Règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plate-forme eHealth [1]

[1] Le Règlement a été approuvé par la section santé du Comité sectoriel de la sécurité sociale et de la santé par sa délibération nr. 14/016 du 18 février 2014, modifiée le 21 février 2017, le 3 juillet 2018 et le 6 octobre 2020, par sa délibération nr. 23/240 du 5 décembre 2023 et par sa délibération nr. 24/198 du 5 novembre 2024.

TABLE DES MATIÈRES

1 Statut du Règlement

Le règlement décrit les règles communes minimales à respecter par l'organisation en vue de l'échange de données de santé entre les utilisateurs affiliés aux différents systèmes d'échange pour lesquels il est fait appel au répertoire des références de la plate-forme eHealth.

La manière selon laquelle les personnes concernées donnent leur consentement pour l'enregistrement des références à leurs données de santé dans le répertoire des références a été approuvée par la délibération n°12/047 du 19 juin 2012 de la section Santé du Comité sectoriel.

La délibération n° 12/047 du 19 juin 2012 porte sur les systèmes d'échange suivants:

- le système des **hubs et du metahub** autorisé par la délibération n° 11/046 du 17 mai 2011 et la délibération n° 12/047 du 19 juin 2012 de la section Santé du Comité sectoriel ;
- **Inter-Med** qui fait partie intégrante du hub Réseau Santé Wallon et dont le règlement va sera soumis à la section « santé » du Comité sectoriel;
- **BruSafe** qui fait partie intégrante du hub Réseau Santé Bruxellois/Brussels Gezondheidsnetwerk et dont le règlement sera soumis à la section Santé du Comité sectoriel ;
- **Vitalink**, autorisé par la délibération n° 12/046 du 19 juin 2012 de la section santé du Comité sectoriel ;
- le **Dossier pharmaceutique partagé**, autorisé par la délibération n° 12/082 du 18 septembre 2012 de la section Santé du Comité sectoriel.

Les délibérations de la section Santé du Comité sectoriel[2], en ce compris les adaptations éventuelles, font intégralement partie du présent règlement.

Le Règlement tient compte de la législation en vigueur, dont le Règlement (UE) n°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), la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 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) n°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, la loi du 22 août 2002 relative aux droits du patient, le secret professionnel (art. 458 du Code pénal), la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

[2] En vertu de 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) n°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, les adaptations éventuelles des délibérations de la section Santé du Comité sectoriel de la sécurité sociale et de la santé est désormais de la compétence de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

2 Objet du règlement: les systèmes d'échange

2.1 Contexte général

L'échange électronique de données à caractère personnel relatives à la santé (dénommées ci-après données de santé) prend une place de plus en plus importante en Belgique. Cela s'explique aisément compte tenu de ses nombreux bénéfices.

Un échange électronique de données à caractère personnel relatives à la santé est avant tout nécessaire à l'appui de soins permanents et de haute qualité. Il intervient prioritairement en support à la continuité des soins et offre les garanties nécessaires sur le plan de la sécurité du patient. Il va de soi que des informations adéquates relatives notamment aux antécédents médicaux du patient (maladies et interventions chirurgicales antérieures, résultats d'examens antérieurs, allergies constatées, ...), à l'état de santé actuel du patient et aux soins de santé actuels administrés au patient (résultats d'examens récents, médicaments, kinésithérapie, ...) sont indispensables pour une prestation de soins optimale au patient. Ces informations se trouvent généralement dispersées dans divers systèmes d'informations de prestataires de soins et établissements de soins et elles doivent être mises à la disposition des prestataires de soins qui traitent le patient, de manière organisée et sécurisée.

Pour le patient et le prestataire de soins, un échange électronique de données à caractère personnel relatives à la santé permet par ailleurs d'éviter bon nombre de charges. Cela permet d'éviter des charges physiques pour le patient, dans la mesure où cela lui évite de devoir subir plusieurs fois le même examen ou de devoir fournir à divers endroits des formulaires et des attestations. Cela permet également de réduire les charges administratives dans la mesure où des prescriptions de soins, des demandes de remboursement de soins ou des renvois par exemple peuvent être effectués de manière beaucoup plus rapide et avec moins de formulaires et de paperasserie.

Une prestation de soins permanente et de haute qualité axée sur le bien-être du patient (tant physique que moral) et une réduction considérable des charges pour tous les acteurs des soins de santé sont donc les principales motivations à l'origine de la volonté d'optimaliser et d'informatiser les échanges de données à caractère personnel relatives à la santé.

Les systèmes d'échange concernés par le présent règlement visent à un tel échange électronique sécurisé entre tous les prestataires de soins dans le cadre spécifique de la prise en charge de la santé de la personne concernée. Les prestataires de soins dans le cadre de la prise en charge de la santé ne comprennent pas les prestataires de soins qui interviennent dans le cadre de la médecine d'assurance, de la médecine judiciaire, de la médecine du travail et des activités des mutualités. L'échange de données pour ces dernières catégories est régi par la législation en vigueur. En concordance avec la législation, cet échange peut se faire soit en utilisant d'autres systèmes que celui décrit dans le présent règlement, tel l'eHealthBox, soit en utilisant certains composants décrits dans ce règlement avec l'accord explicite de l'instance qui met à disposition le composant concerné et avec l'autorisation du Comité sectoriel de la santé.

2.2 Objectifs généraux

Le but final est de permettre l'interconnexion entre les systèmes régionaux et locaux d'échange d'informations relatives à la santé afin de permettre à un prestataire de soins de retrouver et de consulter les données électroniques relatives à la santé disponibles au sujet d'un patient et ce indépendamment, d'une part, du lieu effectif de stockage des données et, d'autre part, du point d'entrée du prestataire dans le système. L'objectif est de supporter l'échange de données dans le contexte de la prise en charge de la santé de la personne concernée, sans qu'il n'y ait nécessairement une centralisation des données, et au travers des relais locaux ou régionaux organisés et gérés par des représentants des prestataires et établissements de soins ou des plateformes de collaboration.

Lors de l'échange électronique de données de santé, une protection adéquate de la vie privée du patient et une sécurité de l'information solide sont évidemment essentielles. Les mesures de protection de la vie privée et de sécurité de l'information doivent donc être implémentées de manière à éviter au

maximum les risques d'utilisation illégitime des données à caractère personnel relatives à la santé, tout en réalisant les avantages poursuivis en matière de qualité et de continuité des soins, de sécurité du patient et de réduction des charges. Il convient donc de trouver un bon équilibre entre la sécurité de l'information et un échange de données efficace.

Par ailleurs, les principes de fonctionnement des systèmes d'échange concernés doivent être clairs pour chaque patient dont les données relatives à la santé font l'objet d'un échange. Chaque patient doit pouvoir obtenir un aperçu précis et compréhensible lui permettant de savoir qui peut échanger quelles données de santé, avec qui, pour quelles finalités et à quel moment.

2.3 Principes généraux et acteurs

2.3.1 Hubs, autres systèmes d'échange de données, metahub et répertoire des références

Pour rappel, une des caractéristiques principales est qu'il y va de la réalisation et de l'interconnexion des systèmes d'échange concernés, sans centralisation systématique de ces données.

La mise en place des systèmes d'échanges décentralisés est intrinsèquement liée à l'instauration du « *répertoire des références* » prévu par l'article 5, 4°, b), de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth. Le répertoire des références est, en effet, la clef de voûte de ce système puisqu'il permet de savoir où se trouve une donnée de santé relative à un patient.

Le répertoire des références mis en place dans le cadre des systèmes d'échange concernés se structure en deux couches.

Une première couche, très agrégée, est stockée au niveau de la plate-forme eHealth. Cette couche, dénommée « *metahub* », contient uniquement une indication du fait qu'il existe une information au sujet d'un patient :

- au sein d'un réseau local ou régional appelé « hub » (Abrumet, Réseau Santé Wallon, Antwerpse Regionale Hub, Collaboratief Zorgplatform, Vlaams Ziekenhuisnetwerk KU Leuven), ou

- dans la mesure où il n'est pas affilié à un hub, dans un « coffre-fort » de santé (« gezondheidskluis », p.ex. Vitalink) ou dans une série de banques de données décentralisées (p.ex. "Pharmaceutical Care Data Hub" pour ce qui concerne le Dossier pharmaceutique partagé).

