Welcome Pack

La plate-forme eHealth met à la disposition des partenaires un inventaire détaillé des informations nécessaires pour l'intégration de ses différents services. Ce catalogue comprend l'ensemble de 'ce qu'il faut savoir', 'ce qu'il faut comprendre' et 'ce qu'il faut prévoir' avant de démarrer un projet ainsi que les adresses de contact utiles.

Un projet doit répondre au minimum aux contraintes suivantes – la mise en production est soumise strictement au respect de ces contraintes

1. Prise de connaissance par le partenaire des informations contenues dans notre Welcome Pack
2. Rédaction et approbation d'un dossier unique
3. Approbation du Comité sectoriel (si nécessaire)
4. Rédaction et approbation d'un planning
5. Rédaction et mise à disposition de la documentation technique (si nécessaire)

Process des projets

1. Prise de connaissance par le partenaire des informations contenues dans notre Welcome Pack
2. A cette issué, prise de contact par le partenaire avec notre cellule projets avec un résumé du projet comprenant la finalité du projet, les flux déterminés, les services sollicités etc..
3. Examen du projet en interne > Attribution si accord à un chef de projet
4. Introduction si nécessaire par le partenaire d'un dossier unique
5. Examen juridique du projet par la plate-forme eHealth (le projet nécessite-t-il une délibération ou un avis du comité sectoriel ?)
6. Proposition de planning en accord avec la cellule IT – introduction du projet dans le release calendar
7. Contact si nécessaire avec la cellule IT (soutien à l'intégration des composants utiles)
8. Mise à disposition si nécessaire des documents techniques par le partenaire

Services de base

1. Coordination de processus partiels électroniques
2. Certificats eHealth
3. Portail
4. Timestamping
5. Répertoire des références (Metahub)
6. Pseudonymisation & Anonymisation
7. Système de cryptage end-to-end
8. eHealthBox
9. RN Consult
10. I.AM (Identity & Access Management)

Architectures

1. Architectures

Application LiveCycle

1. Releases Management
2. eHealth Business Continuity Plan
3. Niveaux de service

Connectors

1. eHealth platform services connectors

Services en ligne

1. Accès aux coffres-forts de soins
2. WalCareNet - MemberData

Sécurité de l'information & Vie privée

1. Toolbox
2. Normes minimales
3. Formation & GDPR

Standards

1. Standards

Important

La plate-forme eHealth rappelle à ses partenaires l'importance de toujours reprendre contact avec ses services s'ils souhaitent développer un nouveau projet ou étendre un projet existant. En l'absence de cette diligence, la plate-forme eHealth peut être impactée à différents niveaux.

En effet, en ce qui concerne le suivi des projets, la plate-forme eHealth risque de ne plus disposer de vue globale sur l'ensemble des projets utilisant ses services de base. Des incohérences sur le plan de l'architecture pourraient par ce biais être générées. Une telle façon de procéder pourrait également surcharger la capacité technique de la plate-forme eHealth en cas d'envois massifs et simultanés de messages, ayant pour conséquence d'impacter la disponibilité du service de base pour l'ensemble des partenaires.

Les conditions générales relatives à l'octroi du certificat eHealth (acceptation et production) énoncent à cette fin depuis le mois de septembre 2013 que « toute utilisation du certificat eHealth se limite, le cas échéant, au champ d'application des délibérations juridiques existantes. En cas d'extension, adaptation ou évolution de la finalité ou portée de cette utilisation, il faut obligatoirement contacter la plate-forme eHealth ».

La plate-forme eHealth invite donc ses partenaires à tenir compte des responsabilités qui leur incombent et de l'obligation qui est la leur de respecter les termes du dossier unique.

Services de base

1. Coordination de processus partiels électroniques

Qu'est-ce que le service « Coordination de processus » ?

Ce service vise à permettre l'intégration, harmonieuse et flexible, des différents services (services de base et applications) au sein d'un système d'échange de données déterminé.

Il veille à ce que les messages soient structurés et compréhensibles par les différents systèmes. Il s'assure que les fonctionnalités sont compatibles, respectent certains standards et qu'il n'y a pas de variation des niveaux de sécurité selon les étapes de la procédure.

Cette coordination est transparente pour l'utilisateur et s'effectue notamment au moyen de ce qu'on appelle un Entreprise Service Bus (ESB).

Quelles sont les fonctionnalités du service ?

Le service de coordination des processus offre les fonctionnalités suivantes :

- standardisation des messages et erreurs ;
- vérification et propagation de l'identité de l'utilisateur (la vérification effectuée dépend du service appelé par l'utilisateur) ;
- gestion de loggins de sécurité ;
- orchestration des appels :
    - transformation des messages,
    - enrichissement des messages,
    - transport des messages vers les services web des partenaires ou de la plate-forme eHealth

En pratique

Dépendances, recommandations et avertissement

Recommandations :

- les services des partenaires doivent prendre les mesures nécessaires pour garantir la stabilité et la conformité des services appelés par notre ESB ;

- les services des partenaires doivent être en mesure d'investiguer les incidents ;
- chaque service consumer doit veiller à suivre les directives relatives à la sécurisation des sites web.

Avertissement

Les services échangeant des données de manière asynchrone ne peuvent pas utiliser ce service.

Quelles sont les conditions d'intégration d'un service au sein de la plate-forme eHealth ?

Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, eHealthppkb@ehealth.fgov.be, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.

La plate-forme eHealth peut inclure ces services dans les connecteurs facilitant l'intégration de l'appel aux services.

Pour plus d'information, contactez support@ehealth.fgov.be.

2. Certificats eHealth

Qu'est-ce qu'un certificat eHealth ?

Les certificats délivrés par la plate-forme eHealth permettent à un individu ou une organisation de s'authentifier en tant que prestataire de soins ou institution reconnue.

Lorsqu'un prestataire de soins souhaite avoir accès à certains services de base de la plate-forme eHealth en utilisant une connexion de système à système et non une application web, il doit disposer d'un certificat eHealth. Ce certificat permet d'identifier et d'authentifier le partenaire « système » tandis que l'eID ou le token permet d'identifier et d'authentifier l'utilisateur (la personne).

Ceci est valable tant pour l'utilisation de services de base que pour l'utilisation d'applications proposées sous forme de services web.

Le certificat, une fois configuré dans le logiciel du prestataire ou de l'institution, permet d'utiliser les services mis à disposition par la plate-forme eHealth et requérant une authentification.

Un certificat eHealth peut être demandé et installé grâce à une application téléchargeable.

Si vous disposez d'une version Java plus récente que Java 8, le lien ci-dessus **ne peut plus** être utilisé pour démarrer l'application. C'est pourquoi l'application est également proposée via un fichier ZIP téléchargeable. Dans ce cas, vous pouvez extraire le fichier dans un dossier sur votre ordinateur et démarrer le programme via le fichier .cmd (Windows) ou .sh (MacOS, Linux).

Les intégrateurs de logiciels (et non les prestataires de soins) peuvent par ailleurs demander des certificats de test. Ces certificats permettent, aux collaborateurs IT de ces intégrateurs de logiciels actifs dans le secteur belge des soins de santé, de tester l'intégration de nos services de base. Pour plus d'information, consultez les pages dédiées aux environnements de test et certificats d'acceptation.

Quelles sont les fonctionnalités d'un certificat eHealth ?

Le certificat offre les fonctionnalités suivantes :

- la possibilité pour le prestataire ou l'institution de s'authentifier lors de l'utilisation des services web eHealth, notamment en demandant un jeton de session (session token) permettant l'accès à ces services ;
- la possibilité de chiffrer des messages, par exemple dans le cadre de l'utilisation d'une eHealthBox (certificat et mot de passe associé servent alors de clé privée de chiffrement) ;
- la possibilité pour un prestataire ou une institution de recevoir des messages chiffrés (une clé publique est en effet créée en même temps que le certificat et mise à disposition du public grâce à un service web dédié, ETEE ETKDepot).

En pratique

Dépendances, recommandations et avertissements

Pour un prestataire de soins individuel, il faut :

- que son profil soit enregistré dans une source authentique validée ;
- disposer d'un moyen d'authentification considéré comme fort (eID).

Pour les prestataires non belges, qui ne disposent pas de facto d'une eID mais qui, exerçant sur le territoire belge, ont besoin d'un accès aux services en ligne et dès lors d'un certificat, il existe une méthode hybride pour la demande d'un certificat eHealth.

Pour les institutions de soins, il faut :

- que leur profil soit enregistré dans une source authentique validée, en ce compris le titulaire du certificat autorisé au nom de l'institution ;
- que le détenteur du certificat dispose d'un moyen d'authentification considéré comme fort ;

- que les normes minimales de la sécurité sociale soient respectées ;
- que le fonctionnement interne de l'institution de soins garantisse que seules les personnes autorisées ont accès au système ;
- qu'elles disposent d'une autorisation contenant les conditions de partage des données relatives aux soins de santé entre les institutions de soins de santé.

Afin d'utiliser un certificat eHealth pour s'authentifier dans un service web, le prestataire ou l'institution devra disposer d'un logiciel médical intégrant l'utilisation des certificats eHealth (ce qui est le cas de l'ensemble des logiciels enregistrés par la plate-forme eHealth).

Avant de procéder à la demande / l'utilisation d'un certificat eHealth, veillez à prendre connaissance des informations disponibles dans le « Welcome Pack », du règlement d'utilisation ainsi que des directives pour un usage des certificats eHealth en toute sécurité dans un contexte médical.

Demande de certificat - Mode d'emploi

Qui peut demander un certificat ?

Les prestataires de soins actifs dans le secteur des soins de santé belge.

Important !

- Il y a lieu d'opérer une distinction entre un certificat individuel (personnel) et un certificat pour une organisation (pour un établissement de soins) :
  - dans le cas d'un certificat pour une organisation ou un établissement, un titulaire de certificat mandataire est responsable, au nom de la personne morale, de la gestion et de l'utilisation correctes du certificat ;
  - le titulaire du certificat est donc responsable du respect rigoureux des conditions d'utilisation .
- Un certificat eHealth est valide 36 mois (peut être renouvelé à partir de 90 jours avant la fin de la période des 36 mois/3 ans).

Processus de demande

Introduisez votre demande via l'application eHealth Certificate Manager.

Cette application permet les opérations suivantes :

- demander un certificat eHealth et des clés d'encryption (voir cryptage end-to-end pour les clés) ;
- renouveler un certificat (endéans la période de renouvellement de trois mois) ;
- révoquer un certificat ;
- modifier le mot de passe des clés d'encryption.

3. Portail

Le portail eSanté est historiquement un point d'entrée sécurisé et coordonné pour les acteurs des soins de santé aux différentes applications et informations disponibles en matière de santé en ligne (eSanté). Il offre également toute l'information disponible en matière de support technique aux développeurs ICT pour l'intégration de nos services de base. La gestion du contenu du portail est assurée par un « Content Management System » (CMS) qui permet de concevoir et de mettre à jour de manière dynamique les différents contenus utiles (textes, FAQ's, outils de support en ligne, documents divers, structures de menus, etc.).

Quelles sont les fonctionnalités d'un CMS ?

L'intégration d'un CMS pour gérer un site web ou une application offre les fonctionnalités suivantes (liste non-exhaustive) :

- gestion de contenus génériques (actualités, FAQs, support,… caractéristiques d'un type de contenu) :
  - champs obligatoires ou optionnels,
  - possibilité de créer des liens entre les contenus,
  - plus de 30 types de données possibles (dates, données numériques, textes libres, couleurs),
  - plusieurs langues possibles ;
- gestion des droits d'accès et de publication selon le profil de l'utilisateur (auteur, publisher, admin…) ;
- gestion de la chaîne de publication (workflow) pour l'approbation et la publication du contenu ;
- gestion des différentes versions ;
- historique des modifications selon la date et l'auteur ;
- possibilité de gérer différents formats de publication (JSON, XML, HTML…).

En pratique

Dépendances, recommandations & avertissements

Il est préférable que l'application ou le site web dispose de sa propre mémoire cache afin de :

- disposer d'un scénario de fall back en cas d'indisponibilité du CMS ;
- de ne pas avoir à faire appel au CMS à chaque requête (éviter les reports de charge), par exemple en ne faisant appel au CMS qu'au maximum une fois toutes les minutes.

Quelles sont les conditions d'intégration du service au sein de la plate-forme eHealth ?

Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth en détaillant clairement le contexte de votre projet.

4. Timestamping

Qu'est-ce que le timestamping ?

La plate-forme eHealth offre un service de timestamping (datation électronique ou horodatage certifié) à ses partenaires.

Le timestamping est un système qui permet de conserver la preuve de l'existence d'un document et de son contenu à une date donnée. Le terme « preuve » indique le fait que personne, pas même le propriétaire du document, ne peut modifier le certificat de timestamping.

Quelles sont les fonctionnalités du timestamping ?

Ce service propose plusieurs fonctionnalités :

- un service web d'horodatage classique (TimeStampAuthority) qui procède à la certification du document et, si besoin, à son archivage (facultatif) ;
- un service web de consultation (TimeStampConsult) des documents horodatés qui assure le contrôle des documents horodatés au cours d'une période donnée.

En pratique

Dépendances, recommandations & avertissements

Le service de timestamping de la plate-forme eHealth est aujourd'hui utilisé dans le cadre de :

- la prescription électronique dans les hôpitaux (majoritairement) ;
- la prescription électronique ambulatoire (Recip-e) ;
- MyCareNet ;
- RCT.

