Transmission des données de trajets de soins : avis du Collège de Médecine Générale

Communiqué

Bruxelles, le 6 décembre 2017. - Des membres du Collège Médecine Générale (CMG) se sont concerté avec le responsable de Healthdata.be et, après avoir obtenu un certain nombre de garanties, ont établi que la transmission et le traitement des données dans le cadre des trajets de soins sont sécurisés et confidentiels de manière satisfaisante (voir Annexe 1 pour plus de détails).

Pour cette raison, le Collège de Médecine Générale suspend la mise en garde du 13 novembre 2017 et ne met plus de réserve à la communication des données.

Toutefois, les entretiens qui ont eu lieu avec la Commission Nationale Médico-Mutualiste (CNMM) et avec Healthdata.be nous ont fait relever plusieurs points d'attention :

- D'un point de vue juridique, le contrat trajet de soins doit être modifié tel que demandé par le Comité sectoriel de la Sécurité Sociale et de la Santé.
- Si le point de vue technique est respecté, les aspects juridiques et éthiques doivent être plus largement précisés et suivis, et ce de manière structurelle.
- Les récoltes de données doivent toujours respecter les finalités fixées et validées par le Comité sectoriel de la Sécurité Sociale et de la Santé.
- Des ouvertures ont été faites pour une meilleure concertation avec Healthdata.be et une concertation régulière est prévue.
- En matière de e-Santé, la SSMG demande clairement de continuer la réflexion sur la gouvernance, sur l'amélioration de la qualité des soins par le recueil de données et sur la qualité des analyses de santé publique (voir Annexe 2).

ANNEXES :

1. Une explication détaillée et approuvée par des membres du Collège et Healthdata.be est jointe à ce communiqué (dans ce document).
2. Les remarques et suggestions de la SSMG (dans ce document).
3. Le schéma technique mentionné dans l'annexe 1, en grand format (annexe séparée).

Pour le Collège de Médecine Générale :

ABSyM :	Dr Luc Herry, Dr Michaël Bernier
GBO :	Dr Paul De Munck, Dr Lawrence Cuvelier, Dr Pierre Drielsma
FAGW :	Dr Guy Delrée, Dr Anne Poupaert
FAMGB :	Dr Michel de Volder, Dr Christophe Barbut
SSMG :	Dr Thomas Orban, Dr Geneviève Bruwier, Dr Vincent Parmentier
UCL (CAMG) :	Dr Guy Beuken
ULg (DUMG) :	Dr Didier Giet
ULB (DUMG) :	Dr Philip Thibaut, Dr Benjamin Fauquert

ANNEXE 1 : explications détaillées

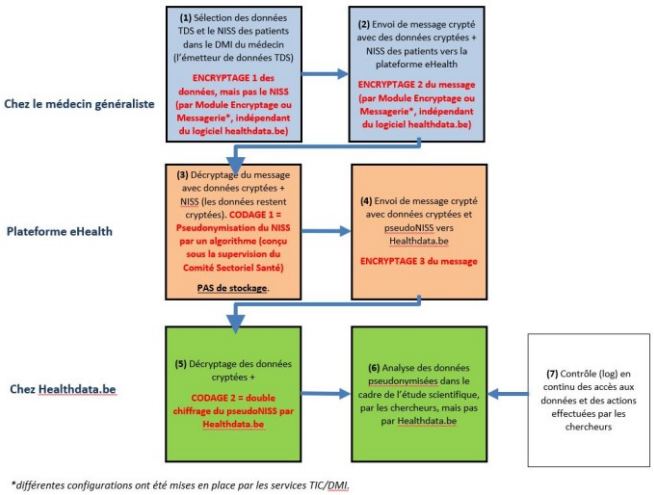
ANNEXE 1 AU COMMUNIQUÉ du 6 décembre 2017. - Conformément à la convention signée entre le médecin généraliste, le patient inclus dans un trajet de soins pour le diabète et/ou l'insuffisance rénale et le spécialiste concerné, les médecins généralistes ont reçu récemment de l'INAMI la demande de transmettre les données convenues dans cette convention. Dans son communiqué du 13 novembre 2017, le Collège de Médecine Générale (CMG) avait émis des réserves concernant cette transmission de données, et avait plus particulièrement demandé des garanties sur le respect du secret professionnel suite à la pseudonymisation (et non l'anonymisation) des données médicales transmises des patients en trajet de soins.