Une seconde couche se situe ensuite au niveau des hubs. En soutien aux fonctionnalités primaires du système du metahub, une des finalités principales des hubs est donc de tenir à jour un répertoire des références qui indique auprès de quel établissement de soins ou autre réseau d'échange affilié au hub se trouve une donnée de santé relative à un patient.

Cette approche « en couches » a été retenue pour deux raisons principales: d'une part, la plate-forme eHealth ne stocke pas ainsi, même indirectement, de données de santé des patients et, d'autre part, cette approche permet de respecter les initiatives (pré)existantes mises en place au niveau de l'échange de données.

Le répertoire des références est donc finalement constitué du répertoire des références du metahub et de l'ensemble des répertoires de références des hubs..

Au sein du répertoire des références (et donc au sein des systèmes d'échange concernés), le patient est identifié par son numéro d'identification de la sécurité sociale (NISS).

2.3.2 Acteurs et utilisateurs

Ce modèle en couches implique que le fonctionnement des systèmes d'échange concernés repose sur la collaboration entre différents acteurs. Le but du présent document est précisément de décrire les rôles de ces acteurs.

Comme indiqué à la section précédente, le répertoire de références est maintenu conjointement par :

- la plate-forme eHealth pour la partie « metahub » ;

- les organisations de prestataires de soins ou établissements de soins responsables de chacun des « hubs » ;
- l'asbl «FarmaFlux» qui est chargée de l'organisation du système d'échange 'Dossier pharmaceutique partagé' ;
- la Plateforme de collaboration Eerstelijnsgezondheidszorg qui est responsable de l'organisation du système d'échange 'Vitalink' .

Les établissements de soins concernés affiliés à un hub jouent également un rôle essentiel puisque, in fine, ils restent responsables de la conservation et de la disponibilité effective des données échangées.

Dans les autres systèmes d'échange (Vitalink, Inter-Med, BruSafe Dossier pharmaceutique partagé), ce sont les systèmes mêmes qui ont la tâche de prévoir la conservation et la disponibilité des données échangées. En effet, ces systèmes ont été conçus sous forme de 'coffres forts' ('kluizen') dans lesquels les différentes catégories d'utilisateurs autorisés peuvent enregistrer et consulter des données de santé.

Les gestionnaires des systèmes d'échange (tant les hubs que les autres systèmes) sont personnellement responsables de leur organisation interne (dans la mesure où ils respectent les principes minimaux décrits dans le présent règlement).

Au niveau des utilisateurs, les systèmes visent l'échange de données de santé entre tous les prestataires de soins visés par la loi du 10 mai 2015 relative à l'exercice des professions des soins de santé et les établissements de soins au sens de la loi instituant la plate-forme eHealth (dans le cadre de la prise en charge du patient). Moyennant l'autorisation explicite de la section Santé du Comité sectoriel, l'échange de données de santé entre des prestataires autres que ceux visés dans la loi du 10 mai 2015 relative à l'exercice des professions des soins de santé est aussi possible.

Finalement, il importe de souligner le rôle central du patient, tant comme sujet principal du système puisque le système est développé dans l'intérêt exclusif du patient et que cet intérêt doit primer sur toute autre considération, que comme utilisateur actif au niveau des « fonctions de régulation », le patient gardant la maîtrise sur la mise à disposition des données le concernant au sein des systèmes d'échange concernés.

2.4 Nature des données échangées

Les données de santé qui peuvent être échangées à travers les systèmes d'échange concernés sont les données de santé qui figurent dans les dossiers de patients ou dans un coffre-fort de santé. Le contenu des données de santé qui sont enregistrées dans le dossier du patient ou dans un coffre-fort de santé relève de la responsabilité du détenteur du dossier du patient ou du fournisseur de la donnée de santé. En aucune façon, les acteurs concernés (les hubs, l'asbl FarmaFlux, la plateforme de collaboration Eerstelijnsgezondheidszorg ou la plate-forme eHealth) ne peuvent être tenus pour responsables de la qualité ou de la complétude des données de santé échangées dans le cadre des systèmes d'échange concernés.

Un dossier de patient contient par exemple des résultats d'examens, des résultats d'imagerie médicale, des lettres de sortie d'hôpital, des rapports sur les interventions chirurgicales et l'historique de médication. Un coffre-fort de santé peut, par exemple contenir un schéma de médication, un schéma de vaccination et/ou un Sumehr.

L'accès aux catégories de données de santé est déterminé pour chaque système d'échange, en fonction de la catégorie du prestataire de soins, par l'autorisation concernée du Comité sectoriel.

Même si un prestataire de soins a accès à toutes ou à certaines données de santé, il ne peut utiliser que les seules données qui sont pertinentes et non excessives au regard de la prise en charge de la santé de la personne concernée, conformément au principe de finalité.

Les prestataires de soins qui interviennent au sein d'une organisation qui respecte le règlement relatif au cercle de confiance et qui l'a fait savoir à son autorité de tutelle, peuvent charger des personnes qui les assistent dans le cadre de leur travail (par exemple, un.e secrétaire, un.e infirmier.ère, un coordinateur de transplantation) d'accéder, sous leur responsabilité, aux systèmes d'échange de

données relatives à la santé, selon les dispositions précisées ci-après. Ce collaborateur reçoit, à ce moment, pour ce système, l'accès du prestataire de soins qui a donné l'ordre. Le prestataire de soins qui confère le mandat doit avoir une relation thérapeutique avec le patient. Ce n'est que dans le cas d'un dossier de transplantation que la relation thérapeutique ne doit pas être vérifiée parce que le patient donateur de l'organe est décédé. Tous les prestataires de soins énumérés dans la loi du 10 mai 2015 relative à l'exercice des professions des soins de santé et précisés dans le présent paragraphe, ne peuvent pas faire l'objet d'une exclusion par le patient.

Le mandat conféré au collaborateur pour traiter les données des patients au nom du prestataire de soins inclut l'aspect du secret médical auquel ce collaborateur est tenu et précise que le médecin traitant assume la responsabilité du traitement de données à caractère personnel et veille au traitement correct. Ce type de mandat peut par exemple être repris dans le contrat du travail ou dans la convention d'utilisation du système d'information local.

En cas de consultations du système des hubs et coffres-forts de eHealth, l'interrogation a lieu sur la base de l'identité du prestataire de soins responsable et de l'identification du CoT. Dans les loggings des systèmes centraux accessibles en ligne par le citoyen concerné, sont seulement enregistrées l'identité du prestataire de soins traitant et l'identification du CoT. Néanmoins, le système d'information local doit prévoir des loggings qui permettent de contrôler quel collaborateur a réalisé la consultation.

2.5 Portée du Règlement

Le Règlement définit les règles communes minimales pour l'organisation de l'échange de données de santé entre les utilisateurs affiliés auprès des différents systèmes d'échange concernés, au moyen du répertoire des références de la plate-forme eHealth

Un système d'échange peut prévoir, dans le cadre de son propre fonctionnement, des modalités ou fonctionnalités supplémentaires, dans la mesure où celles-ci sont conformes à la législation en vigueur et aux règles communes minimales décrites dans le présent Règlement.

3 Architecture et répartitions des tâches

Cette section du document a pour objectif de décrire les différentes fonctions qui permettent de garantir l'échange de données entre les différents systèmes concernés.

Le système, dans sa globalité, se doit de supporter deux groupes de fonctionnalités majeures.

