Comité sectoriel de la sécurité sociale et de la santé
Section "Santé"

CSSSS/17/047

DÉLIBÉRATION N° 17/023 DU 21 MARS 2017 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LA PLATE-FORME EHEALTH OU À LA PLATE-FORME EHEALTH, DANS LE CADRE DU SERVICE DE BASE "LOGS DE SÉCURITÉ"

La section santé du Comité sectoriel de la sécurité sociale et de la santé (dénommée ci-après « le Comité sectoriel »);

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment l'article 37;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;*

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 du 14 mars 2017;

Vu le rapport de monsieur Yves Roger.

Émet, après délibération, la décision suivante, le 21 mars 2016:

I. OBJET

1. La Plate-forme eHealth a développé une application web pour la consultation des données des logs de sécurité. La solution permettra aux conseillers en sécurité de consulter les logs de sécurité générés par la Plate-forme eHealth via une application web sécurisée et ce en temps réel.

2. Les trois principales fonctionnalités de cette application sont les suivantes:

- la recherche de logs sur la base de critères et l'affichage des résultats dans un tableau;
- l'affichage de statistiques (nombre de logs générés par mois et par institution/application);
- l'exportation des résultats de la recherche dans un format standard.

3. L'application sera mise à la disposition des utilisateurs suivants:

- Le *Host Security Responsible:* ce rôle est attribué aux responsables en sécurité de l'organisation (entreprise belge) qui héberge les applications pour le compte d'une plateforme ou d'une organisation. Ces derniers ont accès uniquement dans l'environnement d'acceptation[1] à l'ensemble des logs de sécurité des applications qui sont hébergées chez eux afin de pouvoir valider la prise de logs correcte. Ils n'ont pas accès aux logs de sécurité dans l'environnement de production.
- Le *Platform Security Responsible:* ce rôle est attribué aux responsables en sécurité de la plateforme dont les applications dépendent (institution fédérale ou régionale). Ces derniers ont accès à l'ensemble des logs de sécurité des applications qui sont hébergées sur leur plateforme ou qui en dépendent dans l'environnement de production.
- Le *Organization Treatment Security Responsible*: ce rôle est attribué aux responsables en sécurité d'une application pour une organisation. Ces derniers ont uniquement accès aux logs de sécurité générés pour les applications pour lesquelles ils assument la responsabilité de traitement dans l'environnement de production.

4. Les flux de données générés dans le cadre du service Logs de sécurité sont les suivants:

- Les actions effectuées par les utilisateurs d'applications sont loggées sur les serveurs applicatifs, en particulier qui a fait quoi, à propos de qui, quand et comment.
- Ces données sont ensuite transférées sur le DBMS (database management system) où elles sont indexées et converties dans un format qui permet de faire des recherches.
- Lorsqu'un utilisateur consulte des logs de sécurité depuis l'application web, les données sont récupérées grâce au moteur de recherche du DBMS et filtrées selon son profil utilisateur. Conformément à l'article 46, § 2, alinéa 2, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, la section Santé du Comité sectoriel est notamment 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.

[1] Une application informatique est développée dans l'*environnement de développement*, un système qui fonctionne de manière tout à fait autonome et qui n'interagit pas avec d'autres systèmes (les développeurs sont les seuls à utiliser l'environnement de développement). Dès que les développeurs ont terminé leur tâche, l'application informatique est copiée dans l'*environnement de test*. Dans cet environnement, il sera vérifié si l'application satisfait aux besoins (l'interaction avec d'autres systèmes est aussi testée à cette occasion). L'application informatique est ensuite transférée vers l'environnement d'acceptation. Il s'agit de l'environnement auquel le demandeur a accès pour accepter l'application informatique (c'est-à-dire vérifier que l'application fonctionne comme elle doit) et qui utilise des données à caractère personnel fictives. Si le demandeur approuve l'application informatique, elle est finalement copiée dans l'*environnement de production* où elle peut être utilisée par tous les utilisateurs avec des données à caractère personnel réelles.

II. COMPÉTENCE

5. Etant donné que les logs contiennent des données à caractère personnel relatives aux utilisateurs et aux personnes concernant lesquelles des actions sont effectuées, leur communication par la Plate-forme eHealth ou à la Plate-forme eHealth requiert, en vertu de l'article 11, alinéa premier, de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la Plate-forme eHealth et portant diverses dispositions*, une autorisation de principe de la section Santé du Comité sectoriel de la sécurité sociale et de la santé.