Quelles sont les conditions d'intégration du service Timestamping de la plate-forme eHealth ?

- Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, Valérie Forton, en détaillant clairement le contexte et la finalité de votre projet ;
- à cette issue, si accord, disposer d'un certificat eHealth.

Prescription électronique dans les hôpitaux - Cadre spécifique

Concrètement, un médecin hospitalier émet une prescription électronique (le document à certifier), laquelle est envoyée à la pharmacie de son hôpital. Cette prescription est « hachée », c'est-à-dire qu'elle est transformée en un code chiffré unique n'ayant aucune signification logique.

Toutes les 5 minutes, les codes chiffrés sont rassemblés au sein d'un package appelé « TimeStampBag ». Ce package est envoyé à la plate-forme eHealth afin que son service de « Timestamping » puisse y apposer une date et une heure précises. Muni de sa datation, ce « package » est alors renvoyé à l'hôpital pour conservation au sein de ses archives. Quant à la plate-forme eHealth, elle conserve une copie du « package » et de sa datation. En d'autres termes, la plate-forme eHealth fournit la preuve que des prescriptions électroniques ont été créées à une heure et une date précises sans pouvoir connaître leur contenu puisqu'elles sont codées. En cas de contrôle, on applique à nouveau le système de haching sur la prescription. Le code obtenu est comparé avec celui stocké au sein de la plate-forme eHealth. Si les codes sont identiques, cela signifie que la prescription n'a pas été modifiée.

Comment un hôpital peut-il utiliser la datation des prescriptions électroniques ?

- La plate-forme eHealth met, à la disposition des hôpitaux, un outil nommé TimeStamping Client et faisant office d'implémentation de référence.
- La documentation détaillant l'installation et le fonctionnement de cet outil se trouve ci dessous.
- Néanmoins, l'hôpital qui le souhaite peut développer sa propre solution ou installer celle proposée par un fournisseur de logiciel du moment que celle-ci suit les mêmes spécifications que l'implémentation de référence.
- Dans tous les cas, cette solution devra interagir avec la plate-forme eHealth via les services TimeStamping Authority et TimeStamping Consultation afin d'horodater les prescriptions et d'effectuer des vérifications entre les archives de l'hôpital et les archives de la plate-forme eHealth.

Conditions légales à l'utilisation du service Timestamping

En ce qui concerne le timestamping et les prescriptions hospitalières, l'utilisation de ce service est réglée par la loi (voir le règlement du 5 décembre 2016 relatif à la prescription électronique intra hospitalière).

Pour plus d'information, contactez support@ehealth.fgov.be.

5. Répertoire des références (Metahub)

Qu'est-ce que le service « Répertoire des références » (Metahub) ?

Le service « Metahub » de la plate-forme eHealth constitue , avec les services annexes « Consent », « Therlink » et « Exclusions », un ensemble de services permettant de gérer l'accès aux données médicales d'un patient. Ces services sont accessibles, selon les cas, aux hubs, aux prestataires de soins individuels, à certaines institutions de soins comme les hôpitaux ou les pharmacies et enfin aux patients.

Il s'agit donc, en d'autres termes, d'un index des données personnelles relatives à la santé des patients.

Un tel index est la clef de voûte de la mise en place de tout système décentralisé de partage de données de santé entre prestataires et établissements de soins.

À cet égard, il est important de noter que le répertoire des références est composé de 2 « couches » principales.

- Une première couche se situe au niveau de la plate-forme eHealth, dénommée « Metahub », qui indique que des informations sont disponibles dans :
    - un réseau local ou régional, dénommé « hub » ou
    - dans la mesure où il n'y a pas de connexion à un hub, dans un coffre-fort de santé.
- Une deuxième couche se situe au niveau des hubs. Chaque hub tient un répertoire des références dans lequel il est indiqué auprès de quel établissement de soins ou de quel autre réseau d'échange connecté au hub une donnée de santé relative à un patient est disponible.

Les concepts suivants sont utilisés par les services liés au service « Metahub » et permettent la gestion de l'accès aux données médicales du patient :

- le « patientlink » ou le lien entre un hub et un patient permet de connaitre dans quel(s) hub(s) il est possible de consulter des données sur le patient :
    - l'ensemble des « patientlinks » constitue le Répertoire des références ;

- le consentement du patient au partage de ses données de santé :
    - aucun accès n'est donné aux données d'un patient en l'absence de son consentement ;
- la relation thérapeutique entre un patient et un prestataire de soins (AR.78) :
    - il s'agit d'une relation de soins établie (par exemple le fait de consulter un médecin généraliste),
    - aucun accès aux données du patient n'est autorisé au prestataire en l'absence de lien thérapeutique, sauf en cas d'urgence selon une procédure dite « breaking the glass » ;
- la relation de soins entre un patient et un prestataire de soins/une organisation de soins (hors AR.78) ;
- l'exclusion d'un prestataire de soins/une organisation de soins par un patient :
    - aucun accès aux données du patient n'est autorisé au prestataire/à une organisation de soins si une exclusion est enregistrée (même si une relation thérapeutique/de soins est enregistrée).

Citons, en particulier, 5 règles fondamentales :

- le partage des documents référencés via le Répertoire des références n'est possible que si le patient a donné son consentement ;
- la consultation d'une référence par un prestataire/organisation requiert l'existence d'une « relation thérapeutique ou de soins » entre ce prestataire/son organisation et le patient concerné ;
- le patient dispose à tout moment de la possibilité de révoquer :
    - son consentement sur l'échange de données de santé,
    - une ou plusieurs relations de soins/de santé préalablement enregistrées ;
- le patient dispose à tout moment de la possibilité d'exclure un prestataire de soins/une organisation de soins de l'accès à ses propres données ;
- le partage des données référencées ne peut se faire que sur base de la matrice d'accès (cf. page Règlements principaux).

Les services liés au « Metahub » sont disponibles comme services web (accessibles via un logiciel médical ou via une application tierce) et pour certaines fonctionnalités disponibles pour le patient, comme application web (accessible via un ordinateur et une eID, ITSME ou TOTP).

Quelles sont les fonctionnalités des services liés au service « Metahub » ?

Le service web « Metahub » est accessible aux hubs uniquement et offre les fonctionnalités suivantes :

- la création ou suppression des liens entre le hub et les patients qui y sont connus (« patientlinks ») permettant le fonctionnement des répertoires de références pour l'accès aux données des patients ;
- la consultation de ces « patientlinks » dans le cadre des répertoires des références pour l'accès aux données des patients ;
- la déclaration, révocation ou consultation du consentement du patient à l'échange de ses données de santé ;
- la déclaration, révocation ou consultation de relations thérapeutique/de soins entre un patient et un prestataire de soins/une organisation de soins (AR 78/hors AR 78) ;
- la déclaration, révocation ou consultation d'exclusions entre un patient et un prestataire de soins/une organisation de soins (AR 78/hors AR 78) ;
- la consultation de l'historique des activités liées au patient au sein du service « Metahub ».

Le service web de gestion du consentement est accessible aux patients (ainsi que leurs mandataires ou leurs parents), aux prestataires individuels, aux hôpitaux et offre les fonctionnalités suivantes :

- la déclaration, révocation ou consultation du consentement du patient au partage de ses données de santé.

Le service web de gestion des relations thérapeutiques/de soins est accessible aux patients (ainsi que leurs mandataires ou leurs parents), aux prestataires individuels/organisations de soins et offre les fonctionnalités suivantes :

- la déclaration, révocation ou consultation de liens thérapeutiques entre un patient et un prestataire de soins ou une pharmacie.

Le service web de gestion des exclusions thérapeutiques est accessible aux patients (ainsi que leurs mandataires ou leurs parents) et offre les fonctionnalités suivantes :

- la déclaration, révocation ou consultation d'exclusions entre un patient et un prestataire de soins/une organisation de soins.

L'application web de gestion du consentement du patient au partage de ses données de santé, des relations thérapeutiques/de soins et des exclusions est accessible aux patients via le portail MaSanté et offre les fonctionnalités suivantes :

- la déclaration, révocation ou consultation du consentement du patient au partage de ses données de santé ;
- la déclaration, révocation ou consultation de relations thérapeutiques/de soins entre un patient et un prestataire de soins/une organisation de soins ;
- la déclaration, révocation ou consultation d'exclusions entre un patient et un prestataire de soins/une organisation de soins ;

- la recherche d'un prestataire de soins sur base de son nom, prénom ou numéro INAMI afin d'enregistrer une relation thérapeutique/de soins ou une exclusion ;
- la recherche d'une organisation de soins sur base de son nom, adresse ou numéro INAMI afin d'enregistrer une relation thérapeutique/de soins ou une exclusion.

En pratique

Dépendances, recommandations & avertissements

Pour utiliser le service web de gestion du consentement du patient au partage de ses données de santé, le service web de gestion des liens thérapeutiques/de soins et le service web de gestion des exclusions sous forme de service web, le prestataire de soins/l'organisation ou le patient devra disposer d'un logiciel médical ayant intégré ce service.

Le service web de gestion du consentement du patient au partage de ses données de santé, le service web de gestion des relations thérapeutiques/de soins et le service web de gestion des exclusions sont disponibles en tant que services REST, facilitant l'intégration dans des applications (web ou mobile) tierces.

Le service web « Metahub » n'est accessible qu'aux hubs reconnus par la plate-forme eHealth et doit donc être intégré dans la solution informatique du hub.

La définition des principes, des fonctionnalités et de l'architecture du Répertoire des références et la relation avec les divers systèmes de santé qui y sont connectés s'effectuent sous l'égide de divers groupes de travail institués par le Comité de concertation avec les utilisateurs de la plate-forme eHealth.

Il est important de noter qu'une procédure spécifique d'approbation est d'application (Comité des utilisateurs, Comité de gestion et Comité de sécurité de l'Information).

Les textes légaux relatifs à cette matière sont disponibles sur la page Règlements principaux.

En ce qui concerne la réalisation, la maintenance et la gestion opérationnelle des différents composants du Répertoire des références, elles sont réparties entre les différents partenaires actifs du projet : la plate-forme eHealth se charge de la partie « Metahub » tandis que les organisations de prestataires de soins et d'établissements de soins ainsi que les autres instances concernées sont chacune responsables de leur « hub » ou système de santé.

Quelles sont les conditions d'intégration du service « Metahub » de la plate-forme eHealth ?

Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, Peter Laridon, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.

Afin de faciliter l'intégration de l'appel aux services web de gestion du consentement et de gestion des liens thérapeutiques, la plate-forme eHealth met à la disposition des acteurs des soins de santé des « connecteurs ».

Pour plus d'information, contactez support@ehealth.fgov.be.

6. Pseudonymisation & Anonymisation

Dans l'Union européenne et à fortiori en Belgique, l'échange de données de santé est strictement réglementée et encadrée par la Loi Vie privée. Dans ce cadre, il est impératif d'obtenir du Comité de sécurité de l'information une autorisation avant de procéder à toute utilisation ou échange de données de santé. Selon les besoins, le CSI imposera le niveau de sécurisation estimé comme adéquat.

A cet égard, la plate-forme eHealth met, à la disposition de ses partenaires, différents services permettant de veiller à ce que les données personnelles de santé soient converties en données codées ou anonymes qui ne permettent pas d'induire directement ou indirectement l'identité du patient et/ou du prestataire de soins.

Pseudonymisation

La pseudonymisation consiste à modifier, de manière réversible, le contenu ou la structure de données de santé afin de rendre impossible l'identification des personnes propriétaires de ces données.

Plusieurs services sont disponibles à cet égard.

1. La pseudonymisation « WS SEALS » qui offre, via l'intégration d'un service web appelé WS Seals, les fonctionnalités suivantes :
    - « Encode » qui permet de soumettre des données en input et de retourner en output ces données encodées ;
    - « Decode » qui permet de soumettre des données encodées en input et de retourner en output les données en clair (décodées).
2. La pseudonymisation « Batch codage » où la plate-forme eHealth assure un rôle de tiers de confiance (TTP –Trusted Third-Party) dans le processus de codage et de décodage des données de santé pour le compte du partenaire.
3. La pseudonymisation « Blinded pseudo » (service dérivé) :
    - elle offre la possibilité d'ajuster les pseudonymes en fonction de la partie qui traite les données, sans dé-pseudonymiser ces données, de sorte que l'identité d'une personne concernée reste protégée ;
    - il ne s'agit pas à proprement parlé d'un service de base mais bien d'un service dérivé qui rencontre néanmoins les mêmes standards de qualité et de sécurité que les services de base décrits dans la loi eHealth;

- certains services dits "Blinded pseudo-compatibles" peuvent intégrer cette catégorie de pseudonymisation

Anonymisation

L'anonymisation est le terme utilisé par la plate-forme eHealth pour désigner l'opération qui consiste à modifier le contenu ou la structure de données afin de rendre impossible l'identification des personnes propriétaires des données. L'anonymisation est irréversible et nécessite l'intervention d'un TTP.

En pratique

Quelles sont les conditions d'intégration ?