- D'une part, le système doit permettre la mise à disposition et la recherche de données relatives à la santé d'un patient ainsi que la sélection et la consultation de ces données. Ces fonctionnalités sont dénommées ci-après « *fonctionnalités primaires* »,
- D'autre part, le système doit supporter toutes les fonctionnalités nécessaires au respect de la vie privée du patient et à l'application des règles relatives à l'échange de données à caractère personnel relatives à la santé. Ces fonctionnalités sont dénommées ci-après « *fonctionnalités de régulation*».

Dans un premier temps, cette section rappelle les principes de base relatifs aux « fonctions de régulation » du système tels que décrits dans [1] et [2] pour, dans un second temps, s'attaquer à la description de l'architecture générale du système et à la répartition des tâches qui en résultent.

3.1 Principes relatifs aux fonctions de régulation

3.1.1 Consentement éclairé du patient

Le patient doit donner son consentement pour permettre la consultation des références dans le répertoire des références. L'enregistrement du consentement ne peut avoir lieu que pour autant que le patient ait été informé correctement de la portée et des conséquences de son consentement.

Le contenu et les modalités du consentement du patient ont été approuvés par le Comité sectoriel, par sa délibération n° 12/047 du 19 juin 2012.

L'échange de données à caractère personnel relatives à la santé ne requiert pas le consentement de la personne concernée lorsque, conformément à l'article 7, § 2, j) de la loi relative à la vie privée, l'échange est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé dans l'intérêt de la personne concernée et que les données sont traitées sous la surveillance d'un professionnel des soins de santé. Le consentement dont il est question dans le présent règlement se limite par conséquent à l'enregistrement et à la consultation des références dans le répertoire des références.

De manière concrète, l'enregistrement du consentement peut intervenir par le biais de différents canaux:

- soit directement par le patient lui-même (ou par son représentant légal),
- soit par un médecin, un pharmacien, un infirmier[3], une sage-femme[3], un dentiste[3], un kinésithérapeute[4], un établissement de soins, une institution publique qui pose des actes dans le cadre de la médecine préventive telle que Kind&Gezin, l'Office de naissance et de l'enfance, les « Centra voor Leerlingenbegeleiding », les Centres psycho-médico-sociaux, ou une mutualité ; un établissement de soins est en l'occurrence défini comme une institution ou une organisation coupole dans le secteur des soins de santé qui a été créée sous la forme d'une personne morale (par exemple un hôpital) ou d'un groupe identifié de prestataires de soins (par exemple dans le cas d'une pratique de groupe de médecins généralistes, d'un regroupement d'infirmiers à domicile, de maisons de repos, etc.),
- par des mandataires au nom d'un patient, par exemple des proches qui assurent les soins, personne de confiance.

Dans la mesure où l'enregistrement n'est pas réalisé directement par le patient ou son représentant légal, un médecin, un pharmacien, un infirmier, une sage-femme, un dentiste ou un kinésithérapeute, il doit au moins être réalisé par un intervenant qui agit sous la responsabilité d'un médecin, d'un pharmacien, d'un infirmier, d'une sage-femme, d'un dentiste ou d'un kinésithérapeute.

Lorsqu'un médecin, un pharmacien, un infirmier, une sage-femme, un dentiste, un kinésithérapeute, un établissement de soins ou une institution publique qui pose des actes dans le cadre de la médecine préventive enregistre le consentement, le numéro d'identification de la sécurité sociale du patient ainsi que le numéro de sa carte d'identité électronique ou de sa carte ISI+ doivent en principe être communiqués.

Si l'enregistrement du consentement est réalisé par le médecin généraliste détenteur du DMG du patient concerné ou par la mutualité, seul le numéro d'identification de la sécurité sociale du patient doit être communiqué.

En ce qui concerne les hubs, les modalités supplémentaires suivantes ont par ailleurs été acceptées.

- Un hub peut par ailleurs demander que les patients des prestataires de soins et hôpitaux affiliés chez lui signent un document comportant le consentement éclairé. Le prestataire de soins ou

[3] Cette possibilité n'entre en vigueur qu'à partir du moment où le logiciel pour ce secteur sera en mesure d'alimenter directement la banque centrale des consentements de la Plate-forme eHealth.

l'hôpital en question est alors responsable de la signature et de la conservation du document relatif au consentement éclairé. Dans ce cas, le numéro de la carte d'identité électronique ou le numéro de la carte ISI+ de l'intéressé ne sont pas obligatoires, tandis que le numéro d'identification à la sécurité sociale demeure indispensable.

- Un hub peut par ailleurs prévoir que le consentement du patient dans le cadre d'un hôpital soit simplement enregistré sur la base du numéro d'identification de la sécurité sociale sans mention du numéro de la carte d'identité électronique ou du numéro de la carte ISI+. Dans ce cas, la présence du patient et la communication effective d'informations doivent être garanties à l'aide d'autres éléments tels que des procédures spécifiques de mise à disposition d'informations au sein des différents services de l'hôpital en question.

Tout acteur concerné par l'obtention du consentement éclairé, est tenu de le communiquer immédiatement à la banque centrale des consentements de la plate-forme eHealth.

Le patient, ou le cas échéant, son représentant légal, pourra enregistrer le consentement au moyen d'une application web spécifique garantissant l'authentification de l'identité du patient par le biais de la carte d'identité électronique.

L'enregistrement par un prestataire, un établissement de soins ou la mutualité devrait idéalement pouvoir être effectué soit à l'aide de leurs outils informatiques usuels, soit à l'aide d'une application web. Toute opération relative à l'enregistrement d'un consentement est loggée.

Le patient peut vérifier en ligne quel médecin, quel pharmacien, quel infirmier, quelle sage-femme, quel dentiste, quel kinésithérapeute, quel établissement de soins, quelle institution publique qui pose des actes dans le cadre de la médecine préventive ou quelle mutualité a réalisé l'enregistrement du consentement. Par ailleurs, le patient dispose à tout moment de la possibilité de retirer son consentement.

En ce qui concerne la possibilité d'enregistrement du consentement des enfants mineurs, il est prévu qu'à partir de l'âge de seize ans les mineurs ont la possibilité de (faire) enregistrer eux-mêmes leur consentement. Avant l'âge de seize ans, ce droit revient à leur représentant légal. La qualité de ces représentants est en principe vérifiée dans des sources authentiques validées. Par dérogation, un hub peut enregistrer la qualité de ces représentants au moyen d'une procédure sur support papier ou au moyen d'une procédure électronique, laquelle exigera non seulement la lecture de l'eID du mineur en question mais également la signature électronique du représentant légal concerné au moyen de sa carte d'identité électronique.

D'autres types de représentation seront ajoutés au Règlement.

3.1.2 Relation thérapeutique et relation de soins

Un prestataire de soins qui traite ou soigne personnellement le patient, possède une relation de soins avec le patient. S'il est question d'une relation de soins entre le patient et un prestataire de soins telle que visée dans la loi du 10 mai 2015 relative à l'exercice des professions des soins de santé, il est par ailleurs question d'une relation thérapeutique.

La consultation de données de santé via les systèmes d'échange concernés requiert la vérification préalable de l'existence d'une **relation thérapeutique** entre le prestataire de soins qui émet la requête de consultation et le patient.

Si, moyennant l'autorisation explicite de la section Santé du Comité sectoriel, l'échange de données de santé entre des prestataires de soins autres que ceux visés dans la loi du 10 mai 2015 relative à l'exercice des professions des soins de santé est prévu, la consultation d'une donnée de santé requiert la vérification préalable de l'existence d'une **relation de soins** entre le prestataire de soins qui envoie la requête de consultation et le patient.

Les catégories de preuves électroniques d'une relation thérapeutique et d'une relation de soins sont décrites dans une note qui a été approuvée par la section Santé du Comité sectoriel par sa délibération n° 11/088 du 18 octobre 2011. Toute adaptation à cette note fera l'objet d'une concertation préalable au sein du Comité de concertation des utilisateurs de la Plate-forme eHealth.

3.1.3 Exclusions

Le patient qui a donné son consentement, a la faculté d'exclure des prestataires de soins individuels de l'accès électronique à ses données de santé.