Le débat

Le sujet a été mis à l'ordre du jour de la Commission Nationale Médico-Mutualiste (CNMM) du 20 novembre dernier, lors de laquelle le représentant de Healthdata.be, monsieur Johan Van Bussel, a expliqué en détail la procédure technique de l'encryptage et du traitement des données transmises. A l'issu de la réunion CNMM, il a été décidé que le débat serait poursuivi entre le représentant Healthdata.be et le CMG. Une réunion dans ce sens a eu lieu le 30 novembre 2017, à laquelle ont assisté, outre que Mr Van Bussel de Healthdata.be et des membres du CMG, deux experts en la matière : Dr Benjamin Fauquert, médecin généraliste, Fédération des Maisons Médicales, administrateur de Figac asbl (qui développe des solutions logicielles pour les maisons médicales belges) et chargé de cours sur l'informatique médicale à la faculté de médecine de l'ULB. Le deuxième expert : Maître Jean-Marc Van Gyseghem, Directeur de recherche à l'Université de Namur et Avocat spécialisé dans le domaine de la protection des données à caractère personnel et, plus spécifiquement, celui des données médicales (télématique, réseaux soins de santé, etc.) tant au niveau belge qu'européen.

Les aspects techniques

Lors de la réunion Mr Van Bussel a réexpliqué les procédures techniques appliquées pour l'encryptage et le traitement des données transmises. En résumé, l'encryptage se fait à différents niveaux, en appliquant des méthodes développées en dehors de Healthdata.be. Les différentes étapes d'encryptage sont décrites schématiquement ci-dessous (schéma grand format en Annexe 3 de ce communiqué) :



*différentes configurations ont été mises en place par les services TIC/DMI.

Commentaires importants :

1. Les données déjà 2 x cryptées et les NISS ne sont à aucun moment stockées au sein de la plateforme eHealth ; ces données résident sur la plateforme pendant un court laps de temps, nécessaire à la pseudonymisation automatique du NISS par un algorithme conçu à cet effet par un technicien sous la supervision du Comité Sectoriel Santé.
2. Cet algorithme est réversible uniquement dans l'optique de pouvoir demander des informations au médecin émetteur si nécessaire, et sous le contrôle strict de la plateforme eHealth ; il n'est jamais réversible vers Healthdata.be. En d'autres termes, seul le médecin émetteur peut établir le lien entre les données et le NISS à l'exclusion de toute autre personne.
3. Sur l'infrastructure de Healthdata.be, les NISS sont encore deux fois chiffrés (par Healthdata.be) afin de prévenir le couplage non autorisé des données.
4. Le contrôle (log) des accès et des actions effectués par les collaborateurs de Healthdata.be et par les chercheurs, est accessible à quiconque qui voudrait le consulter : autrement dit, Healthdata.be est ouvert à des contrôles externes des logs.
5. Outre les mesures susmentionnées, Healthdata.be a pris plusieurs autres mesures techniques et organisationnelles pour protéger la vie privée, et elle continue à investir dans de nouvelles mesures.
6. Pour chaque nouveau projet par la plateforme Healthdata.be, une demande d'autorisation est adressée au Comité sectoriel Santé pour le traitement de données à caractère personnel codées relatives à la santé. Chaque projet d'étude est d'ailleurs préalablement évalué par le Comité de pilotage Healthdata.be, dans lequel siègent entre autres 3 médecins généralistes et des éthiciens.

Conclusion

Les experts présents lors de la rencontre avec le responsable de Healthdata.be estiment que des garanties suffisantes sont données pour pouvoir lever la suspension provisoire de la transmission des données TDS.

