Comité sectoriel du Registre national

Délibération RN n° 25/2017 du 17 mai 2017

Objet : demande formulée par la Vlaams Agentschap Zorg en Gezondheid (Agence flamande Soins et Santé), l'asbl FRATEM (InterMed - Réseau Santé Wallon) et l'asbl ABRUMET (BruSafe - Réseau Santé Bruxellois) afin d'accéder à certaines données du Registre national pour l'organisation de l'enregistrement et de la consultation de données relatives à la santé dans les coffres-forts de première ligne (RN-MA-2017-067)

Le Comité sectoriel du Registre national (ci-après le "Comité") ;

Vu la loi du 8 août 1983 *organisant un Registre national des personnes physiques* (ci-après la "LRN") ;

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* (ci-après la "LVP"), en particulier l'article 31*bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée* ;

Vu la demande de la Vlaams Agentschap Zorg en Gezondheid (Agence flamande Soins et Santé), de l'asbl FRATEM (InterMed - Réseau Santé Wallon) et de l'asbl ABRUMET (BruSafe - Réseau Santé Bruxellois), reçue le 23/03/2017 ainsi que les informations complémentaires ;

Vu la demande d'avis technique et juridique adressée au Service public fédéral Intérieur en date du 19/04/2017 ;

Vu le rapport de la Présidente ;

Émet, après délibération, la décision suivante, le 17 mai 2017 :

I. OBJET DE LA DEMANDE

1. En Belgique, il y a trois coffres-forts de première ligne : Vitalink (gérée par l'Agence flamande Soins et Santé), InterMed qui est relié au hub 'Réseau Santé Wallon' (ci-après RSW) (exploité par l'asbl FRATEM) et BruSafe qui est relié au hub 'Réseau Santé Bruxellois' (exploité par l'asbl ABRUMET).

2. La présente demande vise à ce que l'Agence flamande Soins et Santé, l'asbl FRATEM et l'asbl ABRUMET, ci-après les demandeurs, soient autorisés à accéder à certaines données du Registre national pour l'organisation de l'enregistrement et de la consultation de données relatives à la santé dans les coffres-forts de première ligne. Vitalink et les hubs auxquels un autre coffre-fort de première ligne est relié (Réseau Santé Wallon pour Intermed et Réseau Santé Bruxellois pour BruSafe) doivent plus précisément avoir accès à la donnée "région de la résidence principale d'un usager de soins"[1] afin d'établir ainsi quel coffre-fort met les informations à disposition, et à la donnée "date du décès d'un usager de soins" afin de pouvoir ainsi déterminer le moment pour détruire les données à caractère personnel.

II. EXAMEN DE LA DEMANDE

3. Tant l'Agence flamande Soins et Santé que l'asbl FRATEM ont déjà été explicitement autorisées par le Comité à utiliser le numéro de Registre national (respectivement via les délibérations RN n° 70/2013 du 9 octobre 2013 et RN n° 50/2009 du 15 juillet 2009). En tant que responsable du coffre-fort BruSafe (plus récemment créé), l'asbl ABRUMET ne dispose pas, en son nom propre, d'une autorisation explicite du Comité. 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* constitue le fondement légal pour l'utilisation du numéro de Registre national par les utilisateurs des services qui ont recours aux services de base de la plate-forme eHealth. Dans le cadre de l'échange de données relatives à la santé, l'asbl ABRUMET utilise nécessairement le répertoire des références de la plate-forme eHealth. L'utilisation du numéro de Registre national par les coffres-forts de première ligne repose dès lors sur une autorisation par ou en vertu de la loi et/ou en vertu d'une délibération du Comité. Pour autant que cela soit nécessaire, le Comité confirme que le numéro de Registre national n'est évidemment pas uniquement utilisé en interne pour identifier de manière

[1] Cela ressort des informations complémentaires du 27/04/2017. Dans la demande initiale, la donnée "résidence principale" et donc l'adresse complète d'un usager de soins était demandée.

unique les personnes concernées dont les données à caractère personnel sont enregistrées dans les coffres-forts mais est aussi utilisé lors de la communication de leurs données à caractère personnel parmi les partenaires dans le cadre de l'échange : les prestataires de soins, les hubs, les coffres-forts et la plate-forme eHealth. Ceux-ci ont également été autorisés à utiliser le numéro de Registre national, soit par des délibérations, soit en vertu de 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*.

4. Lors de son examen, le Comité peut dès lors se limiter à vérifier si :

   - les finalités pour lesquelles l'accès à certaines données du Registre national est demandé sont déterminées, explicites et légitimes (article 4, § 1, 2° de la LVP) ;

   - l'accès à ces données est proportionnel à la lumière des finalités (article 4, § 1, 3° de la LVP).