- Il est obligatoire de disposer d'un accord du Comité de sécurité de l'information.
- Prendre contact avec le responsable du service au sein de la plate-forme eHealth, en détaillant clairement le contexte et la finalité de votre projet. Il est à noter qu'il est obligatoire de disposer d'un accord du Comité de sécurité de l'information :
  - pour le service pseudonymisation « WS SEALS » > nicolas.donnez@ehealth.fgov.be ;
  - pour le service de pseudonymisation « Batch codage » > wolf.wauters@health.fgov.be ;
  - pour le service dérivé de pseudonymisation « Blinded Pseudo » > pseudo@ehealth.fgov.be ;
  - pour le service d'anonymisation > nicolas.donnez@ehealth.fgov.be ;
  - pour toute question complémentaire > TTP@ehealth.fgov.be.
- A cette issue, si accord, disposer d'un certificat eHealth et prévoir l'intégration d'un service d'encryption.

7. Système de cryptage end-to-end

Que sont les services End-to-End Encryption de la plate-forme eHealth ?

Les services End-to-End Encryption (ETEE) (également appelés services de chiffrement ou de cryptage) de la plate-forme eHealth sont un ensemble de services permettant de chiffrer des messages à destination de prestataires de soins (individuels ou institutions). Ces services sont accessibles aux prestataires de soins individuels et aux institutions et, dans certains cas, aux patients.

Les services de chiffrement sont utilisés, entre autres, dans le cadre de l'utilisation du service eHealthBox ou de prescriptions électroniques (Recip-e).

Les services ETEE sont les suivants :

- ETKDepot (SOAP & REST) et KeyDepot (REST) pour le chiffrement vers un destinataire connu ;
- KGSS (SOAP & REST) pour le chiffrement vers un destinataire inconnu.

Les services ETEE sont disponibles comme services web (accessibles via un logiciel médical ou via une application tierce).

Quelles sont les fonctionnalités des services End-to-End Encryption ?

Le service web ETKDepot est accessible à tous les publics et offre les fonctionnalités suivantes :

- la recherche d'un ETK, qui est la clé publique associée au certificat eHealth d'un prestataire de soins ou d'une institution dont les identifiants (NISS, numéro INAMI, numéro BCE) sont connus. Le service REST permet également de rechercher le détenteur d'un certificat ;
- une fois obtenu, cet ETK permettra de chiffrer un message pour un destinataire connu (le prestataire de soin ou l'institution).

Le service web KGSS (Key Generation and Storage System) est accessible à tous les publics et offre les fonctionnalités suivantes :

- la création d'une clé de chiffrement symétrique qui sera stockée par la plate-forme eHealth et sera accessible sous certaines conditions définies par le créateur de la clé ;
- la récupération d'une clé existante, à condition de connaitre l'identifiant de la clé et de satisfaire aux conditions d'accès définies lors de la création de la clé (exemple : être authentifié en tant que pharmacie reconnue par la plate-forme eHealth) ;
- le service REST permet également de supprimer une clé existante par son détenteur.

Ces fonctionnalités permettent d'utiliser le service KGSS lorsque l'identité du destinataire du message chiffré n'est pas connue à l'avance, mais que certaines conditions doivent être remplies pour l'obtention de la clé de chiffrement.

Le service web KeyDepot est accessible à tous les publics et offre les fonctionnalités suivantes :

- la création d'une paire de clés (la clé publique sera stockée par la plate-forme eHealth et sera accessible à tous les publics) ;
- l'ajout, par son détenteur, d'informations pour une clé publique déjà existante ;
- la recherche d'une clé publique ;

- la suppression, par son détenteur, de clés publiques ;
- la recherche de toutes les clés publiques liées à une personne ;
- la recherche de l'attestation object liée à une clé publique ;
- la recherche d'informations sur le détenteur d'une clé.

En pratique

Dépendances, recommandations & avertissements

Pour utiliser le service web ETKDepot, le service web KGSS ou le service web KeyDepot, le prestataire de soins ou le patient devra disposer d'un logiciel médical ayant intégré ce service. Les deux services web KGSS et ETKDepot sont également intégrés au sein de solutions plus globales comme Recip-e, Chapitre IV, eHealthBox.

Afin de faciliter vos opérations de cryptage, une librairie technique est mise à votre disposition.

Quelles sont les conditions d'intégration des services End-to-End Encryption de la plate-forme eHealth ?

Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, Kris Van Aken, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.

Pour plus d'information, contactez support@ehealth.fgov.be.

8. eHealthBox

Qu'est-ce que le service eHealthBox ?

Le service eHealthBox de la plate-forme eHealth est une boîte aux lettres électronique sécurisée, développée spécifiquement pour les prestataires de soins et les institutions. Son objectif est d'assurer une communication électronique sécurisée des données médicales et confidentielles utiles entre les acteurs des soins de santé belges.
Le service eHealthBox est disponible comme service web (accessible via un logiciel médical) et comme application web (accessible via un ordinateur et une eID/ITSME ou TOTP).

Quelles sont les fonctionnalités du service eHealthBox ?

Le service eHealthBox offre les fonctionnalités suivantes.

- Sous forme d'application web, un package comprend :

- un service de consultation des messages ;
- un service de publication des messages ;
- le service « eHealth update info », qui est une application permettant d'être averti, via une adresse mail (par exemple l'adresse d'une simple messagerie web choisie par le prestataire de soins), de l'arrivée de nouveaux messages dans l'eHealthBox ;
- un service qui permet de consulter les informations générales relatives à la capacité de sa messagerie (taille actuelle, taille maximale autorisée, nombre de messages non reçus lorsque la boîte est pleine…) ;
- un service de notification qui offre un aperçu du statut des accusés de réception et/ou de lecture des messages ;
- la possibilité d'organiser, de déplacer les messages dans les différents dossiers.

- Sous forme de service web, un package comprend :
  - un service de publication qui permet d'envoyer des messages et inclut :
    - un service « out of office » qui permet de référencer un prestataire de soins remplaçant,
    - une fonctionnalité de messagerie groupée qui permet d'envoyer un ou plusieurs messages à un groupe de prestataires (par exemple un message à l'ensemble du personnel infirmier d'un hôpital),
    - un service d'encryption qui permet de garantir l'intégrité des données transmises,
    - la possibilité d'envoyer des pièces jointes (la taille du message ne peut dépasser 10 MB),
    - la possibilité d'envoyer des messages de type « news » qui sont des messages que l'on peut mettre à jour de manière illimitée ;
  - un service de consultation des messages qui comprend :
    - un service qui permet de consulter les informations générales relatives à la capacité de sa messagerie (taille actuelle, taille maximale autorisée, nombre de messages non reçus lorsque la boîte est pleine…),
    - un service de notification qui offre un aperçu du statut des accusés de réception et/ou de lecture des messages,
    - un service permettant de consulter un récapitulatif des messages (triés selon la date),
    - la possibilité de consulter simultanément plusieurs messageries (par exemple la messagerie d'un prestataire de soins en sa qualité de prestataire privé simultanément avec sa messagerie en sa qualité de prestataire au sein d'un hôpital),
    - la possibilité d'organiser, de déplacer les messages dans les différents dossiers ;

- un service dénommé « eHealth Addressbook » qui permet de :
  - rechercher un prestataire de soins sur base de :
    - son numéro de registre national (et optionnellement sa profession),
    - son numéro INAMI (et optionnellement sa profession),
    - sa profession et son nom (et optionnellement son prénom),
    - sa profession et son code postal,
    - sa profession et sa ville,
    - son adresse mail ;
  - rechercher une institution de soins sur base de :
    - son numéro EHP (et optionnellement le type de l'institution),
    - son numéro INAMI (et optionnellement le type de l'institution),
    - son numéro d'entreprise BCE (et optionnellement le type de l'institution),
    - son nom et son type d'institution,
    - son type d'institution et son code postal,
    - son type d'institution et sa ville ;
  - consulter les données de contact les plus actuelles (enregistrées dans les sources authentiques) d'un acteur de soins de santé ou d'une institution de soins :
    - pour un acteur de soins de santé : numéro de registre national / nom / prénom(s) / langue / genre / date de naissance / date de décès éventuelle / adresse postale / informations de contact / numéro INAMI / nom de la profession / code de la profession / nom de la spécialisation / code de la spécialisation / adresse(s) professionnelle(s) / eHealthBox,
    - pour une institution de soins : identifiant (avec son type EHP/CBE/NIHII) de l'institution / description de l'institution / type d'institution / nom / adresses / autres informations de contacts / eHealthBox,
    - les données eHeathBox retournées contiennent l'identifiant de la boîte et le type d'identifiant (NISS, NIHI, CBE), éventuellement le sous-type (hôpital par exemple), ainsi que la qualité de l'acteur de soins de santé ou de l'institution.

En pratique

Dépendances, recommandations et avertissements

Le service eHealthBox a été développé à l'attention des institutions de soins et des prestataires de soins détenteurs d'un numéro INAMI.

Pour utiliser eHealthBox sous forme d'application web, le prestataire de soins devra se connecter sur l'application via un ordinateur, avec une eID, ITSME ou un TOTP. Il est également essentiel d'utiliser un navigateur web (browser) testé par la plate-forme eHealth .

Pour utiliser eHealthBox, sous forme de service web, le prestataire de soins devra disposer d'un logiciel médical ayant intégré ce service (ce qui est le cas de l'ensemble des logiciels enregistrés par la plate-forme eHealth).

Quelles sont les conditions d'intégration du service eHealthBox de la plate-forme eHealth ?

- Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, Wolf Wauters, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet ;
- à cette issue, si accord, disposer d'un certificat eHealth et prévoir l'intégration d'un service d'encryption.

Afin de faciliter l'intégration de l'appel au service web de publication et de consultation de l'eHealthBox, la plate-forme eHealth met à la disposition des acteurs des soins de santé des connecteurs.

Pour plus d'information, contactez support@ehealth.fgov.be.

9. RN Consult

Qu'est-ce que RN Consult ?

RN Consult regroupe un ensemble de services qui permet de rechercher et consulter des données d'une personne dans le Registre national et les registres de la Banque Carrefour.

Ces services sont accessibles aux institutions et aux professionnels de la santé (reconnus par l'arrêté royal AR78), qui ont obtenu au préalable l'autorisation du Comité de sécurité de l'information (CSI, anciennement le Comité sectoriel de la sécurité sociale et de la santé).

Les autorisations obtenues par le passé auprès du Comité sectoriel du Registre national ou du Comité sectoriel de la sécurité sociale et de la santé restent valables.

Ces autorisations sont obtenues en fonction :

- du type d'institution et/ou des prestations réalisées (hôpitaux, laboratoires agréés, médecins généralistes) ;
- de la finalité de la demande (ex. : vérification et actualisation des données d'identification des patients dans le dossier médical…) ;

- du type de données auxquelles l'accès est demandé (nom, date de naissance, sexe, résidence…).

Pour le détail des délibérations, nous vous invitons à consulter l'onglet « Comité de sécurité de l'information ».

Quels sont les services proposés par RN Consult ?

Important : chaque utilisateur reçoit uniquement un accès aux données pour lesquelles une autorisation juridique préalable a été obtenue.

PersonService

Consultation des données d'identification d'une personne :

- sur base du NISS ou NISS BIS ;
- sur base de critères phonétiques.

CBSSPersonService

Création d'un NISS/NISS BIS par les instances autorisées.

PersonInfoService

Consultation de l'historique de certaines données du Registre national et des registres de la BCSS sur base du NISS/NISS BIS d'un patient.

InscriptionService

Gestion par les organisations/institutions de l'inscription d'un patient au service d'abonnement des mutations. Pour une utilisation optimale, il est nécessaire d'implémenter également l'application PersonNotificationService.

PersonNotificationService

Gestion des mutations (recherche et suppression) par une instance autorisée.

SSINHistory

Affichage de la liste des identifiants uniques (NISS/NISS BIS) qu'une personne possède ou a possédés. Ce service est utilisé dans le cadre de la création d'un NISS/NISS BIS.

Qui a accès à RN Consult ?

Institutions déjà autorisées en vertu de délibérations générales à utiliser ces services

- Hôpitaux
- Laboratoires agréés de biologie clinique
- Laboratoires agréés d'anatomie pathologique
- Maisons de repos ou maisons de soins agréées
- Maisons de soins psychiatriques ou initiatives d'habitation protégée

Professionnels des soins de santé autorisés (AR78)

Les professionnels des soins de santé ont été autorisés sur le plan juridique à utiliser le numéro de Registre national dans le cadre de l'utilisation des applications utilisant les services de base de la plate-forme eHealth et à enregistrer à cette fin le numéro de Registre national dans leur dossier. Dans un premier temps, cette possibilité est offerte aux médecins généralistes.

Autres organisations

D'autres organisations ayant introduit un dossier justifiant la finalité et la proportionnalité ont également reçu une délibération spécifique.

Afin d'obtenir des informations complémentaires ou en vue de l'obtention de toute nouvelle délibération, nous vous invitons à contacter la plate-forme eHealth : RRNConsult@ehealth.fgov.be.

Comment accéder à RN Consult ?

Pour utiliser les services eHealth RN Consult, l'institution ou le prestataire de soins devra disposer d'un certificat eHealth et d'un logiciel médical qui aura intégré ce service.

Procédure d'intégration pour hôpital, laboratoire agréé, maison de soins psychiatriques, initiative d'habitation protégée, maison de repos et de soins

Voir les formulaires en bas de page.