L'exigence d'un traitement de qualité implique cependant qu'il n'est pas opportun qu'un membre déterminé d'une équipe de prestataires de soins puisse être exclu, par exemple au sein d'une institution de soins. Le fonctionnement de l'équipe est, en effet, compromis si l'un des membres est exclu. Ceci a pour conséquence que l'opposition à l'égard d'un membre d'un groupe de prestataires fixe peut s'étendre à l'ensemble de ce groupe[4] en fonction du contexte des soins fournis.

Contrairement à l'enregistrement du consentement qui peut être effectué non seulement par le patient mais également par un médecin, un pharmacien, un infirmier, une sage-femme, un dentiste, un kinésithérapeute, un établissement de soins, une institution publique qui pose des actes dans le cadre de la médecine préventive ou une mutualité, l'exclusion de prestataires de soins peut uniquement être effectuée par le patient ou par son représentant légal.

Par dérogation, un hub peut prévoir - s'il le souhaite – qu'un prestataire de soins puisse également enregistrer une exclusion à la demande du patient, moyennant la preuve de l'existence préalable d'une relation thérapeutique entre le patient et le prestataire de soins qui enregistre l'exclusion.

3.1.4 Droits d'accès

Dans le cadre des différents systèmes d'échange concernés, il est techniquement possible de rendre certaines données de santé uniquement accessibles à une ou plusieurs catégories de prestataires de soins.

L'accès concret aux différentes catégories de données de santé est déterminé, en fonction de la catégorie de prestataires de soins et par projet, par la chambre sécurité sociale et santé du Comité de sécurité de l'information, après concertation au sein du Comité de Concertation des utilisateurs de la Plate-forme eHealth.

3.1.5 Publication

En ce qui concerne la publication de données de santé, tant le prestataire de soins que le patient peut décider qu'une donnée de santé ne sera pas publiée. Dans ce cas, aucune référence à cette donnée de santé ne sera enregistrée dans les différentes couches du répertoire des références.

Les hubs prévoient à cet égard une politique relative à la publication des données de santé "antérieures". En particulier, dans le cas de la cessation des activités professionnelles d'un prestataire de soins liées à un hôpital (par ex. en cas de décès, de départ à la pension ou de changement d'institution hospitalière), la responsabilité de la publication des données des dossiers médicaux hospitaliers du prestataire de soins en question est transmise au médecin en chef de l'hôpital concerné.

3.1.6 Données de logging

Des données de logging et des mécanismes de détection sont prévus de sorte qu'en cas de besoin, l'identité de toute personne qui a eu accès aux données à caractère personnel ou qui a traité ces données, puisse être retrouvée.

La gestion et la conservation de ces données de logs se fait "en cascades". Ainsi, la plate-forme eHealth conservera les données de loggings relatives à l'accès aux références contenues dans la partie "metahub" du répertoire de références, tandis que les systèmes d'échange concernés conserveront les données de logging relatives aux accès effectués à leurs références et données de santé.

[4] Ceci ne veut pas dire que le patient connaîtra effectivement la composition des dits « groupes » mais qu'il devra être correctement informé de l'éventualité de cette extension de la portée d'une exclusion individuelle.

3.1.7 Situation d'urgence

Dans le cas d'une urgence thérapeutique, les vérifications préalables liées à l'existence d'un consentement et d'une relation thérapeutique ou d'une relation de soins ne sont pas nécessaires (« *break the glass*»). Dans pareil cas, il n'est pas non plus tenu compte des exclusions enregistrées.

Cette exception requiert cependant qu'il soit enregistré dans les données de logging que le prestataire de soins concerné a invoqué l'existence d'une situation d'urgence.

3.2 Architecture et répartition des tâches

Dans cette section, on rappelle les grands principes de l'architecture mise en place au sein des différents systèmes de sorte à pouvoir identifier les principales responsabilités fonctionnelles des différents acteurs. Cette architecture sera évidemment sujette à évolution notamment sur base de l'expérience effective du système, des éventuelles extensions d'utilisation et des évolutions en termes d'interaction entre les systèmes. Il importera donc de faire évoluer celle-ci en collaboration avec les différents acteurs impliqués.

Cette section se limite aux grands principes fondateurs des systèmes et à ceux qui impliquent une coordination entre différents systèmes. L'architecture interne de chaque système reste du ressort de chaque système et ne fait donc pas l'objet du présent règlement.

En conséquence, cette section se structure en six sous-sections : les cinq premières sont respectivement dédiées aux systèmes « hubs & metahub », Inter-Med, BruSafe, Vitalink et Dossier Pharmaceutique Partagé, tandis que la dernière section aborde les interactions entre ces trois systèmes (telles que convenues à ce jour).

Le système des hubs et metahub étant en lui-même basé sur la collaboration des différents hubs, sa description sera naturellement plus détaillée.

Rappelons que tous les systèmes décrits se conforment évidemment aux principes des fonctionnalités de régulation décrits à la section 3.1. Les précisions qui suivent ne concernent que l'implémentation effective de ces principes dans la mesure où cette implémentation requière la collaboration de différents acteurs.

3.2.1 Hubs & metahub

3.2.1.1 Architecture : principes généraux

L'architecture retenue est une architecture distribuée de type « System-to-System » dont les hubs sont l'élément clef. Chaque hub permet l'échange de documents entre les systèmes et les prestataires de soins qui sont affiliés au hub. Chaque hub maintient un répertoire de références indiquant au sein de quel système appartenant à son réseau se trouvent un ou plusieurs documents associés à un patient.

Le service de base appelé « *metahub* » mis à disposition par la plate-forme eHealth intervient en support de l'échange de données entre hubs. Plus précisément, ce service permet à un hub de savoir s'il existe des documents associés à un patient au sein d'un autre hub. Cependant, les flux d'échange de données à proprement parler transitent au travers des hubs et pas au travers du metahub. Les qualités requises pour accéder aux services du metahub ou pour permettre les connexions de hub à hub sont validées au travers du « User and Access Management » de la plate-forme eHealth. Le metahub est alimenté par les hubs.

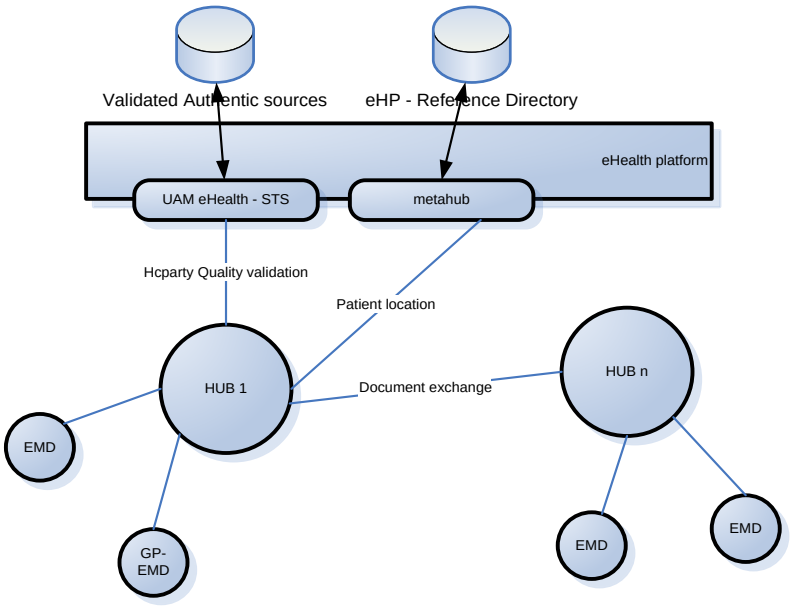

Figure 1 : Architecture générale

Pour supporter cette architecture, chaque hub est amené à interagir avec trois types d'acteurs principaux : ses clients (les hôpitaux et les prestataires de soins connectés aux hubs), les autres hubs et le metahub. On distingue donc trois types d'interaction standard : les fonctionnalités offertes par un hub à ses clients des hubs –dites « intrahub »-, les fonctionnalités à destination des autres hubs –dites « interhub »- et les interactions entre les hubs et le metahub.