Suite du débat

Il est apparu lors de la réunion du 30 novembre dernier avec HealthData que différents points devraient faire l'objet d'un suivi et de débats futurs :

1. Le schéma technique présenté ci-dessus donne suffisamment de garanties en termes de protections des données des patients. Néanmoins, cela implique que la convention doit être revue pour refléter ce schéma technique.
2. Dans un contexte plus large, et vu l'évolution rapide des possibilités de l'informatique, on peut s'attendre à la mise sur pied de plus en plus d'études scientifiques basées sur des données de patients. Le Collège de Médecine Générale plaide pour un renforcement considérable de la prise en compte des principes éthiques fondamentaux, tel que c'est le cas par exemple au sein des comités éthiques des hôpitaux ou dans le cadre d'études de recherche clinique. A ce sujet on peut se référer à la Déclaration d'Helsinki, dont on retiendra que le devoir du médecin est de protéger la vie, la santé, la dignité et l'intimité de la personne. La première priorité de l'investigateur est donc la santé de son patient, et non la recherche. Une étude ne peut être

réalisée que si l'importance de l'objectif recherché prévaut sur les contraintes et risques encourus par le sujet.

3. De point de vue juridique, les textes publiés par le Comité sectoriel Santé qui veille sur le cadre des recherches par l'ISP et Healthdata.be ne tiennent pas compte des développements du projet. En effet, on constate que certains textes font référence à des textes antérieurs, qui ne reflètent plus la situation telle qu'elle existe actuellement. Afin de pouvoir disposer d'une information adéquate et complète, gage de transparence tant à l'égard des médecins que des patients, l'ISP-INAMI devrait rapidement produire une note contextuelle actualisant ces documents qui sont sources d'ambigüité. Cela pourrait donner lieu, le cas échéant, à une nouvelle délibération du Comité sectoriel *ad hoc*.
4. Le Collège de Médecine Générale mettra en place une procédure de nomination d'un médecin mandaté pour le contrôle des logs et des processus Healthdata.be.
5. Une réunion de suivi du Collège aura lieu au cours du premier semestre 2018 avec Mr Van Bussel de Healthdata.be.

ANNEXE 2 : remarques et suggestions SSMG

ANNEXE 2 AU COMMUNIQUÉ du 6 décembre 2017. - La SSMG a analysé de façon factuelle la thématique de la transmission des données et a constaté 2 pierres d'achoppement.

1. Une inquiétude liée à la gouvernance qui empêche l'instauration d'une pleine confiance que ce soit à la fois du marché privé (monopole DMI) ou public (mainmise du gouvernement).

2. Une inquiétude liée à la conception du recueil de données qui ne permet pas de convaincre à l'amélioration de la qualité des soins, de la qualité des analyses de santé publique sans surcharge pour les médecins.

1) Au niveau gouvernance/confiance

Au niveau de la gouvernance et des processus décisionnels, nous constatons qu'une amélioration est souhaitable. Pour cette raison, nous demandons que le modèle suivant soit négocié et emporte l'agrément des autorités avant de pouvoir donner une consigne aux médecins :

Vu qu'à la fois le cryptage des identités et des données se trouvent dans des institutions, certes différentes, mais contrôlées par l'État. Vu la rapidité d'execution des décisions au sein de ces structures, à priori différentes, mais ayant des liens étroits de personnes et de systèmes. Vu l'utilisation du comité d'architecture utilisé essentiellement à la validation de protocoles déjà discutés et/ou non sollicité dans des dossiers clés.

La pleine confiance ne pourrait être établie que si la deuxième station des données (phase de cryptage des identités) passe de eHealth aux hubs régionaux/RSW avec le financement afférent.

Arguments :

Il n'y a pas de changement majeur technique ou budgétaire à faire.