Etape 1 : Les instances visées ci-dessus souhaitant intégrer le service web au sein d'une de leurs applications doivent tout d'abord transmettre (de préférence par mail) les documents énumérés ci-après à :

Comité de sécurité de l'information, chambre sécurité sociale et santé

Madame Joke Vanderpoorten

Quai de Willebroeck, 38 à 1000 Bruxelles

ivc@mail.fgov.be

1. un engagement par lequel l'institution déclare respecter les conditions décrites dans la délibération. Vous devez choisir le formulaire adéquat en fonction du type de votre institution :
    - hôpital,
    - laboratoire agréé de biologie,
    - laboratoire agréé d'anatomie pathologique,
    - maison de soins psychiatriques ou initiative d'habitation protégée,
    - maison de repos ou maison de soins ;
2. un acte d'agrément de votre institution (preuve du statut ou de l'agrément) ;
3. un formulaire d'évaluation/information du « Data Protection Officer » (DPO) de votre organisation ;
4. un formulaire de déclaration de conformité portant sur les mesures de référence en matière de sécurité ;
5. une demande d'autorisation d'utilisation des services web eHealth.

Etape 2 : Le Comité de sécurité de l'information, chambre sécurité sociale et santé, vous communiquera sa décision et, en cas d'accord, vous octroiera un Acceptation Application ID. Il informera en même temps le Registre national.

Etape 3 : Vous pouvez ensuite entamer la partie technique et envoyer un rapport de test à integration-support@ehealth.fgov.be. Vous trouverez toutes les informations à ce sujet dans les cookbooks figurant sur cette page.

Etape 4 : Après la validation du rapport de test, la plate-forme eHealth fera le nécessaire afin de configurer vos accès en production. A cette fin, vous recevrez un Production Application ID.

Procédure spécifique « Circle of Trust » (CoT)

Voir les formulaires et les documents informatifs en bas de page.

Les laboratoires agréés de biologie clinique et les hôpitaux qui ont rempli le formulaire « Circle of Trust » (CoT) doivent suivre la procédure suivante :

1. compléter la déclaration CoT et la renvoyer à votre institution de tutelle (voir également les explications concernant cette déclaration sur l'honneur) ;
2. compléter le formulaire de demande d'utilisation des services web RN Consult eHealth en vue de l'attribution des numéros BIS ;

3. respecter les normes minimales de sécurité ;
4. respecter les pratiques professionnelles à implémenter par les laboratoires CoT et les hôpitaux CoT pour la création des numéros BIS ;
5. demander des cas de test à l'équipe de support (integration-support@ehealth.fgov.be) et leur envoyer le rapport de test .

Après validation de vos tests, vous recevrez un Application ID de production pour un accès en production.

Dans le cadre de la crise sanitaire, les laboratoires agréés de biologie clinique et les hôpitaux qui sont déjà abonnés au service RN Consult peuvent faire également appel au service web permettant de créer à certaines conditions des numéros BIS.

Votre institution ne relève pas des catégories mentionnées ci-dessus

Dans ce cas, nous vous invitons à prendre contact avec la plate-forme eHealth (RRNConsult@ehealth.fgov.be) et à lui soumettre le contexte, la base légale, la finalité de votre demande ainsi qu'une estimation du volume de votre projet.

Nous examinerons votre demande et vérifierons si vous disposez d'une autorisation juridique pour le Registre national et les registres BCSS.

Une fois les autorisations obtenues, il vous sera demandé de compléter le formulaire de demande d'utilisation des services web et de le renvoyer par mail.

Ensuite, l'Acceptation Application ID qui vous permettra d'entamer la partie technique vous sera transmis. Après validation de votre rapport de test, la plate-forme eHealth fera le nécessaire pour configurer vos accès en production.

Remarque : Si le DPO de votre institution n'est pas encore connu auprès de la plate-forme eHealth, vous devez nous envoyer le formulaire d'évaluation de votre DPO.

Points importants

- Si votre organisation évolue sur le plan juridique ou administratif (fusion, retrait d'agrément...) ou en cas de changement de DPO, il vous est demandé de directement prendre contact avec la plate-forme eHealth. Ces évolutions peuvent en effet avoir des conséquences tant sur le plan juridique que sur le plan technique (par exemple pour ce qui concerne l'accès aux services de la plate-forme eHealth au moyen des certificats eHealth).
- Pour les médecins : dans le cadre de la continuité des soins médicaux, les médecins ayant un visa actif mais qui ne possèdent pas de logiciel peuvent avoir recours à l'application web eHealthCreaBis pour être en capacité de créer des numéros BIS.
- Pour tout renseignement complémentaire relatif à l'utilisation de ce service, nous restons à votre disposition via l'adresse mail RRNConsult@ehealth.fgov.be.

10. I.AM (Identity & Access Management)

Qu'est-ce que le service « Gestion intégrée des utilisateurs et des accès » / I.AM (Identity & Access Management) ?

Le service « Gestion intégrée des utilisateurs et des accès de la plate-forme eHealth » a pour objectif de faciliter l'identification, l'authentification et l'autorisation d'acteurs de soins de santé.

Ce service est constitué de plusieurs composants qui travaillent ensemble pour permettre l'authentification (unique), l'autorisation et la propagation d'identité des utilisateurs de soins de santé, demandant l'accès aux services (hébergés par les organisations de soins de santé et la plate-forme eHealth).

Ces composants sont conformes aux normes internationales pour les communications interentreprises afin de garantir la sécurité et la stabilité et de faciliter l'intégration.

Quelles sont les fonctionnalités du service I.AM ?

Le service « Gestion intégrée des utilisateurs et des accès » offre les fonctionnalités suivantes :

- authentification de l'utilisateur :
  - via certificat eHealth,
  - via une clé numérique supportée par la plate-forme eHealth ;
- identification de l'utilisateur, choix de son profil selon :
  - sa qualité / le type de prestataire de soins individuels (sur base des informations contenues dans la base de données CoBRHA),
  - l'organisation au nom de laquelle il/elle peut agir,
  - le mandant pour lequel il/elle peut agir,
  - son/ses enfant(s) (sur base des données présentes au Registre national) ;
- authentification unique (single-sign-on) :
  - dans le cadre d'une application web, l'utilisateur ne devra pas se ré-authentifier (sauf si c'est explicitement demandé pour une application),
  - dans le cadre d'un service web, l'utilisateur se crée une session qui peut être utilisée dans le cadre de plusieurs services sur une durée déterminée (durée dépendant du profil de l'utilisateur) ;

Remarque : le single-sign-on IDP (voir document Identity Provider (IDP) renseignant les spécifications techniques) ne doit pas être confondu avec un comportement « isPassive » dans lequel les écrans de l'IDP proposés à l'utilisateur sont limités au strict minimum. Le « isPassive » est uniquement applicable entre les applications web supportant cette fonctionnalité. Cela permet notamment à l'utilisateur de sélectionner un profil dans une application et de ne plus devoir sélectionner de profil s'il passe vers une 2e application (supportant ce profil) protégée par notre I.AM IDP.

- délégation d'accès aux applications :
  - au sein d'une institution
    - il est possible de définir les utilisateurs qui peuvent agir au nom d'une institution pour certaines applications disponibles (voir la page Comment accéder aux applications ? du portail eSanté pour effectuer la délégation via UserManagement) ;
    - en complément de ces attributions d'application aux utilisateurs, il est possible de définir des fonctions au sein de cette institution (voir la page Comment accéder aux applications ? du portail eSanté pour effectuer la délégation via Management et Remaph). Cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des services web. Si elle l'est, le projet doit demander à utiliser IDP ;
    - si une personne travaillant dans l'institution peut agir au nom d'un autre utilisateur de cette institution, il est possible de définir un lien hiérarchique entre ces 2 personnes (voir la page Comment accéder aux applications ? du portail eSanté pour effectuer la délégation via Management et Remaph). Cette fonctionnalité ne peut en principe pas être utilisée dans le cadre des services web. Si elle l'est, le projet doit demander à avoir accès à IDP et AttributeAuthority (qui permet à nos partenaires d'interroger les sources authentiques eHealth). Ce système a été défini afin de scinder les accès applicatifs des accès aux données. L'application est responsable de l'affichage pour le subordonné de la liste de ses supérieurs hiérarchiques, après que ce subordonné a reçu l'autorisation d'accéder à l'application (depuis notre IDP) ;
  - d'une institution vers une autre institution (voir la page Comment accéder aux applications ? du portail eSanté pour effectuer la délégation via l'application web Mandats). Si les types de mandats présents dans l'application ne répondent pas aux attentes de l'application, il est nécessaire de demander la création d'un nouveau type de mandat par l'intermédiaire du chef de projet eHealth responsable ;
  - d'une personne physique à une autre personne physique (voir la page Comment accéder aux applications ? du portail eSanté pour effectuer la délégation via l'application web Mandats) ;
- accès aux données :

    - certaines données (adresse de contact d'un prestataire de soins, dénomination d'une institution, liste de responsables hiérarchiques d'un subordonné au sein d'une institution…) présentes dans nos sources authentiques (dont la base de données CoBRHA) sont accessibles via le service web I.AM AA (AttributeAuthority, qui permet à nos partenaires d'interroger les sources authentiques eHealth) ;
    - l'accès à ces données est sécurisé ;
- sécurisation d'application via un mécanisme d'autorisation basée sur l'identité de l'utilisateur.

En pratique

Dépendances, recommandations & avertissements

L'intégration de ce service de base est étroitement liée aux architectures proposées par la plate-forme eHealth.

Dans le cadre du développement d'une application web (server side), nous vous recommandons d'utiliser le logiciel Shibboleth SP pour faciliter l'intégration de votre application avec notre I.AM IDP.

Si votre système nécessite l'accès à certains services REST (Representational State Transfert) de la plate-forme eHealth, une intégration avec notre I.AM Connect devra être réalisée.

Si votre application doit être capable d'utiliser notre token eXchange, certaines règles sont à respecter et un contrat doit être signé.

Pour pouvoir utiliser I.AM STS et I.AM AA, l'eID de l'acteur de soins de santé ou un certificat délivré par la plate-forme eHealth est requis.

I.AM ne peut être utilisé que pour des acteurs de soins reconnus par la plate-forme eHealth.

Quelles sont les conditions d'intégration du service I.AM de la plate-forme eHealth ?

- Prendre contact avec le chef de projet responsable au sein de la plate-forme eHealth, eHealthppkb@ehealth.fgov.be, en détaillant clairement le contexte, la finalité ainsi qu'une estimation volumétrique de votre projet.
- A cette issue, si accord, fournir les documents nécessaires à la configuration des services souhaités :
    - CAB-I.AM / eDU à remplir en concertation avec votre chef de projet responsable au sein de la plate-forme eHealth ;
    - pour utiliser la fonctionnalité d'accès aux données :

        - obtenir un certificat eHealth par environnement souhaité,
        - compléter et soumettre le formulaire I.AM Registration, par environnement, en y mentionnant le certificat obtenu ;
    - pour utiliser I.AM Connect :
        - remplir le bon formulaire client en fonction du realm, formulaire Healthcare ou formulaire M2M ;
    - pour utiliser l'I.AM IDP :
        - compléter et soumettre le formulaire I.AM Registration, par environnement, en y mentionnant le certificat obtenu.

Afin de faciliter l'intégration de l'appel au service web STS, la plate-forme eHealth met à la disposition des acteurs des soins de santé des « connecteurs ».

Pour plus d'information, contactez support@ehealth.fgov.be.

Identity & Access management - Organisation technique

Introduction

Le système I.AM (Identity & Access Management) de la plate-forme eHealth intègre l'ensemble des services de base dont les fonctionnalités permettent d'assurer une gestion des accès, une gestion des utilisateurs et une gestion de l'accès aux données.

Selon les besoins applicatifs, il est possible de distinguer 4 contextes :

1. La sécurisation de Web App
2. La sécurisation de services web « Simple Object Access Protocol » (SOAP)
3. La sécurisation de services web « Representational State Transfert » (REST)
4. Le Data Access

L'authentification et l'autorisation sont des aspects importants pour chacun de ces contextes.

La sécurisation de Web App

Pour accéder à une application de type Web App sécurisée, il faut s'authentifier et obtenir une autorisation :

- pour les applications web classiques (typiquement des applications server-side HTML), via le composant « I.AM IDP » ;
- pour les applications web mobiles (applications utilisant du JavaScript pour appeler des services REST par exemple) ou applications natives, via le composant « I.AM Connect ».

Dans tous les cas, le système offre la possibilité aux utilisateurs d'avoir du « single sign-on » qui permet de s'identifier une seule fois pour accéder à plusieurs applications différentes.

Dans le cas d'applications web classiques, la gestion des autorisations est effectuée par notre IDP (Identity Provider), via User & Acces Management (UAM).

Dans le cas d'applications web mobiles, la gestion des autorisations est effectuée par les différents services appelés.

Documentation utile pour les applications web classiques :

- I.AM overview
- I.AM federation metadata
- I.AM IDP (Identity Provider)
- I.AM federation attributes
- I.AM logout
- I.AM SP Shibboleth
- I.AM SP Shibboleth upgrade
- I.AM registration
- UAM (User Access Management)
- Gestion intégrée des utilisateurs et des accès SLA

Documentation utile pour les applications web mobiles ou applications natives :

- I.AM Connect - Mobile integration - Technical specifications.