3.2.1.2 Fonctionnalités primaires

Fonctionnalités intrahub

Un hub doit permettre à ses clients d'alimenter et de consulter son répertoire de références. En d'autres termes, il doit permettre

- de déclarer un document associé à un patient en fournissant quelques informations minimales telles que l'auteur médical du document,
- de consulter la liste des références de documents associés à un patient (en supportant quelques critères additionnels de recherche tels que l'auteur ou le type du document, p.ex. 'résultat d'examen' ou 'notification d'admission'),
- de révoquer la déclaration d'un document.

Un hub doit également permettre à son client d'obtenir un document sur base d'une référence. En d'autres termes, il doit permettre la transmission sécurisée d'un document conservé, soit chez un de ses clients, soit auprès d'un client d'un autre hub (depuis ce hub).

Les opérations de consultation doivent pouvoir porter sur l'ensemble du système « hubs & metahub ».

Dans le contexte d'une consultation interne au hub, toutes les vérifications liées à la régulation des accès sont à charge du hub. Dans le contexte d'une consultation « inter-hub », les vérifications uniquement liées au prestataire de soins et au patient sont sous la responsabilité du hub où est effectuée la requête tandis que les vérifications impliquant des droits d'accès spécifiques au niveau documentaire sont à charge du hub dépositaire du document.

Tous les accès aux documents médicaux (ou aux références) doivent être enregistrés.

Fonctionnalités interhub

Pour permettre les recherches et les consultations dans l'ensemble du système, chaque hub doit offrir aux autres hubs ces mêmes fonctionnalités. Plus précisément, un hub doit permettre aux autres hubs

- de consulter la liste des références de documents associés à un patient en son sein (en supportant les critères de recherche minimaux définis au niveau des fonctionnalités intrahub).
- d'obtenir sur base d'une référence un document stocké chez un de ses clients.

Rappelons que lorsqu'un hub utilise un des services fournis par un autre hub, il incombe au hub utilisateur de garantir que le patient adhère au système et que la consultation est justifiée par l'existence d'une relation thérapeutique entre le prestataire et le patient.

Interactions avec le metahub

Lors d'une recherche globale de documents, le hub initiateur de la recherche consulte le metahub pour identifier les autres hubs susceptibles de référencer des documents relatifs à ce patient. Pour que le metahub puisse remplir cette fonction, il faut qu'un hub qui référence un document associé à un patient déclare un lien avec ce patient au niveau du metahub. Un tel lien ne peut être consultable que si le patient a donné son consentement au système.

3.2.1.3 Fonctionnalités de régulation

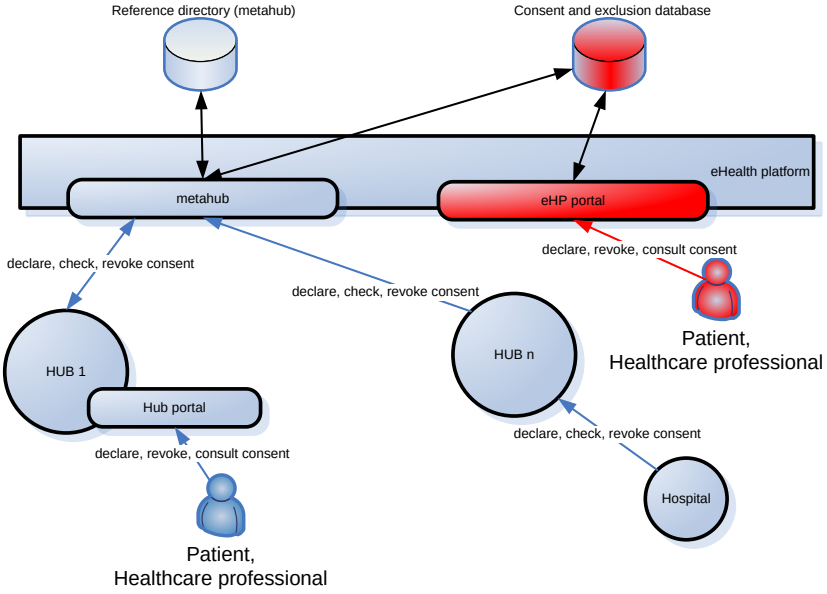

Figure 2 : Consentements

Consentements

Aucune référence relative à un patient n'est consultable sans que celui-ci n'ait donné son consentement eHealth. Ces consentements sont enregistrés au sein d'une banque de données de la plate-forme eHealth. Ils peuvent être introduits, révoqués ou consultés au travers de différents canaux d'entrée (selon les modalités rappelées dans la section 3.1.1 et détaillées dans [2]).

En particulier, une application web permettant la gestion de ces consentements par les différents acteurs autorisés est mise à disposition par la plate-forme eHealth.

Fonctionnalités intrahub

Chaque hub permet à ses clients de vérifier l'existence du consentement d'un patient et d'obtenir les informations relatives à celui-ci (p.ex. acteur ayant introduit ce consentement), de déclarer ou de révoquer un consentement.

Certains hubs offrent des portails permettant la gestion des consentements.

Interactions avec le metahub

Le metahub doit permettre aux hubs de déclarer et de révoquer des consentements. Il doit également permettre de vérifier l'existence d'un consentement et d'obtenir les informations relatives à celui-ci (p.ex. acteur ayant introduit ce consentement).

Pour que ce service puisse fonctionner, toute déclaration ou révocation de consentement effectuée au niveau d'un hub doit être transmise par celui-ci au metahub. Réciproquement, le metahub offre aux hubs un mécanisme permettant de connaître les altérations effectuées au niveau des consentements.

Liens thérapeutiques

Aucune donnée relative à un patient ne peut être consultée par un prestataire de soins sans qu'il n'existe une relation thérapeutique qui justifie cette consultation. Il appartient au hub au sein duquel est émise la requête de consultation de vérifier l'existence de la déclaration de cette relation thérapeutique.

Fonctionnalités intrahub

Un hub permet à ses clients de déclarer un lien thérapeutique, de vérifier l'existence d'un lien thérapeutique et de révoquer un lien thérapeutique (en accord avec les principes de preuves décrits dans [3]).

Certains hubs offrent des portails permettant la gestion des liens thérapeutiques (propres au hub).

Interactions avec le metahub

Le metahub ne stocke aucune information relative aux liens thérapeutiques. Cependant, les liens thérapeutiques enregistrés au sein d'une source authentique validée accessible au travers de services de base de la plate-forme eHealth (tels que l'existence d'un DMG) peuvent être consultables au travers du service « metahub » de sorte à proposer une seule interface technique aux hubs.

Exclusions

Une référence relative à un patient ne peut être consultée par un prestataire de soins s'il existe une exclusion entre ce patient et ce prestataire de soins. Il appartient au hub au sein duquel est émise la requête de consultation de vérifier l'inexistence d'une telle exclusion.

Tout comme les consentements, les exclusions de type « patient-prestataire de soins » sont enregistrées au sein d'une banque de données de la plate-forme eHealth. De nouveau, ces exclusions peuvent être introduites, consultées et révoquées au travers de différents canaux d'entrée (dont, en particulier, l'application web de la plate-forme eHealth susmentionnée pour les consentements).

Fonctionnalités intrahub

Chaque hub permet à ses clients de vérifier l'inexistence d'une exclusion et, éventuellement, de déclarer ou de révoquer une exclusion (selon les modalités décrites dans [2]).

Certains hubs offrent des portails permettant la gestion des exclusions.

Interactions avec le metahub

Le metahub doit permettre aux hubs de déclarer et de révoquer des exclusions. Il doit également permettre de vérifier l'inexistence d'une exclusion et d'obtenir les informations relatives à celle-ci (p.ex. acteur ayant introduit cette exclusion).

Pour que ce service puisse fonctionner, toute déclaration ou révocation d'exclusion effectuée au niveau d'un hub doit être transmise par celui-ci au metahub. Réciproquement, le metahub offre aux hubs un mécanisme permettant de connaître les altérations effectuées au niveau des exclusions.