A. FINALITÉS

5. Dans le cadre du partage de données dans les soins de santé via des coffres-forts de première ligne, on distingue 2 sortes de données : des données communes, supportées et proposées par tous les coffres-forts et d'autres données, pour lesquelles chaque coffre-fort détermine de manière autonome quelles données il supporte.

6. Entre les trois coffres-forts de première ligne, il a été convenu que les données communes, comme le Sumehr[2] ou le schéma de médication, qui pourraient être enregistrées dans chacun des coffres-forts, ne seraient enregistrées dans les faits que dans un seul coffre-fort de première ligne. Dans ce contexte, la région où le citoyen réside détermine le coffre-fort.

7. Par conséquent, cela donne lieu aux possibilités suivantes :

   - résidence principale en Région flamande : Vitalink
   - résidence principale en Région wallonne : Intermed (coffre-fort Réseau Santé Wallon)
   - résidence principale en Région bruxelloise ou résidence principale inconnue ou non située en Belgique : BruSafe (coffre-fort Réseau Santé Bruxellois).

[2] Un Sumehr ou SUMmarized Electronic Health Record est utilisé pour l'échange d'informations médicales. Le Sumehr est considéré comme une photo de santé unique de la situation médicale d'un usager de soins. Un médecin traitant ou un titulaire d'un dossier médical global (DMG) gère et constitue un Sumehr afin que celui-ci puisse être consulté par d'autres médecins, tant de première ligne que des médecins et des spécialistes dans les hôpitaux.

8. Cette méthode requiert la connaissance de la région de la résidence principale d'un usager de soins via une consultation du Registre national. Cela signifie évidemment aussi que si un citoyen déménage d'une région vers une autre, la conservation des données passera au coffre-fort du nouveau domicile. Il est uniquement nécessaire de connaître la région du domicile. L'adresse complète n'est pas requise. Le Comité présume que le code postal en tant qu'indicateur pour l'attribution à une région déterminée est concluant et donc suffisant.

9. La finalité de la consultation dans le Registre national de la date du décès est de pouvoir déterminer le moment pour détruire les données à caractère personnel, conformément au principe de proportionnalité. L'Agence flamande Soins et Santé dispose déjà d'une autorisation du Comité pour consulter la date du décès pour cette finalité (voir la délibération RN n° 70/2013 du 9 octobre 2013). Dans le cadre de la présente demande, la même autorisation est demandée pour les deux autres coffres-forts de première ligne.

10. Le gateway Vitalink et le hub auquel un autre coffre-fort de première ligne est relié (Réseau Santé Wallon pour Intermed et Réseau Santé Bruxellois pour BruSafe) contiennent la logique nécessaire pour vérifier la région du domicile d'un usager de soins afin de déterminer ainsi quel coffre-fort met à disposition les informations. Vitalink et les hubs utiliseront le sous-service IdentifyPerson du service web ConsultRR afin de déterminer la région du domicile d'un usager de soins. Le sous-service MutationSender doit leur permettre de prendre connaissance du décès d'une personne. Il s'agit d'un processus automatique permettant uniquement aux collaborateurs des trois coffres-forts de première ligne impliqués dans l'interface d'administration, pour autant que cela soit nécessaire, d'accéder aux données consultées du Registre national.

B. PROPORTIONNALITÉ

B.1. Quant à l'accès aux données

11. Les 3 demandeurs souhaitent accéder à la donnée "région de la résidence principale" et obtenir une communication automatique des modifications. La région de la résidence principale détermine quel coffre-fort de première ligne est responsable de la conservation des données relatives à la santé. Une modification de la région de la résidence principale a pour conséquence qu'un autre coffre-fort de première ligne devient responsable.

12. L'asbl FRATEM et l'asbl ABRUMET souhaitent également un accès à la donnée mentionnée à l'article 3, premier alinéa, 6° de la LRN, à savoir la date du décès et une communication automatique des modifications. Comme déjà précisé, l'Agence flamande Soins et Santé dispose

déjà d'une autorisation du Comité afin de consulter la date du décès pour cette finalité (voir la délibération RN n° 70/2013 du 9 octobre 2013).

13. La finalité de la consultation de la date du décès est de pouvoir déterminer le moment pour supprimer les données à caractère personnel de la banque de données, conformément au principe de proportionnalité.