La sécurisation de services web SOAP

SOAP (Simple Object Access Protocol) est un protocole orienté « objet » qui permet la transmission de messages structurés (format XML dans une Enveloppe SOAP) entre un WSC (Web Service Consumer) et un WSP (Web Service Provider).

Ce protocole est notamment utilisé dans le cadre d'architectures de type SOA (Service Oriented Architecture).

L'authentification des WSC s'effectue via le service « I.AM STS » (Secure Token Service) au moyen d'un certificat eHealth ou d'une carte d'identité électronique (eID). L'assertion obtenue par le WSC est ensuite évaluée dans le cadre de l'autorisation.

L'autorisation est principalement effectuée, pour chaque service appelé, par le service Bus de la plate-forme eHealth sur base de règles préalablement définies. Pour chaque service SOAP disponible et protégé sur l'Enterprise Service Bus (ESB) de la plate-forme eHealth, les règles d'accès définies sont évaluées afin d'autoriser ou non l'accès au service.

Il est également possible, pour un utilisateur, de basculer d'une authentification/autorisation de type Web Service, vers une authentification/autorisation de type Web App, via le service « I.AM STS to IDP ».

Documentation utile :

- Certificat eHealth
- I.AM STS
- Coordination de processus
- Sécurisation des services web

La sécurisation de services web REST

Les services web REST (Representational State Transfert) sont utilisés dans le cadre d'architecture de type REST. Cette architecture se repose sur le protocole HTTP via ces différentes opérations : GET, POST, PUT, DELETE.

Le format des messages échangés ici n'est plus du XML mais du JSON.

Ce type de services s'adresse plus particulièrement aux applications mobiles.

L'authentification et l'autorisation des clients s'effectuent via le service « I.AM Connect » qui se base sur le standard OIDC (OpenID Connect).

I.AM Connect permet, entre autres, de délivrer un « Access token » au client qui peut l'envoyer ensuite vers le service REST.

Le service REST vérifie alors le contenu de cet « Access token » afin de traiter les contraintes de sécurité préalablement établies.

Documentation utile :

- I.AM Connect - Mobile integration - Technical specifications

Le Data Access

Ce système fait appel au composant « I.AM AA » dont la fonction est d'interroger différentes sources de données afin de vérifier si les conditions préétablies pour accéder aux données sont remplies et, le cas échéant, autoriser ou non l'accès.

I.AM AA (AttributeAuthority)

I.AM AA permet à nos partenaires d'interroger les sources authentiques eHealth. Ces sources contiennent des informations concernant les acteurs des soins de santé (CoBRHA), les mandats…

Ce système a été défini afin de scinder les accès applicatifs des accès aux données.

I.AM STS (Secure Token Service)

I.AM STS permet à un acteur de soins de santé de s'identifier via la génération d'un token (par opposition à l'identification par eID ou username). Il est dédié à l'identification pour les services web intégrés aux logiciels médecin et permet de s'identifier en tant que médecin, médecin spécialiste, infirmier, etc.

I.AM IDP (Identity Provider)

I.AM IDP est le service permettant de créer, de maintenir et de gérer les informations d'identité des utilisateurs pouvant s'authentifier dans un réseau distribué ou au sein d'une fédération.

Différentes méthodes d'authentification sont supportées par l'IDP afin de s'assurer que l'utilisateur puisse prouver qu'il est bien celui qu'il prétend être.

I.AM IDP permet de sécuriser l'accès aux applications web proposées et hostées par des fournisseurs de service (Service Providers) via UAM.

I.AM Connect

I.AM Connect est une solution de gestion d'identité et d'accès pour les applications web et les services web RESTful basée sur OIDC (OpenID Connect).

Elle permet aux clients de demander et recevoir des informations sur les sessions authentifiées et les utilisateurs finaux. I.AM Connect permet également aux clients de vérifier l'identité de l'utilisateur final en fonction de l'authentification effectuée par notre serveur d'autorisation.

Les clients de tous types sont pris en charge : clients d'applications web, clients JavaScript, applications natives (clients « mobile »).

Documentation utile :

- I.AM Connect - Mobile integration - Technical specifications

UAM

UAM = User & Access Management

L'UAM est utilisé dans le cadre de Web Apps classiques, de Web services via le service Bus de la plate-forme eHealth et permet d'autoriser ou non l'accès d'un utilisateur à une ressource protégée.

L'UAM fonctionne sur base du Policy Enforcement Model générique, comprenant le Policy Enforcement Point (PEP), le Policy Decision Point (PDP), le Policy Administration Point (PAP) et le Policy Information Points (PIP).

Plus d'information sur UAM.

Architectures

Dans le cadre du développement et de la maintenance de ses projets et services, la plate-forme eHealth propose différentes structures et organisations des systèmes informatiques, appelés ‘architectures’.

1. Architectures

1. Introduction

Dans le cadre du développement et de la maintenance de ses projets et services, la plate-forme eHealth propose différentes structures et organisations des systèmes informatiques, appelés « architectures ».

Ces modèles sont élaborés sur base des besoins des partenaires mais sont tenus de respecter certaines normes de qualité et de sécurité. Ils sont soumis à de constantes évolutions, en relation directe avec le secteur.

Lors du démarrage d'un projet, il importe donc de comprendre les différents systèmes proposés afin d'assurer une mise en place optimale des différents composants mais également d'anticiper les évolutions futures possibles.

La plate-forme eHealth propose principalement 2 types d'architectures :

- une architecture de type SOAP (Simple Object Access Protocol), destinée aux applications et services dont l'objectif est de fonctionner sur un seul dispositif, un seul ordinateur ;
- une architecture de type REST (Representational State Transfert), destinée aux applications et services dont l'objectif est de fonctionner sur plusieurs dispositifs (simultanément un ordinateur, un smartphone, une tablette...).

Comme mentionné préalablement, l'informatique est un domaine en constante évolution. Au démarrage de la plate-forme eHealth, l'utilisation de dispositifs mobiles tels que les tablettes et smartphones n'en était qu'à ses débuts, raison pour laquelle l'architecture de type SOAP a majoritairement été développée et structure aujourd'hui encore de nombreux systèmes mis en place avec nos partenaires. La maintenance et le support pour ce modèle demeurent aujourd'hui parmi nos missions et responsabilités. Néanmoins, parce qu'il n'est pas recommandé pour le développement de projets de type mobiles (il ne permet notamment pas l'encryption des messages), la priorité est logiquement donnée à la promotion de l'architecture de type REST.

2. Développement d’un projet dans le cadre de la santé en ligne : ce qu’il faut prévoir, comprendre et définir

2.1. Le projet doit intégrer des contraintes en matière d'identification et de gestion des accès

Afin de permettre l'accès mobile aux services eHealth, nous devons être en mesure d'authentifier TOUS les utilisateurs qui ont besoin d'utiliser les services de la plate-forme eHealth, quel que soit l'appareil ou le système utilisé pour se connecter.

Dans l’ensemble, nous distinguons deux catégories d’utilisateurs de nos services :

- les personnes (citoyens belges ou étrangers, professionnels, membres d'une organisation, mandataires) ;
- les systèmes.

Il doit être possible de construire une identité numérique pour chacun d'entre eux.

2.1.1. Enregistrement

Tous les utilisateurs doivent être enregistrés dans une source authentique accessible à la plate-forme eHealth (directement ou indirectement) :

- les personnes présentes dans le registre national avec un NISS pour citoyens belges ou NISS BIS pour étrangers (les groupes cibles de la plate-forme eHealth incluent les citoyens belges et les étrangers qui vivent ici ou à l’étranger) ;
- les systèmes doivent appartenir à une organisation qui peut être identifiée de manière univoque dans une source authentique pour le type spécifique d'organisation.

Tout utilisateur doit être en mesure de prouver son identité en ligne avec une clé numérique. Au moins une clé doit lui être remise lors de l'enregistrement.

2.1.2. Authentification

L'authentification doit être supportée pour tous les types de clients : web (navigateur), natif (application mobile), desktop, serveur (backend, batch).

Pour s'authentifier, l'utilisateur doit utiliser l'une de ses clés numériques pour prouver qu'il est bien celui qu'il prétend être. Le modèle d'identité fédérée de la plate-forme eHealth doit être réutilisable pour tous les utilisateurs.

Toutes les clés numériques doivent répondre à des exigences minimales de sécurité.

Une personne doit pouvoir utiliser plusieurs dispositifs pour s'authentifier vis-à-vis de nos services.

Une personne doit être en mesure de choisir un profil d'utilisateur applicable (c.-à-d. citoyen, qualité, appartenance à une organisation, mandat) qui sera utilisé pour l'authentification vis-à-vis de nos services.

Il doit être possible de transmettre l'identité choisie aux ressources demandées ou celles-ci doivent pouvoir la récupérer.

2.1.3. Autorisation

Les autorisations doivent être basées sur l'identité numérique choisie pour chacune des ressources demandées.

Il doit être possible de propager les autorisations aux ressources demandées ou celles-ci doivent pouvoir les obtenir.

Il doit être possible de laisser l'utilisateur décider s'il souhaite ou non donner des autorisations à l'application cliente qui utilisera ces autorisations en son nom.

Les utilisateurs doivent pouvoir révoquer les autorisations accordées.

2.2. Le projet doit intégrer des contraintes en matière d 'identification et de sécurité de l'information

2.2.1. Confidentialité

Toute communication entre le client et le serveur doit être considérée comme confidentielle et doit être protégée contre toute interception, au moins lorsqu'elle transite par un support non sécurisé comme Internet.

Les données médicales doivent être protégées au niveau du message afin d'empêcher la divulgation des données lorsqu'on passe d'un point à un autre sur le réseau. Si le cryptage de bout en bout entre l'expéditeur d'origine et le destinataire final n'est pas nécessaire, il doit au moins être configuré point à point entre ces deux parties de sorte que les données médicales ne soient jamais envoyées sans protection entre deux points. La question de savoir si le point à point est suffisant est à décider par projet.

Les utilisateurs doivent pouvoir signer et chiffrer des messages sur différents appareils (ordinateur portable, smartphone et tablette) sans devoir transférer et exposer des clés numériques entre ces appareils.

2.2.2. Intégrité

Lorsque des données médicales sont envoyées du client au serveur, elles doivent être signées au niveau du message pour assurer l'intégrité du contenu.

2.3. Le projet doit définir les standards de communication parmi ceux proposés

Identity & Access Management

Voici la liste des langages/protocoles proposés :

- SAML 2.0
- Oauth 2.0
- OIDC 1.0
- JWT
- Signed JWT Assertion
- PKCE

Information Security

Voici la liste des langages/protocoles proposés :

- TLS
- JWS
- JWE
- JWK
- WebAuthn

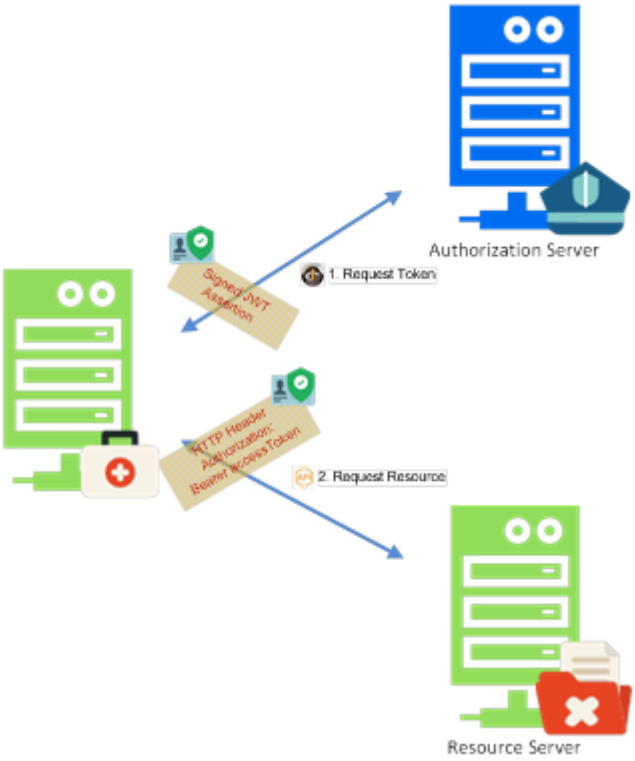
2.4. Le projet doit définir un ou plusieurs types de flux parmi ceux proposés

2.4.1. En ce qui concerne le volet « identification et gestion des Accès », il y a lieu de faire la distinction entre ces applications