Droits d'accès documentaires

Les droits d'accès spécifiques aux documents sont vérifiés par le hub dépositaire du document sur base des informations fournies par le hub émetteur de la requête de consultation.

Fonctionnalités intrahub

Les hubs prévoient des services techniques permettant la déclaration, la révocation et la vérification de droits d'accès spécifiques au niveau des documents.

Données de « logs »

Tous les accès aux documents médicaux (ou aux références) doivent être enregistrés.

Fonctionnalités intrahub

Chaque hub permet à ses clients de consulter les accès effectués sur les données d'un patient (dans l'ensemble du système).

Fonctionnalités interhub

Chaque hub permet aux autres hubs de consulter les accès effectués sur les données d'un patient (en son sein).

Interactions avec le metahub

Le metahub permet aux hubs de consulter les opérations effectuées sur les données d'un patient (au niveau du metahub).

3.2.1.4 Éléments techniques

Sans entrer dans le détail des spécifications techniques, cette section énonce quelques principes généraux à respecter au niveau de l'implémentation.

Standards d'échange

Pour supporter une telle architecture, il est nécessaire de standardiser les interfaces techniques définissant les échanges entre les différents acteurs. La règle générale est que les interfaces techniques sont implémentées au travers de « webservices standard » (appelés « webservices KMEHR ») dont la spécification est publiée par la plate-forme eHealth.

Plus précisément, cette spécification comporte trois parties.

1. La spécification du service de base « metahub » de la plate-forme eHealth.
2. La spécification des webservices correspondant aux fonctionnalités interhub.

   Cette spécification est établie conjointement par les partenaires et doit être implémentée par tous les hubs participant au système « hubs & metahub ».
3. La spécification des webservices correspondant aux fonctionnalités intrahub.

   Cette spécification est établie conjointement par les partenaires et est recommandée à tous les partenaires.

   Bien qu'un hub soit tenu de supporter les fonctionnalités intrahub décrites à la section 3.2., il peut faire le choix de ne pas employer en son sein la structure de message commune établie pour celles-ci. Comme, par ailleurs, cette même structure sera employée au niveau des échanges entre hubs, un tel hub se doit donc de mettre en place les conversions techniques adéquates.

   Ce sont ces « webservices standard» et uniquement eux qui sont maintenus et publiés par la plate-forme eHealth et, à ce titre, sont ou seront intégrés au niveau des leviers supportés par la plate-forme eHealth en termes de standardisation (tels que l'enregistrement des logiciels ou le développement de librairies de connexions).

Chiffrement

Si la vocation primaire d'un hub est de mettre en place un répertoire de références pour permettre la recherche de documents associés à un patient, un hub n'a pas pour vocation de stocker les documents qu'il référence. A terme, le stockage de documents médicaux n'entre donc pas dans les fonctionnalités standard d'un hub. Il n'est également pas, a priori, du ressort d'un hub de visualiser un document médical. Le hub prend en charge le transfert sécurisé du document médical mais ne s'occupe pas de la présentation finale de ce document au prestataire de soins. Cette fonctionnalité est du ressort du « client » du hub (typiquement de l'hôpital ou du logiciel du médecin extrahospitalier).

En conséquence, les finalités primaires d'un hub ne nécessitent pas qu'un hub ait accès au contenu médical d'un document. La solution la plus simple pour garantir la confidentialité de ce contenu médical réside dans la mise en place d'un système de chiffrement de « bout en bout ». Il est cependant évident que les hubs qui ne travailleront pas avec des « webservices standard » à destination de leurs clients ne pourront mettre en place un tel système au vu des conversions techniques qu'ils devront supporter. Ces hubs se devront donc de reporter la mise en place des garanties de confidentialité au niveau organisationnel.

Concrètement, le contenu[5] des échanges inter-hubs seront préférablement chiffrés de « bout en bout » (p.ex. d'hôpital à hôpital). Si un hub « sans chiffrement » intervient dans un tel échange, les opérations de chiffrement et de déchiffrement seront à charge de ce hub et celui-ci devra, par d'autres moyens, garantir la confidentialité du document.

Dans un but de simplification et afin de s'inscrire dans une vision globale, un seul mécanisme de chiffrement est retenu. Ce mécanisme repose sur la solution de chiffrement spécifiée et développée par la plate-forme eHealth. L'objectif est que, in fine, chaque prestataire de soins (personne physique ou organisation) devant réaliser une opération de chiffrement[6] ne soit confronté qu'à une seule spécification technique permettant de réaliser cette opération.

Puisque certains hubs appliquent un principe de chiffrement de « bout en bout » et d'autres pas, la solution mise en place supporte différentes « profondeurs » de chiffrement. Par exemple, un hôpital au sein d'un hub appliquant un principe de chiffrement de « bout en bout » peut être amené à chiffrer un message à destination d'un autre hôpital ou à destination d'un hub.

3.2.2 Inter-Med

3.2.2.1 Architecture : principes généraux

Le projet Inter-Med est en fait une composante du hub Réseau Santé Wallon qui intervient en soutien à la communication avec la première ligne. Cette composante vise à permettre le stockage et le partage de données en provenance des prestataires de soins de première ligne. Dans la phase actuelle, il s'agit des Sumehrs et des schémas de médication.

L'architecture Inter-Med se confond donc avec l'architecture de son « hub ». Le serveur Inter-Med peut être vu comme une forme de « fournisseur de données » du hub (tout comme un hôpital connecté au hub) qui contient les données qui ont été chargées par les prestataires de soins de première ligne.

3.2.2.2 Fonctionnalités primaires

Le système Inter-Med permet le stockage de données en provenance de la première ligne et leur partage au travers du système « hubs & metahub ». Il est peut être vu comme « un coffre-fort de données de santé » intégré au sein du hub

Les données de santé stockées au niveau d'Inter-Med sont intégrées au sein du répertoire de références du hub.

3.2.2.3 Fonctionnalités de régulation

Les fonctionnalités de régulation d'Inter-Med sont identiques à celles mises en place au sein du hub auquel il appartient-.

3.2.2.4 Eléments techniques

Les webservices permettant la communication avec Inter-Med font partie intégrante de ceux définis dans le contexte du système « hubs & metahub ».

3.2.3 BruSafe

3.2.3.1 Architecture : principes généraux

Le projet BruSafe est en fait une composante du hub Réseau Santé Bruxellois / Brussels Gezondheidsnetwerk qui intervient à titre de support dans le cadre de la communication avec la première ligne. Ce projet vise à permettre l'enregistrement et le partage de données en provenance des

[5] La discussion porte ici uniquement sur le contenu médical, hors éléments nécessaires au fonctionnement du répertoire de références, des échanges et non sur la sécurisation globale du système.
[6] Rappelons qu'il s'agit ici uniquement de chiffrement de données médicales au niveau « message » et non de chiffrement lié aux couches transports.

prestataires de soins de première ligne. Dans la phase actuelle il s'agit des Sumehrs et des schémas de médication.

L'architecture de BruSafe se confond donc avec l'architecture de son « hub ». Le serveur BruSafe peut être considéré comme une sorte de « fournisseur de données » du hub (tout comme un hôpital connecté au hub) qui contient les données qui ont été chargées par les prestataires de soins de première ligne.

3.2.3.2 Fonctionnalités primaires

Le système BruSafe permet l'enregistrement de données en provenance de la première ligne et leur partage au travers du système « hubs & metahub ». Il est peut être considéré comme « un coffre-fort de données de santé » intégré au sein du hub

Les données de santé stockées au niveau de BruSafe sont intégrées au sein du répertoire de références du hub.

3.2.3.3 Fonctionnalités de régulation

Les fonctionnalités de régulation de BruSafe sont identiques à celles mises en place au sein du hub auquel il appartient.

3.2.3.4 Eléments techniques

Les webservices permettant la communication avec BruSafe font partie intégrante de ceux définis dans le contexte du système « hubs & metahub ».