14. Pour que la communication automatique de ces modifications se fasse de manière proportionnelle, elle doit être limitée aux personnes pour lesquelles les demandeurs disposent d'un dossier actif. Cela requiert de travailler avec un répertoire de références. Les demandeurs ont recours pour ce faire aux services d'un intégrateur de services, à savoir la plate-forme eHealth, pour organiser cette communication proportionnelle.

15. Le Comité estime, compte tenu des renseignements fournis dans la demande, qu'un accès à la donnée "région de la résidence principale", y compris une communication automatique des modifications, dans le chef des demandeurs et un accès à la donnée "date du décès", y compris une communication automatique des modifications, dans le chef de l'asbl FRATEM et de l'asbl ABRUMET, sont proportionnels, adéquats et non excessifs au regard des finalités poursuivies (article 4, § 1, 3° de la LVP).

B.2. Quant à la fréquence de l'accès et à la durée pour laquelle l'accès et l'utilisation sont demandés

16. Les demandeurs souhaitent obtenir un accès permanent aux données demandées. L'organisation de l'enregistrement et de la consultation de données relatives à la santé dans les coffres-forts de première ligne constitue une activité permanente et continue. La prise de connaissance de la date du décès est une nécessité permanente. En outre, en cas de modification d'une région de la résidence principale, les données relatives à la santé doivent pouvoir être transférées immédiatement au coffre-fort de première ligne responsable.

17. Les demandeurs souhaitent une autorisation d'une durée indéterminée. La réalisation des finalités n'est pas limitée dans le temps.

18. Au regard de ce qui précède, le Comité estime qu'un accès permanent et une autorisation à durée indéterminée sont conformes à l'article 4, § 1, 3° de la LVP.

B.3. Quant au délai de conservation

19. L'article 4, § 1, 5° de la LVP exige que les données à caractère personnel ne soient conservées que pour la durée nécessaire à la réalisation de la finalité du traitement.

20. Les données à caractère personnel sont détruites après expiration d'une période suivant le décès de la personne concernée, qui reste à spécifier.

21. Cet élément est précisé comme suit dans les informations complémentaires :

- Vitalink est un coffre-fort de santé organisé par l'Autorité flamande et il ne considère pas les fichiers par patient comme étant un élément d'un dossier du patient au sens de la loi du 22 août 2002 *relative aux droits du patient*. Dans le cadre de Vitalink même, les prestataires de soins restent responsables de la conservation des données (originales) relatives à la santé pour la durée telle qu'imposée par la réglementation applicable (par ex. le code de déontologie de l'Ordre des médecins). Vitalink n'a pas besoin de conserver les données plus longtemps et détruira dès lors les données à caractère personnel après réception de l'avis de décès ;

- La relation entre les prestataires de soins et Intermed/RSW et BruSafe/ABRUMET est de nature contractuelle. RSW et ABRUMET sont des sous-traitants des prestataires de soins. Les données enregistrées font partie du dossier du patient auquel s'applique la loi du 22 août 2002 *relative aux droits du patient*. La connaissance de la date du décès est requise pour RSW et ABRUMET afin de savoir quand certains droits doivent pouvoir être exécutés (par ex. l'article 9, § 4 de la loi du 22 août 2002 *relative aux droits du patient* : accès par l'époux(se) ou des membres de la famille aux données après le décès). Le délai de conservation final de l'ensemble des données est imposé par le délai de conservation qui s'applique pour les données médicales (article 46 du code de déontologie de l'Ordre des médecins : 30 ans après le dernier contact avec le patient (https://www.ordomedic.be/fr/code/chapitre/le-dossier-m%E9dical). Un même délai de conservation est également imposé aux hôpitaux). Pour RSW et ABRUMET, il n'y a donc aucune raison de conserver les données plus de 30 ans après le décès de la personne concernée (= dernier contact possible).

22. Dans la mesure où les demandeurs respectent ce qui est mentionné ci-dessus, ils agissent conformément à l'article 4, § 1, 5° de la LVP.

B.4. Usage interne et/ou communication à des tiers

23. Les collaborateurs des demandeurs qui sont impliqués dans l'interface d'administration auront accès aux données consultées (résidence principale et date du décès) du Registre national. Il n'y a pas de communication à des tiers.

C. SÉCURITÉ

C.1. Conseiller en sécurité de l'information

24. Les bénéficiaires de l'autorisation sont obligés de désigner un conseiller en sécurité de l'information et en protection de la vie privée (article 10 de la LRN). Le Comité constate que l'identité du conseiller des demandeurs a été communiquée.