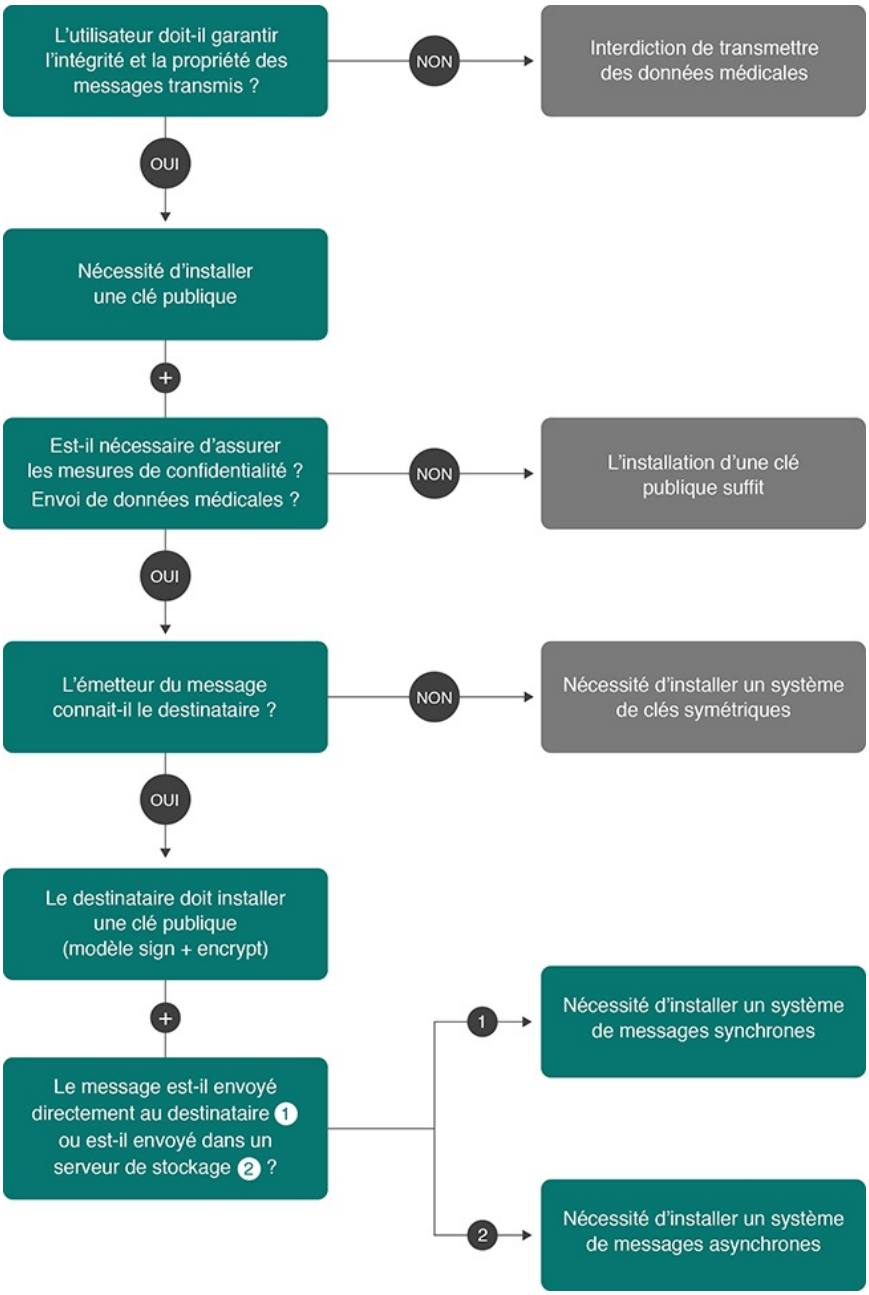
2.4.1.1. Une application destinée à fonctionner sur le dispositif mobile de l'utilisateur (native app/public client)

2.4.1.2. Une application « server based », hébergée par un partenaire et « appelée » par l'utilisateur pour utilisation sur son outil mobile (confidential client)

2.4.1.3. Une application ne nécessitant pas d'intervention humaine, destinée à fonctionner automatiquement de serveur à serveur, pour la mise à jour automatique de banques de données par exemple (system client)

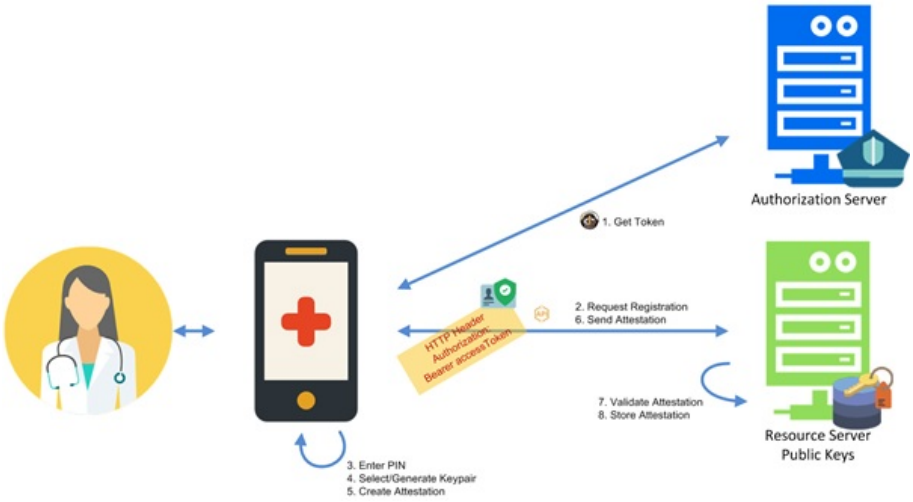


2.4.2. En ce qui concerne le volet « Sécurité de l'information », il y a lieu de s'interroger sur plusieurs aspects

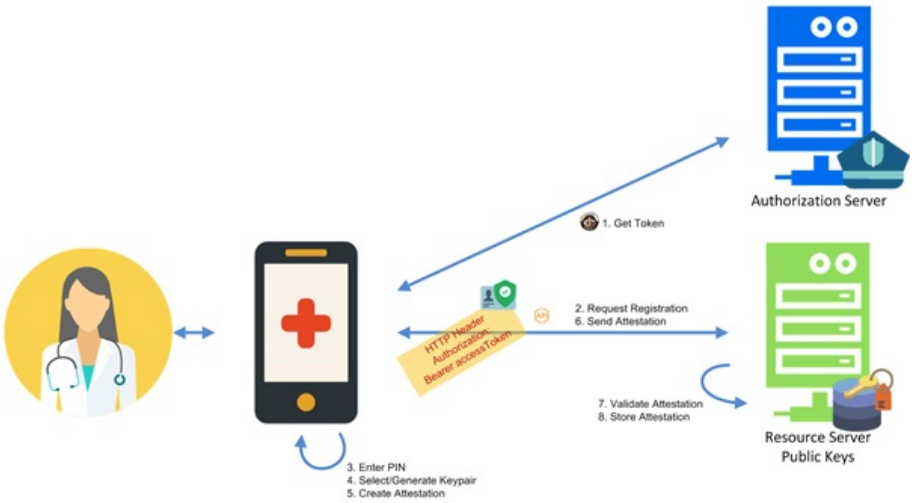


3. Cas pratiques schématisés

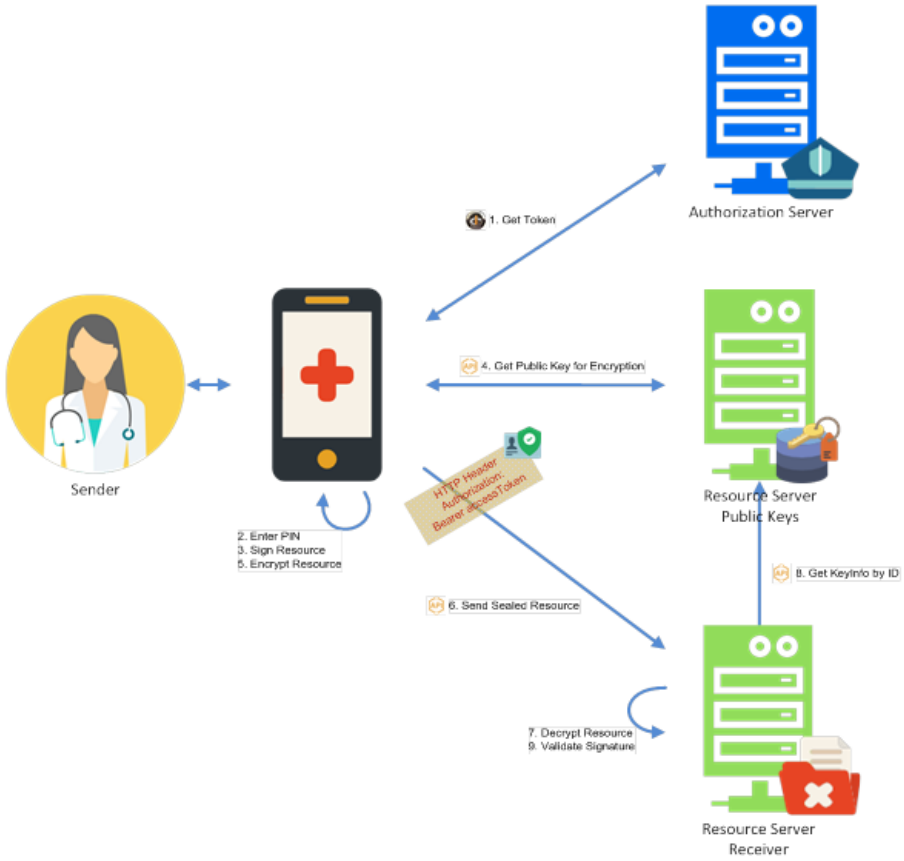
3.1. Enregistrement d'une clé publique (use case : enregistrement d'une clé dans le cadre de la demande d'un certificat eHealth au sein d'une architecture de type SOAP)



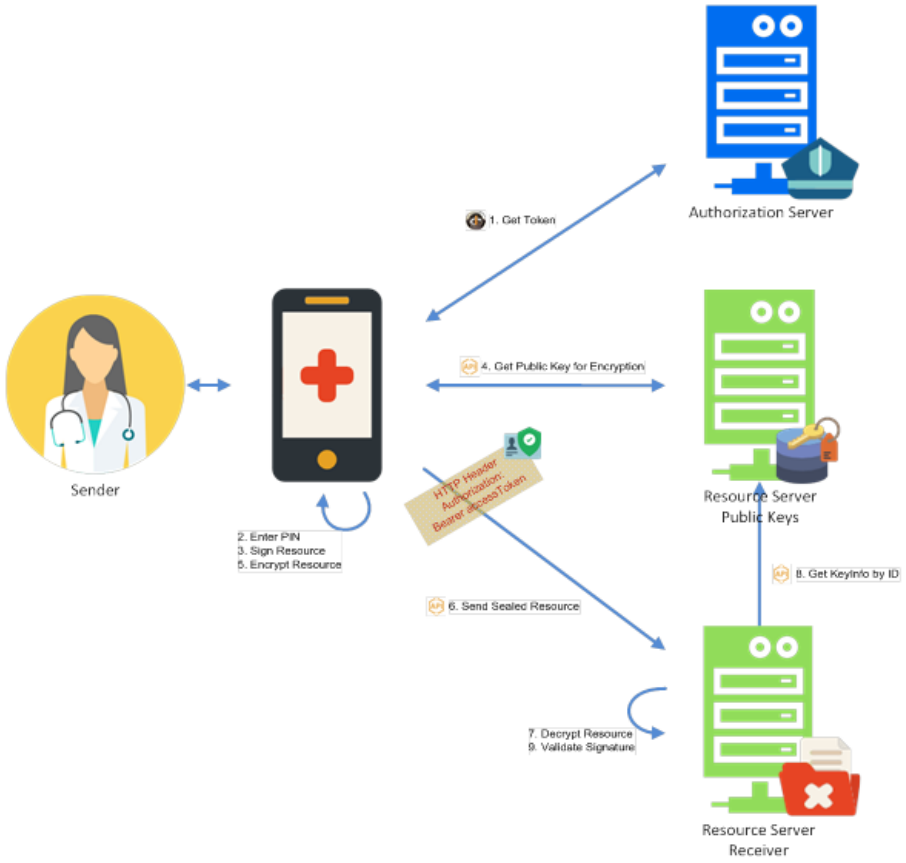
3.2. Enregistrement d'une clé symétrique (use case : enregistrement d'une clé dans le cadre de Recip-e)



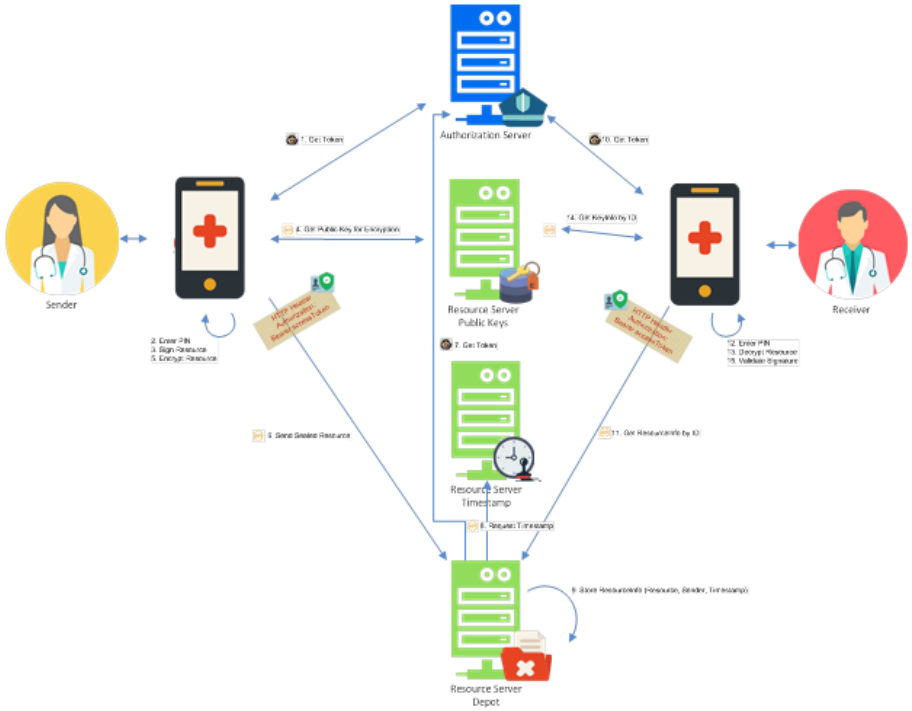
3.3. Destinataire connu, communication synchrone (use case le plus fréquent : lorsqu'un client doit contacter directement un service de plate-forme eHealth qui impose le système d'encryption)



3.4. Destinataire connu, communication asynchrone (use case : eHealthBox)



3.5. Destinataire inconnu (use case : Recip-e)



Application LiveCycle

1. Releases Management

Le tableau ci-dessous reprend les dates des prochaines MR (Major Releases) prévues ainsi que les dates de début des tests en acceptation.

