.

25. Si le SPF BOSA constate que l'organisation qui offre le moyen électronique ne respecte pas les conditions de la présente délibération, il peut mettre fin, de manière unilatérale et sans préavis, à la collaboration entre l'organisation offrant le moyen d'identification électronique et le FAS.

Par ces motifs,

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

conclut que la Plate-forme eHealth peut autoriser l'utilisation de moyens d'identification électronique offerts par des organisations privées lorsque ceux-ci sont offerts en vue de l'accès à des applications au sein du secteur de la santé, en collaboration avec le Service d'authentification fédéral (« FAS ») du SPF BOSA, pour autant qu'il soit satisfait aux conditions décrites dans la présente délibération.

L'organisation offrant un moyen d'identification électronique qui satisfait aux conditions de la présente délibération, est autorisée à utiliser le numéro de registre national de l'intéressé identifié par ce moyen.

Bart VIAENE