Le RSW/RSB ont la capacité de reprendre la deuxième étape de transmission car ils maîtrisent déjà la première étape : le RSW a développé ses propres modules de cryptage et client d'envoi pour l'eHealthbox et a déjà connecté ses composants au logiciel HD4DP dans son produit X-Connect, qu'elle met à la disposition de plus de 30 hôpitaux en Wallonie, à Bruxelles et en Flandre. Le X-Connect est géré par l'équipe RSW à Charleroi.

2) Le problème de conception qui ne permet pas d'atteindre le but d'amélioration de la qualité et l'efficience dans des conditions d'ergonomie acceptables pour les médecins

La conception actuelle des TDS ne permet ni l'amélioration de la qualité des soins, ni des analyses de qualité pour la santé publique :

a) Les données scientifiques concernant le diabète sont insuffisantes.
b) Les éléments essentiels : benchmarking, feedback et support décisionnel dans des processus EBP multidisciplinaires coordonnés n'ont été ni prévus au préalable, ni définis pour être évalués.
c) L'ergonomie et le principe de "code once" (plan eSanté) ne sont pas respectés.

En effet, de nombreuses études montrent qu'il s'agit d'une perte de temps et d'argent de ne pas disposer de l'ensemble des données en permanence surtout dans le cas de polypathologies/maladies chroniques. De plus, il est de notoriété publique que les médecins généralistes ne sont pas experts dans la transmission et l'encodage de données patients de même que ces étapes demandent un temps

dont il ne dispose pas. On s'expose donc inutilement à un risque de non transmission, de données faussées ou incomplètes.

Pour ne pas gaspiller le temps des médecins et les ressources de l'INAMI et de l'ISP sans obtenir de résultats devant servir la qualité des soins et non dans un but de contrôle : nous demandons que le modèle suivant soit négocié et emporte l'agrément des autorités.

Passer au Point 6 du Plan eSanté : dossier patient multidisciplinaire en première priorité, le loger et le financer au niveau du RSW.

Le RSW transforme Intermed (SumEhr) + le schéma médication + la liste résultats en une Plateforme DPM standard HL7 FHIR + Smart on Fhir avec lequel les DMI devront se synchroniser automatiquement (fonctions des liens thérapeutiques).

A partir de la base des données du DPM le RSW crée une Data Warehouse anonyme complète et détaillée.

Cette Data Warehouse peut être exposée comme une API ouverte pour des requêtes.

Et enfin, synchroniser la politique HealthData avec les autres points du Plan eSanté.

Avantages pour les Autorités (SPF/INAMI/ISP)

Selon nous, cette solution permettrait de rendre disponible des données plus complètes, plus détaillées et plus accessibles (API standard) ce qui augmentera les possibilités et la qualité des analyses pour la santé publique (SPF/INAMI/ISP) et pour la recherche par rapport au modèle d'extraction HD4DP actuel.

Étendre la collecte des données avec des Apps Web mobiles pour les prestataires et les patients rapidement et à un moindre coût.

Selon nous, cette solution peut garantir :

1) Une interopérabilité 100% avec un risque technologique moindre que le modèle actuel.
2) Une meilleure sécurité médicale patient (le dernier état des données disponible sans latence et en permanence, bien loin du modèle du SUMERH)
3) De permettre la coordination soins chroniques (impossible actuellement)
4) De permettre la mise en place d'une Evidence Best Practice à un coût de développement accessible
5) De permettre le mHeath.

Avantages pour les Médecins

Après l'accord initial du médecin traitant et du patient : le codage, la récolte et la transmission de données seront automatisables dans le flux du travail normal du médecin généraliste et via l'interface normale de son DMI, c'est à dire on élimine le travail lié à l'extraction, la vérification et l'envoi par HD4DP.
Le contenu du Data Warehouse peut être aussi utilisé pour le développement professionnel, la défense professionnelle et pour tout mécanisme de feed back individuel ou par région.
Le DPM va également assurer une vraie concurrence entre les DMI : le médecin peut changer de DMI en quelques minutes sans pertes et éliminer le stockage sur des serveurs cloud privés des données patients.