3.2.4 Vitalink

On ne fournit ici que les principes fondateurs du système. Le détail des fonctionnalités et garanties en matière de sécurité est fourni dans [5].

3.2.4.1 Architecture : principes généraux

Comme le système hubs & metahub, le système Vitalink est primairement basé sur une architecture de type « system-to-system» reposant sur un ensemble de webservices directement intégrables au sein des systèmes informatiques des prestataires et organisations de soins « clientes ».

Le système Vitalink n'est par contre pas un système distribué et vise à soutenir le partage multidisciplinaire de données de santé et de bien-être entre tous les acteurs de première ligne impliqués dans la prise en charge du patient, par la mise en place d'un « coffre-fort » pour les données nécessaires à cette finalité.

3.2.4.2 Fonctionnalités primaires

Le système Vitalink permet à ses clients[7] :

- de « stocker » des données de santé (en fournissant un ensemble de meta-données telles que le « type » de la donnée de santé) ;
- de mettre à jour ces données de santé ;
- de consulter les données de santé associées à un patient (en supportant quelques critères additionnels de recherche tels que le type de la donnée de santé).

[7] Cette section ne concerne que le système Vitalink pris isolément. Les principes relatifs aux échanges de données Hubs-Vitalink sont décrits dans la section 3.2.6.

3.2.4.3 Fonctionnalités de régulation

Consentements

Aucune donnée relative à un patient n'est publiée sans que celui-ci n'ait donné son consentement eHealth. Vitalink vérifie l'existence de ce consentement au travers du « User and Access Management eHealth ».

Liens thérapeutiques

Aucune donnée relative à un patient ne peut être consultée par un prestataire de soins sans qu'il existe une relation de soins qui justifie cette consultation. Il appartient à Vitalink de vérifier l'existence d'une déclaration pour cette relation de soins.

Pour les prestataires individuels, Vitalink effectue cette vérification auprès du « User and Access Management » de la plate-forme eHealth. Pour les établissements de soins, Vitalink applique le principe du « tiers de confiance ».

Exclusions

Aucune donnée relative à un patient ne peut être consultée par un prestataire de soins s'il existe une exclusion entre ce patient et ce prestataire de soins. Vitalink vérifie l'inexistence d'une telle exclusion auprès du « User and Access Management » de la plate-forme eHealth.

Droits d'accès documentaires

Vitalink limite les accès à certaines catégories de données en fonction du type de prestataire de soins, en accord avec les décisions de la section Santé du Comité sectoriel (cf. [5] pour la grille des accès actuels).

Données de « logs »

Tous les accès aux données de santé sont enregistrés.

3.2.4.4 Éléments techniques

Chiffrement

Les données mises à disposition au travers du projet Vitalink sont en effet conservées selon un principe de « threshold encryption » à deux parties. Au-delà des principes rappelés précédemment, l'accès aux données n'est techniquement possible que si on dispose des deux morceaux d'une clef privée répartie entre deux acteurs indépendants (qui sont ici la plate-forme eHealth et un « comité indépendant de gestionnaires de clefs » regroupant des représentants des médecins, des patients, des mutualités et des acteurs de première ligne).

3.2.5 Dossier Pharmaceutique Partagé (DPP)

On ne fournit ici que les principes fondateurs du système. Le détail des fonctionnalités et garanties en matière de sécurité est fourni dans [6].

3.2.5.1 Architecture : principes généraux

Le système du DPP repose sur deux composants principaux dénommés TIP (« Trusted Intermediary for Pharmacists » et PCDH (« Pharmaceutical Care Data Hub »). Le TIP est une forme de système de collecte central cohérente et qualitative des données émises par les officines qui assure l'uniformité et la sécurisation des flux de données tandis que le système de stockage et de partage à proprement parler réside au niveau du PCDH.

Tout comme les systèmes précédemment décrits, tant le TIP que le PCDH proposent leurs services sous forme de webservices visant une intégration directe au sein des logiciels des officines.

Le TIP est un composant générique de « capture de données » au niveau des officines allant au-delà des systèmes de partage visés par le présent document.

3.2.5.2 Fonctionnalités primaires

Le DPP permet à ses clients (les officines)

- de « stocker » les données relatives au suivi des soins pharmaceutiques d'un patient au sein du PCDH,
- de consulter les données de santé associées à un patient dans le cadre des soins pharmaceutiques.

3.2.5.3 Fonctionnalités de régulation

Consentements

Aucune donnée relative à un patient n'est consultable sans que celui-ci n'ait donné son consentement eHealth. Le PCDH vérifie l'existence de ce consentement au travers du « User and Access Management » de la plate-forme eHealth.

Liens thérapeutiques

Aucune donnée relative à un patient ne peut être consultée par un prestataire de soins sans qu'il n'existe une relation thérapeutique qui justifie cette consultation. Il appartient au PCDH de vérifier l'existence d'une déclaration pour cette relation thérapeutique. Le PCDH met en place son propre système de vérification des relations thérapeutiques.

Exclusions

Aucune donnée relative à un patient ne peut être consultée par un prestataire de soins s'il existe une exclusion entre ce patient et ce prestataire de soins. Le PCDH vérifie l'inexistence d'une telle exclusion auprès du « User and Access Management » de la plate-forme eHealth.

Données de « logs »

Tous les accès aux données de santé sont enregistrés.

3.2.5.4 Éléments techniques

Chiffrement

Les données au sein du PCDH sont conservées[8] de manière chiffrée selon le même principe de chiffrement que celui appliqué pour le système Recip-e.

Ce système repose sur un principe de chiffrement symétrique : chaque délivrance est chiffrée sur base d'une clef de chiffrement qui est conservée au niveau de la plate-forme eHealth tandis que le système ne conserve que la délivrance chiffrée. Ce n'est que lorsque que la délivrance est effectivement consultée qu'elle peut être déchiffrée.

3.2.6 Interactions Hubs, Inter-Med, BruSafe et Vitalink

Seuls les principes d'interaction entre les hubs (en ce compris les composantes Inter-Med et BruSafe) et Vitalink ont été discutés[9].

3.2.6.1 Architecture : principes généraux

L'objectif principal est de permettre à un prestataire de soins de pouvoir accéder à l'ensemble des informations mises à disposition au travers de l'un ou l'autre des systèmes participants, ce dans le respect des règles d'accès établies par ceux-ci ; lesquelles se conforment aux principes minimaux établis par la note relative au consentement éclairé du patient [1].

[8] L'historique des délivrances est limité à une année.

[9] Ces principes ne sont pas encore effectivement mis en place. Cette section sera donc d'application après que les développements requis aient été réalisés.

La consultation via un hub permet d'accéder à l'ensemble des informations mise à disposition tandis que la consultation via Vitalink est limitée au contenu informationnel disponible en son sein. En d'autres termes, l'interconnexion mise en place est unidirectionnelle (des hubs vers Vitalink). Il n'est donc pas possible d'accéder via Vitalink à une information qui ne se trouve pas dans Vitalink tandis qu'il est possible d'accéder, via un hub, au informations des hubs, d'Inter-Med et de Vitalink.

Un second objectif est de permettre aux hôpitaux de mettre à jour/à disposition des données au sein de Vitalink. Cette mise à jour/à disposition peut se faire au travers des hubs. Ce second objectif concerne uniquement les hôpitaux néerlandophones.

Entre les trois coffres-forts de santé de la première ligne (Vitalink, Inter-Med et BruSafe) il est convenu que les données de personnes avec un NISS qui pourraient être enregistrées dans chacun des coffres-forts (par exemple le Sumehr ou le schéma de médication) ne seront effectivement enregistrées que dans un seul coffre-fort de santé de première ligne. C'est la région du domicile de l'intéressé qui détermine le coffre-fort de santé. Ceci signifie que si l'intéressé déménage d'une région vers une autre, la conservation de ses données sera reprise par le coffre-fort de santé de son nouveau domicile. Cette méthode de travail requiert la consultation du Registre national. Une autorisation du Comité sectoriel doit être obtenue pour cette consultation. Si un citoyen n'a plus de domicile mais dispose d'un numéro NISS, les données seront enregistrées dans le coffre-fort de santé bruxellois.