6. Dans la mesure où les logs contiennent des données à caractère personnel relatives à la santé, leur communication doit, conformément à l'article 42, § 2, 3 °, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé* aussi faire l'objet d'une autorisation de la section Santé du Comité sectoriel de la sécurité sociale et de la santé.

III. EXAMEN

7. La communication des données à caractère personnel par la Plate-forme eHealth aux différentes catégories de responsables en sécurité poursuit une finalité légitime, à savoir permettre la consultation des logs relatifs à l'utilisation des applications pour lesquelles ils sont responsables.

8. Les données à caractère personnel communiquées sont adéquates, pertinentes et non excessives par rapport à cette finalité. Elles se limitent aux informations indiquant quelle personne a effectué quelle action, concernant quelle personne, à quel moment et de quelle manière. A cet égard, les personnes physiques sont identifiées par le numéro d'identification de la sécurité sociale. Les organismes et les personnes morales sont identifiés au moyen du numéro d'identification (BCE, numéro INAMI, etc.) utilisé le cas échéant.

9. Le Comité sectoriel constate que certains logs de sécurité peuvent, suite à l'identité des établissements ou prestataire de soins concernés (p.ex. hôpitaux psychiatriques, certains médecins-spécialistes), également contenir des données relatives à la santé. Le Comité sectoriel déclare que le fait de prévoir des logs de sécurité constitue un élément essentiel des mesures techniques et organisationnelles requises par la loi relative à la vie privée en vue de la protection des données à caractère personnel (art. 16, § 4, de la loi relative à la vie privée), de sorte que la communication de données à caractère personnel ayant potentiellement un caractère de santé dans le cadre de la création de logs de sécurité doit être considérée comme adéquate, pertinente et non excessive.

10. Trois rôles sont créés pour les utilisateurs du service 'Logs de sécurité', en particulier le *Host Security Responsible*, le *Platform Security Responsible* et le *Organization Treatment Security Responsible*, qui disposent chacun de droits d'accès spécifiques comme précisé ci-dessus. L'exemple suivant permet de préciser leurs compétences spécifiques.

11. L'application SACEx de l'AFMPS permet aux producteurs belges de dispositifs médicaux tels les implants de demander des certificats d'exportation. Cette application génère des logs de sécurité suite à l'utilisation du NISS. Cette application est accessible via la Plate-forme

eHealth et est hébergée par l'asbl Smals. Des logs de sécurité sont générés dans les cas suivants:

- Un utilisateur d'une entreprise belge a accès aux données du représentant légal (NISS, nom, prénom, date de naissance).
- Un collaborateur de l'INAMI consulte les données du représentant légal d'une entreprise (NISS, nom, prénom, date de naissance) dans le cadre de la consultation du détail des données de l'entreprise.
- Un collaborateur de l'AFMPS consulte les données des représentants légaux d'une entreprise (NISS, nom, prénom, date de naissance) dans le cadre de la consultation du détail des données de l'entreprise.

12. Dans ce cadre, les rôles sont attribués comme suit:

- Le *Host Security Responsible* est le responsable en sécurité de la Smals. Ce dernier a accès aux logs de sécurité dans l'environnement d'acceptation afin de valider la prise de logs correcte par l'application. Il n'a pas accès aux logs de sécurité dans l'environnement de production.
- Le *Platform Security Responsible* est le responsable en sécurité de la Plate-forme eHealth. Ce dernier a accès à l'ensemble des logs de sécurité de la plate-forme dans l'environnement de production, dont ceux pris par l'application afin de pouvoir répondre à une demande d'un citoyen par exemple.
- Le *Organization Treatment Security Responsible* est le responsable en sécurité de l'AFMPS. Ce dernier a dans l'environnement de production uniquement accès aux logs de sécurité générés par l'application pour laquelle l'AFMPS a la responsabilité de traitement. Dans le cadre de l'application SACEx, il a par conséquent accès aux logs de sécurité générés par un utilisateur d'une entreprise, par un collaborateur de l'INAMI ou par sa propre organisation (l'AFMPS).

13. L'application est sécurisée au moyen de l'application de connexion de la Plate-forme eHealth, ce qui implique que l'accès des utilisateurs est configuré dans la gestion des accès (User Management) par un responsable accès entreprises ou un gestionnaire local de l'entreprise. Les utilisateurs mêmes sont identifiés et authentifiés au moyen de leur carte d'identité électronique.

Par ces motifs,

la section santé du Comité sectoriel de la sécurité sociale et de la santé,

autorise, conformément aux dispositions de la présente délibération, la communication de données à caractère personnel par la Plate-forme eHealth ou à la Plate-forme eHealth, dans le cadre du service de base "logs de sécurité".

Yves ROGER
Président