Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Normes et architecture
Recommandations IV

Communication entre communautés / Portail d'accès

Adoptées par le comité de pilotage

Berne, le 17 janvier 2013

ehealthsuisse
Koordinationsorgan Bund-Kantone
Organe de coordination Confédération-cantons
Organi di coordinamento Confederazione-Cantoni

Impressum

Organisation du projet
Comité de pilotage : Alain Berset (conseiller fédéral, chef du DFI), Pascal Strupler (directeur de l'OFSP), Stefan Spycher (vice-directeur de l'OFSP), Andreas Faller (vice-directeur de l'OFSP jusqu'en décembre 2012), Carlo Conti (conseiller d'Etat, directeur de la santé, canton BS), Guido Graf (conseiller d'Etat, directeur de la santé, canton LU), Heidi Hanselmann (conseillère d'Etat, directrice de la santé, canton SG), Pierre-François Unger (conseiller d'Etat, directeur de la santé, canton GE).
Organe directeur du projet : Adrian Schmid ("eHealth Suisse", président); Christian Affolter (santésuisse); Lotte Arnold (SPO); Hansjörg Looser (GD SG); Daniel Notter (pharmaSuisse) ; Caroline Piana (H+); Georg Schielke (CDS); Michael Stettler (OFSP jusque mars 2012) ; Adrian Jaggi (OFSP jusqu'en décembre 2012) ; Walter Stüdeli (IG eHealth); Salome von Greyerz (OFSP); Judith Wagner (FMH).

Secrétariat de l'Organe de coordination "Health Suisse" : Adrian Schmid (responsable), Catherine Bugmann, Isabelle Hofmänner, Sang-Il Kim, Stefan Wyss.

Expert scientifique : Christian Lovis (Hôpitaux Universitaires de Genève HUG, président de la SSIM)

Autres informations et sources :
www.e-health-suisse.ch

Objectif et positionnement de ce document

Suite à l'adoption de recommandations sur différents sujets les 20 août 2009 et 20 octobre 2010 par le Comité de pilotage de la Confédération et des cantons pour la mise en œuvre de la « Stratégie Cybersanté (eHealth) Suisse », celui-ci a également adopté le Concept d'évaluation des essais pilotes le 27 janvier 2011. Le présent document contient des propositions en vue d'autres recommandations dans le domaine « Normes et architecture ». Deux documents établis par le consortium Poste/ELCA (communication entre communautés) et la société Swisscom en collaboration avec medshare GmbH et la Fondation Health On the Net - HON (portail d'accès) ont servi de documentation préparatoire. Les propositions de recommandations et les documents préparatoires peuvent être consultés sur www.e-health-suisse.ch.

Afin de faciliter la lecture de ce document et sauf mention contraire, le masculin générique est utilisé pour désigner les deux sexes.

Table des matières

1 Rappel de la situation 4
1.1 Introduction 4
1.2 Limites 5
1.3 Quelques définitions 7
2 Composantes et services centraux 10
3 Communication entre les communautés 14
3.1 Principes généraux 14
3.2 Concept d'autorisation 15
3.3 Identification et authentification 17
4 Audit et notification 18
5 Portail d'accès 21
6 Conclusions 25
Annexe 1 : Principes architecturaux pertinents 28
Annexe 2 : Indications techniques 30
Annexe 3 : Attributs services CPI-S (Registre des communautés) 33

1 Rappel de la situation

1.1 Introduction

Basé sur les recommandations précédentes

Le présent document est basé sur les recommandations et rapports publiés jusqu'ici par « eHealth Suisse » ; voir :

http://www.e-health-suisse.ch/umsetzung/00146/00148/index.html?lang=fr

Positionnement du présent document

Le présent document explique sur le plan technique comment la communication entre communautés peut être assurée, quelles sont les composantes centrales nécessaires et comment est aménagée la composante architecturale « Portail d'accès ». Il définit en partie des tâches nouvelles pour lesquelles les compétences ne sont pas encore attribuées. Ces compétences, de même que le caractère contraignant de leur application, relèvent de décisions politiques qui devront être clarifiées dans le cadre des projets législatifs. On peut concevoir l'institution de bases légales à l'échelle fédérale – ou cantonale – ou des conventions contractuelles entre les différents acteurs.

Importance de la communication

Les concepts recommandés par la suite font référence, dans l'« Architecture eHealth Suisse », à la communication entre communautés (avec prise en compte des composantes coordonnées au niveau national) ainsi qu'à la composante architecturale « Portail d'accès » (voir figure 1). Ils décrivent les autres éléments importants de toute l' « Architecture eHealth Suisse » nécessaires à la mise en place d'une solution fédérale décentralisée.