3.2.6.2 Fonctionnalités primaires

Interactions hubs-Vitalink

Vitalink permet à un hub

- de « stocker » des données de santé (en fournissant un ensemble de meta-données telles que le « type » de la donnée de santé) ;
- de mettre à jour ces données de santé ;
- de consulter les données de santé associées à un patient (en supportant quelques critères additionnels de recherche tels que le type de la donnée de santé).

Interactions avec le metahub

Dans le cadre de l'interconnexion avec le système hubs & metahub, Vitalink déclare un lien avec un patient si une information est disponible au sujet de ce patient.

3.2.6.3 Fonctionnalités de régulation

Vitalink considère un hub comme un « tiers de confiance ». En d'autres termes, les principes définis à cet égard au niveau des échanges interhub sont d'application.

3.2.6.4 Éléments techniques

Les exigences suivantes ont été posées.

1. **Exigence 1**
   Une exigence réside dans la minimisation des impacts techniques au niveau des « clients » des systèmes partenaires (hubs et Vitalink). Plus précisément, la solution retenue doit permettre de réaliser l'objectif 1 sans nécessiter de modification au niveau des interfaces proposées aux clients actuels des hubs et de Vitalink.
2. **Exigence 2**
   Par ailleurs, les principes d'encryption mis en place au niveau de chaque système ne peuvent être remis en cause.

La combinaison de ces deux exigences implique que les hubs doivent pouvoir jouer le rôle de « tiers de confiance » pour Vitalink au niveau du chiffrement des données.

Les hubs se connectent au système Vitalink selon les standards Vitalink (concrètement au travers du connecteur Vitalink). Le système Vitalink supporte cependant additionnellement la fonctionnalité de « recherche des références associées à un patient » selon le standard des webservices Kmehr établi dans le cadre du système hubs et metahub.

4 Principes de gouvernance

4.1 Organisation et gestion

Le Comité de gestion de la plate-forme eHealth est chargé de la coordination et de l'organisation du système des hubs et du metahub.

Le Comité de gestion de la plate-forme eHealth est également chargé de la coordination et de la collaboration entre les différents systèmes d'échange, plus précisément :

- le système des hubs et du metahub ;
- Vitalink ;
- le Dossier pharmaceutique partagé ;
- Inter-Med;
- BruSafe

Le mode d'organisation du traitement de données à caractère personnel au sein des systèmes Vitalink, du Dossier pharmaceutique partagé, d'Inter-Med et de BruSafe est déterminé, respectivement, par la Plateforme de collaboration Eerstelijnsgezondheidszorg, l'asbl FarmaFlux, l'asbl Fratem et l'asbl Abrumet, moyennant l'approbation de la section Santé du Comité sectoriel.

Afin d'assister le Comité de gestion dans ses missions d'organisation et de coordination, le Comité de concertation des utilisateurs de la Plate-forme eHealth organise, conformément à ses missions légales, à la demande du Comité de gestion ou de sa propre initiative, des groupes de travail spécifiques. La mission et la composition de ces groupes de travail sont déterminées en concertation avec le Comité de concertation.

Le règlement donne une description de la situation actuelle de la collaboration entre les systèmes d'échange concernés. Il a indéniablement un caractère évolutif. Si cela s'avère pertinent, il est adapté aux évolutions technologiques et sociales en la matière.

Après une concertation préalable au niveau du Comité de concertation des utilisateurs de la Plate-forme eHealth ou d'un groupe de travail défini à cet égard par celui-ci, le règlement et toute modification au règlement sont soumis à l'approbation de la section Santé du Comité sectoriel.

Après son approbation par la section Santé du Comité sectoriel, le règlement et toute modification du règlement doivent obligatoirement être respectés par les systèmes d'échange concernés et l'ensemble des utilisateurs de ces systèmes d'échange.

4.2 Système des hubs et du metahub

4.2.1 Conditions

Pour accéder au système des hubs et du metahub, chaque hub doit remplir les conditions décrites dans le présent règlement.

Chaque hub est tenu de prendre les mesures organisationnelles nécessaires afin de garantir l'exécution des règles fonctionnelles telles que fixées dans le règlement, notamment sur le plan des procédures, des ressources et des mesures de protection.

Chaque hub doit garantir le libre choix d'affiliation des utilisateurs du système des hubs et du metahub.

4.2.2 Accès au système des hubs et du metahub

Tout hub candidat est tenu d'introduire une demande de connexion auprès de la section Santé du Comité sectoriel.

La section Santé du Comité sectoriel vérifie ensuite si le hub candidat remplit les conditions décrites dans le présent Règlement.

Ce n'est qu'après que la section Santé du Comité sectoriel ait constaté qu'un hub candidat répond aux conditions décrites dans le règlement qu'un hub peut accéder au système des hubs et du metahub.

La section Santé du Comité sectoriel assure la surveillance du respect des dispositions du présent Règlement par les hubs connectés. Dans le cadre de cette surveillance, tout hub est tenu d'honorer immédiatement toute demande de communication d'information de la part de la section Santé du Comité sectoriel.

Si un hub souhaite quitter le projet des hubs et du metahub, pour quelle que raison que ce soit, il est tenu d'en informer la plate-forme eHealth dans les meilleurs délais. Le cas échéant, le hub est tenu de prendre toutes les mesures nécessaires afin de garantir la continuité du système des hubs et du metahub. Ceci signifie qu'il mettra les données de son répertoire des références ainsi que les données de l'*audit trail* à la disposition du système des hubs et du metahub.

4.3 Responsabilités

La plate-forme eHealth, les systèmes d'échange concernés et tout utilisateur doivent être considérés comme les responsables en ce qui concerne les traitements de données à caractère personnel qui sont exécutés sous leur surveillance et contrôle respectifs.

Les responsabilités de la plate-forme eHealth sont, en tout cas, limitées aux dispositions prévues par la loi.

Les engagements de la plate-forme eHealth, des hubs, Inter-Med, BruSafe, Vitalink et de l'asbl « FarmaFlux » sont qualifiés d'obligations de moyens.

La plate-forme eHealth, les systèmes d'échange concernés et les utilisateurs sont, chacun pour eux et à l'exclusion des autres, responsables de toute perte, tout dommage ou tout tort à des tiers suite à l'exécution de leurs responsabilités dans le cadre des modalités des systèmes d'échanges telles que fixées dans le cadre du présent règlement.

Références

https://www.ehealth.fgov.be/fr/ehealth-en-pratique/services-de-base/repertoire-des-references/en-savoir-plus

Principes généraux : consentements et preuves de relations thérapeutiques et relations de soins

[1] Délibération 12/047 (juin 2016) sur la portée du consentement éclairé

[2] Annexe de la délibération 11/046 (juin 2016) sur les modalités du consentement éclairé

[3] Annexe de la délibération 11/088 du 18 octobre 2011 (juin 2016) sur les "Preuves de relations thérapeutiques"

https://www.ehealth.fgov.be/fr/a-propos-de-ehealth/organisation/comite-sectoriel/presentation

Systèmes de partage de données couverts par le consentement éclairé

[4] Annexe de la délibération 11/089 du 22 novembre 2011 décrivant le "règlement général du projet hubs & metahub"

[5] Délibération n° 12/046 du 19 juin 2012, modifiée en dernier lieu le 17 septembre 2013, relative au projet Vitalink

[6] Délibération n° 12/082 du 18 septembre 2012 relative au système GFD-DPP

https://www.ehealth.fgov.be/fr/a-propos-de-ehealth/organisation/comite-sectoriel/presentation

Application eHealthConsent

Les projets associés à l'application eHealthConsent sont listés au niveau de la page

https://www.ehealth.fgov.be/fr/citoyens/services-en-ligne/ehealthconsent/en-savoir-plus-0