25. Le Comité rappelle aux bénéficiaires de l'autorisation leurs responsabilités à cet égard.

26. Les bénéficiaires de l'autorisation désignent un conseiller sur la base de ses qualités professionnelles et de ses connaissances spécialisées, en particulier, des pratiques en matière de protection des données et du droit pertinent dans le contexte. Ces capacités permettent au conseiller d'accomplir ses missions et de disposer d'une connaissance suffisante de l'environnement informatique des bénéficiaires de l'autorisation ainsi que de la sécurité de l'information. Le conseiller doit en permanence tenir cette connaissance à jour.

27. Le conseiller fait directement rapport au niveau le plus élevé de la direction des bénéficiaires de l'autorisation. Que le conseiller soit un membre du personnel ou une personne externe, il ne peut pas y avoir de conflit d'intérêts entre la fonction de conseiller et d'autres activités qui sont incompatibles avec cette fonction. En particulier, la fonction ne peut pas être cumulée avec celle de responsable final du service informatique ni avec celle de personne assumant le niveau le plus élevé de la direction des bénéficiaires de l'autorisation (par exemple directeur général).

28. Les bénéficiaires de l'autorisation veillent à ce que le conseiller puisse exercer ses missions en toute indépendance et à ce qu'il ne reçoive aucune instruction pour s'en acquitter. Le conseiller ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions.

29. Si les tâches de conseiller sont confiées à plusieurs personnes, la responsabilité finale doit être confiée à une seule d'entre elles pour faire rapport au niveau le plus élevé de la direction quant aux activités communes et pour assumer le rôle de personne de contact à l'égard du Comité.

30. Les bénéficiaires de l'autorisation aident le conseiller en fournissant les ressources et le temps nécessaires pour exercer ses missions et en lui permettant d'entretenir ses connaissances spécialisées. L'accès aux données à caractère personnel et aux opérations de traitement est notamment fourni au conseiller. Les bénéficiaires de l'autorisation veillent à ce que le conseiller soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

C.2. Politique de sécurité de l'information

31. Il ressort des documents transmis par les demandeurs que ces derniers disposent d'une politique de sécurité de l'information. Le Comité en prend acte.

C.3. Personnes ayant accès aux données et liste de ces personnes

32. Les collaborateurs des demandeurs qui sont impliqués dans l'interface d'administration auront accès aux données consultées (région de la résidence principale et date du décès) du Registre national. Il n'y a pas de communication à des tiers.

33. Comme le prescrit l'article 12 de la LRN, les demandeurs doivent dresser une liste des personnes susmentionnées. Cette liste sera constamment actualisée et tenue à la disposition du Comité. Elle sera soumise au Comité à la première demande. Les personnes figurant sur cette liste doivent en outre signer une déclaration par laquelle elles s'engagent à préserver la sécurité et le caractère confidentiel des informations.

PAR CES MOTIFS,

le Comité

1° autorise l'Agence flamande Soins et Santé, l'asbl FRATEM (InterMed - Réseau Santé Wallon) et l'asbl ABRUMET (BruSafe - Réseau Santé Bruxellois), pour les finalités mentionnées au point A et aux conditions définies dans la présente délibération à obtenir pour une durée indéterminée un accès permanent à la donnée "région de la résidence principale d'un usager de soins", y compris une communication automatique des modifications ;

2° autorise l'asbl FRATEM (InterMed-Réseau Santé Wallon) et l'asbl ABRUMET(BruSafe-Réseau Santé Bruxellois), pour les finalités mentionnées au point A et aux conditions définies dans la présente délibération, à obtenir pour une durée indéterminée un accès permanent à la donnée "date du décès d'un usager de soins", y compris une communication automatique des modifications ;

3 décide que lors de toute modification ultérieure de l'organisation de la sécurité de l'information pouvant avoir un impact sur les réponses données au questionnaire sécurité fourni au Comité (désignation du conseiller en sécurité de l'information et réponses aux questions relatives à l'organisation de la sécurité), les bénéficiaires de l'autorisation adresseront au Comité un nouveau questionnaire relatif à l'état de la sécurité de l'information complété conformément à la vérité. Le Comité en accusera réception et se réserve le droit de réagir ultérieurement, s'il y a lieu ;

4° décide également que, lorsqu'il enverra aux bénéficiaires de l'autorisation un questionnaire relatif à l'état de la sécurité de l'information, ceux-ci devront compléter ce questionnaire conformément à la vérité et le renvoyer au Comité. Il en accusera réception et se réserve le droit de réagir ultérieurement, s'il y a lieu.

L'Administrateur f.f., La Présidente,

(sé) An Machtens (sé) Mireille Salmon