Prochaines releases

Nom Release	Type de release	Content freeze	Code freeze	Mise en ACC sur AZ UP	Mise en ACC sur AZ IN et début tests	Mise en PRD sur AZ UP	Mise en PRD sur AZ IN
R2023.2.2	Minor	24/11/2023	04/01/2024	16/01/2024	23/01/2024	13/02/2024	20/02/2024
R2024.1	Major	16/11/2023	05/02/2024	27/02/2024	19/03/2024	07/05/2024	12/05/2024
R2024.1.1	Minor	04/04/2024	09/05/2024	21/05/2024	28/05/2024	11/06/2024	18/06/2024
R2024.1.2	Minor	02/05/2024	06/06/2024	25/06/2024	02/07/2024	16/07/2024	23/07/2024
R2024.2	Major	23/05/2024	08/07/2024	30/07/2024	20/08/2024	08/10/2024	13/10/2024
R2024.2.1	Minor	05/09/2024	10/10/2024	22/10/2024	29/10/2024	26/11/2024	03/12/2024
R2024.2.2	Minor	22/11/2024	02/01/2025	14/01/2025	21/01/2025	11/02/2025	18/02/2025
R2025.1	Major	14/11/2024	04/02/2025	25/02/2025	18/03/2025	06/05/2025	11/05/2025
R2025.1.1	Minor	03/04/2025	08/05/2025	20/05/2025	27/05/2025	10/06/2025	17/06/2025
R2025.1.2	Minor	30/04/2025	05/06/2025	24/06/2025	01/07/2025	15/07/2025	22/07/2025
R2025.2	Major	22/05/2025	08/07/2025	29/07/2025	19/08/2025	07/10/2025	12/10/2025
R2025.2.1	Minor	04/09/2025	09/10/2025	21/10/2025	28/10/2025	25/11/2025	02/12/2025

Chaque mention de release suit la logique suivante : R.2023.**x.y**, où **x** indique la « Major Release » (MR) et **y** la « minor Release » (mR). Par exemple, R.2023.1.2 est la 2e « minor Release » qui suit la première « Major Release » de l'année 2023.

Une MR est planifiée un an avant sa mise en place. Ci-dessous vous trouverez les étapes importantes du processus avec X = jour de la release majeure.

Étapes importantes du processus avec X

Timing	Étapes
X - 1 an :	Un an avant la release, on décide du contenu des changements apportés à la nouvelle release par rapport à la précédente.
X - 6 mois :	« content freeze » : plus aucune modification n'est apportée quant aux changements par rapport à la major release précédente.
X - 3 mois :	« code freeze » : plus aucune modification n'est apportée au code de la major release, les cookbooks sont publiés.
X - 5 semaines :	Début des tests dans l'environnement d'acceptation de la major release.
X - 2 semaines :	« acceptation freeze ».
X - 1 semaine :	Évaluation de la nouvelle version, c.à.d. le Go/noGo.
X	Montée en production.

Depuis juin 2021, notre nouvelle infrastructure est composée de deux AZ (Availability zone). Le trafic est réparti par défaut à 95 % sur l'AZ IN et 5 % sur l'AZ UP.

Chaque nouvelle mise en production se fera en mode « Canary release » (*). Dans le calendrier ci-dessus, vous trouverez 2 dates par environnements (AZ UP et AZ IN). Ces dates correspondent à la mise en ACC et PRD de la release.

(*) Explication du mode « Canary release »

Notre nouvelle infrastructure est composée de 2 AZ (Availability zone) qui nous permettent de mettre la nouvelle version de la release sur une de ces AZ (par défaut l'AZ UP) et ensuite de libérer le trafic petit à petit sur cette AZ (UP) contenant la nouvelle release et ce afin de mettre à jour l'autre AZ (IN) avec la nouvelle release.

Modalités de mise en production d'une release mineure (*)

Mise en production release mineure

Timing	Étapes
J1 Vendredi (qui précède la mise en PRD sur l'AZ UP)	*Tout le trafic est basculé (à 12 h 30) sur l'AZ IN afin de permettre la mise en production sur l'AZ UP sans perturber la production.*
J2 Samedi	X
J3 Dimanche	X
J4 Lundi	X
J5 Mardi	*La mise en production se fait sur l'AZ UP durant la journée.*
J6 Mercredi	*Le trafic est redirigé sur l'AZ UP en 2 temps : à 12 h 00 5 % et à 14 h 30 50 %.*
J7 Jeudi	*95 % du trafic est redirigé sur l'AZ UP à 12 h 30.*
J8 Vendredi	*100 % du trafic est redirigé sur l'AZ UP à 12 h 30.*
J9 Samedi	X
J10 Dimanche	X
J11 Lundi	X
J12 Mardi	*La mise en production se fait sur l'AZ IN durant la journée.*
J13 Mercredi	*Le trafic est redirigé sur l'AZ IN en trois temps : à 12 h 00 5 % et à 14 h 00 50 % et 95 % à 22 h 00.*

(*) Ce planning est susceptible d'être légèrement modifié en fonction de l'état d'avancement des déploiements de la release

Vous trouverez ces potentiels changements via ce lien :
https://status.ehealth.fgov.be/fr/interventions

Modalités de mise en production d'une release majeure (*)

Mise en production release majeure

Timing	Étapes
J1 Vendredi (qui précède la mise en PRD sur l'AZ UP)	*Tout le trafic est basculé (à 12 h 30) sur l'AZ IN afin de permettre la mise en production sur l'AZ UP sans perturber la production.*
J2 Samedi	X
J3 Dimanche	X
J4 Lundi	X
J5 Mardi	X
J6 Mercredi	*Le trafic est redirigé sur l'AZ UP en 2 temps : à 12 h 00 5 % et à 14 h 00 50 %.*
J7 Jeudi	*95 % du trafic est redirigé sur l'AZ UP à 12 h 30.*
J8 Vendredi	*100 % du trafic est redirigé sur l'AZ UP à 12 h 30.*
J9 Samedi	X
J10 Dimanche	*La mise en production se fait sur l'AZ IN durant la journée.*
J11 Lundi	*Le trafic est redirigé sur l'AZ IN en 3 temps : à 12 h 00 5 % et à 14 h 00 50 % et 95 % à 22 h 00.*

(*) Ce planning est susceptible d'être légèrement modifié en fonction de l'état d'avancement des déploiements de la release

Vous trouverez ces potentiels changements via ce lien :
https://status.ehealth.fgov.be/fr/interventions

L'environnement d'acceptation permet de réaliser les tests nécessaires à la mise en place de la release dans l'environnement de production.

Veuillez noter qu'il est indispensable d'utiliser des données (à caractère personnel) fictives lors des processus de tests ; l'utilisation de données réelles est strictement interdite.

Il est conseillé de procéder à des tests dans le but, pour chaque major release ou à chaque intégration d'un nouveau composant, de vous assurer que vos composants sont compatibles avec les (nouvelles) versions mises en ligne de nos services.

Les eHealth Release Notes sont des documents dans lesquels figurent les nouveaux développements principaux, les adaptations des services de base de la plate-forme eHealth, la fin de vie de services et les problèmes éventuels connus.

Les Release Notes sont publiées, sur le portail de la plate-forme eHealth, 3 mois avant une release majeure et un mois avant une release mineure.

2. eHealth Business Continuity Plan

Le Business Continuity Plan de la plate-forme eHealth a pour but de garantir la maintenance de nos services après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données, tout en conservant un certain niveau de sécurité. Ce plan est l'un des points essentiels de notre politique de sécurité informatique.

Quel que soit le niveau de responsabilité ou la source de l'incident, si un impact est constaté au niveau de la disponibilité des services de la plate-forme eHealth et/ou des services eSanté, l'objectif est de mettre à disposition une solution de secours afin d'assurer la disponibilité des fonctionnalités les plus importantes.

La détermination des fonctionnalités prioritaires, de leur niveau de priorité ainsi que l'implémentation technique des solutions sont réalisées en étroite collaboration avec les partenaires institutionnels et fournisseurs de logiciels. En ce qui concerne la communication des informations et étant donné la complexité des attentes des différents groupes-cibles (utilisateurs finaux/prestataires et intégrateurs ICT/fournisseurs de logiciels), l'ensemble des informations directement utiles aux prestataires est communiqué via le site eHealth Status, qui propose un aperçu détaillé des procédures mises en place et des logiciels qui les ont intégrées. Les informations et procédures spécifiquement dédiées aux intégrateurs ICT sont consolidées sur cette page du site web de la plate-forme eHealth, particulièrement consacrée à cette mission.

La mise en place d'un BCP, l'intégration des différentes interfaces ainsi que les exercices indispensables de tests nécessitent du temps et des adaptions continues. La priorité a été donnée, dans un premier temps, aux médecins généralistes et aux pharmaciens. L'implémentation des solutions est d'ores et déjà documentée sur le site eHealth Status.

La poursuite des différents processus verra simultanément :

- la participation consolidée de nouveaux partenaires selon leurs responsabilités ;
- la continuité et validation des processus en cours d'intégration chez les partenaires selon les standards imposés ;
- l'amélioration continue des outils et solutions sur base des observations de terrain ;
- la mise en place graduelle de nouvelles solutions pour l'ensemble des utilisateurs finaux.

La plate-forme eHealth met à la disposition des intégrateurs ICT les informations utiles pour l'intégration de sa solution BCP au sein de leur système. Pour ce faire, différents supports de documentation sont proposés :

- un cookbook d'implémentation générique de la solution BCP ;

- un document récapitulatif présentant une application concrète et déjà fonctionnelle du BCP dans le cadre du service assurabilité destiné aux pharmaciens ;
- les cookbooks de certains services (STS et ETK depot) contiennent des procédures BCP spécifiques à leur utilisation et complémentaires de la solution BCP décrite dans le cookbook BCP ;
- les connecteurs constituent également des support à l'intégration.

3. Niveaux de service

Les niveaux de service de la plate-forme eHealth sont formalisés au sein de deux types de documents :

- le « MSA » (Master Service Agreement) qui fournit un cadre global ;
- le « SLA » (Service Level Agreement) qui est spécifique à chaque service.

Le « MSA »

Le MSA propose, aux utilisateurs des services de la plate-forme eHealth, un cadre global traitant principalement de la gestion des incidents, problèmes et changements. Ce document décrit les engagements pris par la plate-forme, les diverses procédures applicables et les descriptions de services.

Le « SLA »

Le SLA clarifie les engagements plus spécifiques à chaque service de la plate-forme eHealth. Ce document contient notamment les objectifs de performance et/ou de disponibilité propres à chaque service, appelés aussi les « KPI » (Key Performance Indicators). Les différents SLA sont accessibles, sur le portail, au niveau des différents chapitres traitant des services proposés par la plate-forme eHealth.

Connectors

Aperçu des différents standards utilisés par la plate-forme eHealth

1. eHealth platform services connectors

Les « *eHealth platform services connectors* » sont des librairies locales (et légères) dont l'objectif est d'aider les développeurs de software à destination des prestataires de soins individuels et des pharmacies de soins à intégrer les services de base de la plate-forme eHealth proposés au travers d'interfaces « webservices ». Ces librairies visent également, plus généralement, à supporter les connexions aux services à valeur ajoutée accessibles via la plate-forme eHealth ou qui souscrivent aux standards ICT mis en place par la plate-forme eHealth (comme, par exemple, les « hubs »). Le développement de ces librairies s'inscrit donc dans une logique de standardisation et de support à l'utilisation des services de base de la plate-forme eHealth.

Ces connecteurs sont structurés en deux « couches » :

- la première couche, dénommée « **connecteurs techniques** », offre une API générique de support à l'utilisation des services de base purement techniques (principalement afférents à la sécurité : authentification, cryptage, etc.) ;
- la seconde couche, dénommée « **connecteurs business** », exploite le connecteur technique pour faciliter les connexions à un ensemble de services associés à un public cible donné au sein d'une même session.

Les connecteurs sont évidemment tributaires des interfaces des services qu'ils intègrent. Les mises à jour des connecteurs inhérentes aux changements de ces interfaces seront mises à disposition dans la mesure des possibilités de la plate-forme eHealth au travers de cette page web.

Ces connecteurs sont disponibles en JAVA et .NET mais sont uniquement développés en JAVA. Le code .NET n'est donc pas un code natif. Cette génération est effectuée via une version de l'outil IKVM légèrement adaptée pour nos besoins. Si vous entendez développer vos propres librairies sur base des nôtres dans la même philosophie, nous vous recommandons d'utiliser cette même version de l'outil et de respecter les « directives d'intégration » proposées avec celle-ci.

Les connecteurs sont des librairies distribuées sous licence libre. Elles sont disponibles pour tous ceux qui souhaitent les utiliser. Pour bénéficier de support dans l'utilisation de ces librairies, il faut, par contre, avoir préalablement introduit une demande auprès de la plate-forme eHealth. Vous pouvez introduire cette demande via l'adresse mail info@ehealth.fgov.be (avec la mention « eHealth platform services connectors » au niveau du sujet du mail).

Modification de mai 2024 par rapport aux versions précédentes

Release 4.5.4 & 3.26.1

Pour rappel, les versions 4.X.X sont destinées aux utilisateurs JAVA et les versions 3.XX.X aux utilisateurs .NET.

Connecteurs business

Bug fixes

- eh2ebox et ehboxv3 : le type MIME du body du message n'est plus restreint à text/plain ou text/html, afin de permettre l'usage d'autre types MIME pour eH2eBox.
- MyCareNet Registration: suppression de la timezone des dates dans le xml généré par le connecteur (certaines mutuelles n'acceptent pas de timezone).

Connecteurs techniques

Mise à jour du fichier de configuration par défaut du connecteur pour démarrer le module de configuration ConfigurationModuleRegisterTransformers, afin de mettre à disposition la transformation XAdES optional-deflate.

Note : les versions mineures des dépendances ont été également été mises à jour pour la version 4.5.4, en particulier le passage de org.apache.commons:commons-compress vers v1.26.1, qui résout des de vulnérabilités de sécurité.

Services couverts au niveau des couches « business »

- eHealth-platform services connectors

Compatibilité du connecteur technique

La compatibilité du connecteur technique version 4.4.0 avec les connecteurs Recip-e est validée.

Download

Les connecteurs « java » et un fichier d'archive pour les connecteurs « .net » sont disponibles via un maven repository. La liste suivante contient des liens vers les connecteurs business des différentes catégories professionnelles et le connecteur technique :

- Physician
- Physiotherapist
- Nurse
- Pharmacy
- Dentist
- Midwife

- Practical Nurse
- Audiologist
- Dietician
- Occupational Therapist
- Logopedist
- Orthoptist
- Podologist
- Trussmaker
- Connecteur technique

Services en ligne

1. Accès aux coffres-forts de soins

En Belgique, les données de santé sont notamment stockées dans ce que l'on appelle les ‘coffres-forts de soins de première ligne’. Il en existe trois en Belgique, un par région. En Flandre, il s'agit de "Vitalink", en Wallonie de "Intermed" et à Bruxelles de "Brusafe". Le service ‘Accès aux coffres-forts régionaux de soins’ permet aux prestataires de soins autorisés, d’accéder -via les logiciels médicaux ayant intégré ce service-, aux données de santé enregistrées au sein de ces coffres-forts. Cet accès est strictement cadré par les conditions fixées par la loi en matière de données de santé. La plate-forme eHealth a pour mission dans ce cadre d’assurer la sécurité des échanges.

2. WalCareNet - MemberData

Le service « Member Data » (MDA) de WalCareNet permet à toute institution ou prestataire de soins autorisé de consulter les informations du bénéficiaire de soins qui sont nécessaires pour effectuer une facturation ou pour délivrer des prestations/des produits de manière correcte.

Ce service offre plusieurs facettes dont la première, les données d'assurabilité du patient, est commune à toutes les institutions et prestataires de soins.

En fonction des décisions du Comité de sécurité de l'information, chaque secteur a droit à accéder à une ou plusieurs facettes.

En fonction du secteur, ce service est accessible en mode synchrone et/ou asynchrone.

Voici l’ensemble des facettes disponibles pour WalCareNet :

- Données d'assurabilité du patient (accessible à tous les secteurs) = facet insurability ;
- Pharmacien de référence = facet ReferencePharmacy ;
- DMG = facet GlobalMedicalfile ;
- Statut Soins palliatif = facet Palliativestatus.
- Trajet de soins = facet Carepath

Pour qui ?

- Les Maisons de Repos et de Soins (MRS), Maisons de Repos (MR) & Centre de Soins et de Jour (CSJ) ;
- Les Maisons de Soins Psychiatriques (MSP).
- Hôpitaux
- IHP (Initiatives d'Habitations Protégées)
- TOM (Technologue orthopédique en-aide à la mobilité)
- CRF (Centres de Revalidation Fonctionnelle)
- SISD (Soins intégrés à domicile)

Comment remplir / utiliser ?

Afin d'utiliser le service « Member Data », le prestataire soumet une requête qui, outre l'identification du patient (soit via son NISS ou son n° d'appartenance mutualiste), précisera la période pour laquelle cette consultation d'informations est demandée ainsi que les données qu'il souhaite recevoir : données d'assurabilité et un ou plusieurs droits dérivés auxquels son secteur a droit.

Seules les données autorisées pour un secteur peuvent être demandées.

Cette requête est aiguillée vers WalCareNet qui traite la requête et fournit, dans sa réponse, les données que le secteur est autorisé à recevoir.

Ce service est disponible en mode synchrone et en mode asynchrone uniquement par web service.

Sécurité de l'information & Vie privée

Nos réglementations, nos service en matière de sécurité et l'information relative au RGPD

1. Toolbox

Sensibilisation

Si la majeure partie des risques informatiques peuvent être évités ou se résoudre avec des outils de sécurité adaptés, il n'en demeure pas moins essentiel d'assurer la parfaite compréhension des risques et solutions auprès des collaborateurs, « l'erreur humaine » étant l'une des failles les plus exploitées. C'est la raison pour laquelle les institutions fédérales de santé publique mettent à destination des hôpitaux des outils didactiques et pédagogiques afin de les soutenir dans leur mission d'information et de prévention à la sécurité informatique. Différents supports sont disponibles comme des affiches, des présentations powerpoint, des flyers ou encore des vidéos à propos de sujets tels que la gestion des mots de passe, le phishing, les malwares ou encore les réflexes de sécurité à respecter en télétravail.

Toutes les informations et le matériel didactique sont disponibles dans les fiches suivantes, regroupées par thème :

- Hameçonnage (Phishing)
- Mots de passe et authentification multifactorielle
- Ingénierie sociale (social engineering)
- Télétravail
- Communiquez en toute sécurité
- Het CyZo Project (Helix-groep) (ce document est disponible uniquement en néerlandais)

Continuité

Pour toute organisation, le contrôle de la continuité des processus d'entreprise est d'une importance fondamentale.

Les attaques à la sécurité informatique des systèmes d'information des hôpitaux, laboratoires et autres institutions des soins de santé sont de plus en plus fréquentes. Aussi convient-il de prendre les mesures nécessaires afin de mieux protéger ces systèmes et leurs processus.

A l'aide d'une série de sujets, nous proposons des informations et des outils (tels que des listes de contrôle) afin d'améliorer la continuité. Vous trouverez les informations utiles dans les fiches d'information suivantes, organisées par thème :

- Incident response plan
- Business Continuity Plan

Les remarques et suggestions sont les bienvenues via mail à security@ehealth.fgov.be.

Auto-évaluation

Cette auto-évaluation permet de se faire une idée du niveau de conformité d'une organisation à différents points du RGPD.

- Auto-évaluation – Conformité RGPD

Budgets SPF Santé

Affectation du budget cybersécurité 2024 du secteur hospitalier

Cette section reprend la note d'instruction sur le financement individuel et contributeur ainsi que les deux formulaires mentionnés dans la circulaire du 15/03/2024 « Affection du budget cyber 2024 du secteur hospitalier ».

- Note d'instruction sur le budget individuel et contributeur – à consulter avant de compléter les formulaires
- Formulaire d'accès au financement individuel – à compléter **pour le 31 mai 2024**
- Formulaire d'accès au financement contributeur – à compléter **pour le 1er avril 2024**

2. Normes minimales

Une liste des normes minimales (MNM) et des Directives de mise en œuvre ont été élaborées pour les institutions dans le secteur de la santé, inspirées de la série ISO 27000. Ces MNM ont pour objectif de renforcer les règles de sécurité et les moyens de les contrôler afin d'accroître le niveau de sécurité global de toutes les institutions qui utilisent la plate-forme eHealth.

Les MNM constituent la base à partir de laquelle le délégué à la protection des données élabore la politique de sécurité de l'information concernant les systèmes et les structures d'information qui l'entourent.

Merci à NBN.

Outil de maturité

En collaboration avec les hôpitaux, un outil de maturité a été créé pour déterminer le niveau de maturité des hôpitaux par rapport aux normes minimales du secteur de la santé.

Rendez-vous sur l'outil de maturité.

3. Formation & GDPR

Conseiller en sécurité – Formations

La plate-forme eHealth propose chaque année une formation de base sur la sécurité de l'information et la protection des données.

Un plan de formation, conçu en étroite collaboration avec le service spécialisé agréé de la Smals, met l'accent sur les connaissances dont doit disposer un DPO ou un conseiller en sécurité afin d'assurer au mieux sa mission, quelle que soit la taille de l'organisation qui l'occupe.

Les parties intéressées qui souhaitent participer à cette formation doivent remplir la condition suivante : l'organisation utilise les services de la plate-forme eHealth.

Pour tout renseignement pratique (date des cours, inscriptions, locaux, ...), veuillez-vous adresser à Joëlle Ankaer (02-787 58 62).

Pour toute information sur le contenu de la formation, veuillez-vous adresser à security@ehealth.fgov.be.

- Description de la formation
- Formulaire d'inscription
- Agenda Formation 2024

General Data Protection Regulation

Le Règlement général européen sur la protection des données (« European General Data Protection Regulation », en abrégé « EU GDPR ») introduit de nouvelles règles en matière de gestion et de protection de données à caractère personnel. La Commission européenne a voulu avec ce Règlement rendre aux citoyens le contrôle de leurs données à caractère personnel et simplifier le cadre réglementaire pour les entreprises internationales en uniformisant les règles au sein de l'Union européenne.

Ce règlement est entré en vigueur le 24 mai 2016. Une période de transition de deux ans a cependant été prévue. Les organisations ont ainsi le temps jusqu'au 25 mai 2018 pour se conformer aux nouvelles exigences du règlement EU GDPR. Contrairement à une directive, il n'y a pas de transposition dans la législation belge.

A travers cette page web, la plate-forme eHealth se propose de rassembler les informations correctes concernant ce nouveau règlement.

Vous trouverez ci-après les liens vers les sources pertinentes :

- Le texte original du règlement EU GDPR
- Circulaire GDPR

Autres informations de la Commission européenne concernant le règlement EU GDPR :

- EU GDPR factsheets
- Informations relatives à la portabilité des données
- Informations relatives au délégué à la protection des données (DPO)
- Informations relatives à l'identification du « responsable du traitement » ou de « l'autorité de contrôle chef de file »
- Publication de données à caractère personnel à des fins de transparence dans le secteur public
- Informations concernant l'analyse d'impact relative à la protection des données
- Toolkit de l'EDPS en ce qui concerne les restrictions en matière de protection de données à caractère personnel
- DPO corner

L'Autorité de Protection des Données (APD) a consacré une page web spécifique au règlement EU GDPR et élaboré un plan par étapes pour la mise en œuvre du règlement EU GDPR.

L'Autorité de Protection des Données (APD) a également rédigé d'initiative une recommandation concernant l'analyse d'impact relative à la protection des données (« data protection impact assessment » ou « DPIA »).

La BCSS a adapté les normes minimales de sécurité de l'information afin de les rendre conformes au règlement EU GDPR.

Cette page web sera régulièrement mise à jour avec de nouveaux textes et adaptée en fonction des évolutions....

Standards

L'interopérabilité entre les divers acteurs du secteur des soins de santé ne peut être réalisée que si des accords clairs ont été conclus. En fonction du degré d'interopérabilité visé, il faut se mettre d'accord sur les règles régissant les échanges de données, l'architecture générale du système d'échange, les messages échangés, la structure des documents médicaux et sur la codification de l'information.

Depuis de nombreuses années déjà, des initiatives de standardisation sont prises et Belgique et des projets sont mis sur pied. Ci-dessous figure un aperçu non exhaustif des standards utilisés, dans une mesure plus ou moins large, dans les soins de santé en Belgique.

Le législateur a confié à la plate-forme eHealth la mission de définir des standards techniques et fonctionnels utiles en matière d'ICT à l'appui de l'échange électronique de données dans les soins de santé. Les standards existants, énumérés ci-après, serviront de point de départ pour les standards à définir en étroite concertation avec les divers acteurs des soins de santé. Les standards définis par la plate-forme eHealth porteront uniquement sur les aspects ICT et non sur les aspects de contenu des soins de santé.

1. Standards

L'interopérabilité entre les divers acteurs du secteur des soins de santé ne peut être réalisée que si des accords clairs ont été conclus. En fonction du degré d'interopérabilité visé, il faut se mettre d'accord sur les règles régissant les échanges de données, l'architecture générale du système d'échange, les messages échangés, la structure des documents médicaux et sur la codification de l'information.

Depuis de nombreuses années déjà, des initiatives de standardisation sont prises en Belgique et des projets sont mis sur pied.

Le législateur a confié à la plate-forme eHealth la mission de définir des standards techniques et fonctionnels utiles en matière d'ICT à l'appui de l'échange électronique de données dans les soins de santé.

Vers le site dédié aux standards