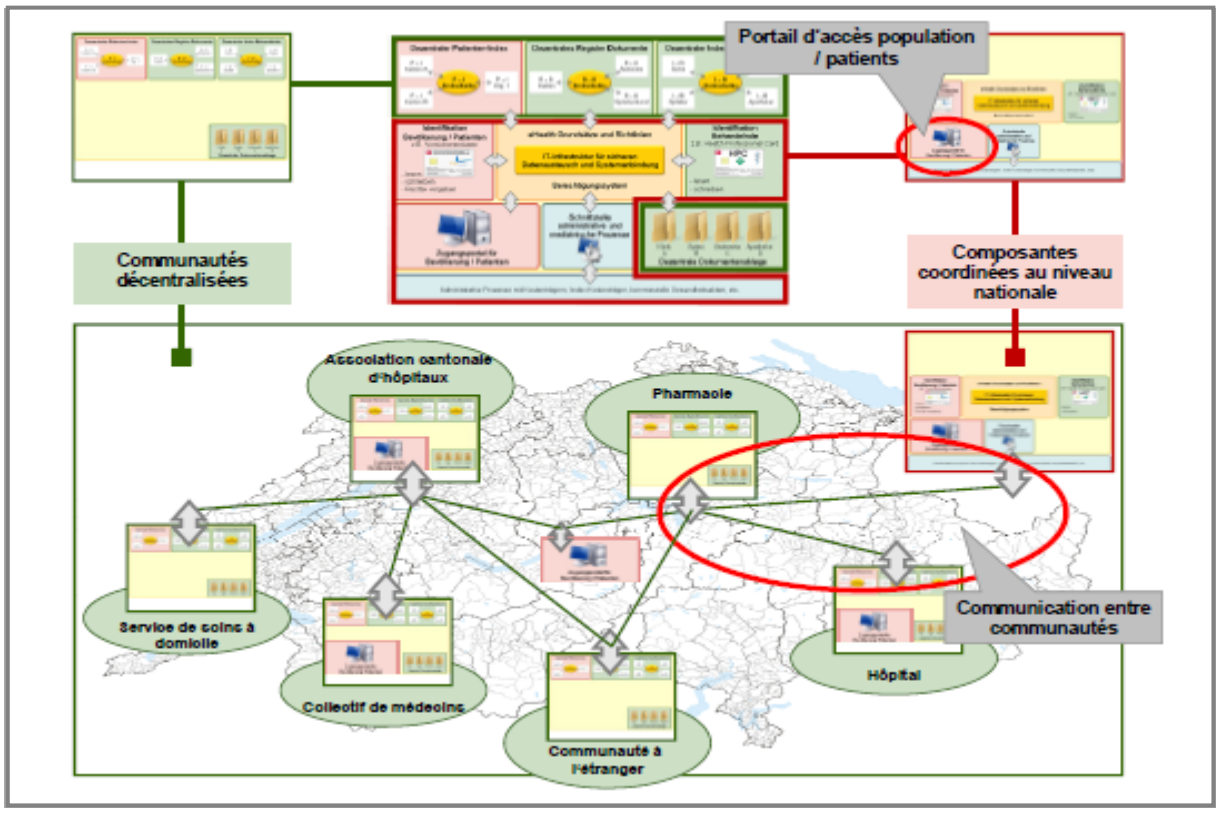

Figure 1 : Positionnement dans l'« Architecture eHealth Suisse »

Complément aux recommandations I à III

Dans les recommandations I à III, l'accent principal était mis sur les composantes décentralisées dans les communautés et sur les concepts de base pour une gestion des autorisations étendue à toute la Suisse. Les recommandations d'aujourd'hui ont pour objet de définir les composantes et processus avec lesquels organiser la communication entre communautés. L'Annexe 1 «Principes architecturaux pertinents» donne un aperçu des recommandations antérieures dans ce domaine.

1.2 Limites

Modèle multiphases

Le développement de la cybersanté est un processus évolutif qui traverse differents degrés de maturité. La figure 2 présente schématiquement un modèle de maturité qui montre un processus de transition de solutions actuelles vers des solutions futures.

- Degré de maturité 1: communication électronique dirigée (p. ex. système point-to-point, métaphore d'envoi de courrier numérique p. ex. sous forme de fax, de courriel avec documents joints, etc.). Le système d'information des professionnels de santé (anc. professionnels traitants[1]) constitue la « mémoire primaire » des documents ;

[1] Dans le contexte du projet de loi sur le dossier électronique du patient, le terme de « professionnel traitant » est remplacé par celui de « professionnel de la santé ».

- Degré de maturité 2 : système centré sur les documents pour une communication non dirigée. Disponibilité et interrogation en tout temps de documents plus ou moins structurés, stockés en copie décentralisée dans une « mémoire secondaire » (dossier électronique du patient, DEP) ;
- Degré de maturité 3: système centré sur les données avec disponibilité multidimensionnelle de données structurées. introduction directe d'informations médicales dans un DEP. La limite entre mémoire « primaire » et « secondaire » s'estompe rapidement. Les professionnels de la santé sont soutenus par des systèmes de « Decision Support ».

A l'instar des recommandations I à III déjà publiées, les présentes recommandations IV se réfèrent au degré de maturité 2 conformément à la « Stratégie Cybersanté« (eHealth) Suisse » dans le but d'établir un dossier électronique du patient valable dans toute la Suisse. Les degrés de maturité 2 et 3 présentent des différences importantes :

- Dans le degré de maturité 2 , seul le traitement différé (asynchrone) des documents est possible ; le degré de maturité 3 permet le traitement simultané (synchrone) de documents par plusieurs utilisateurs ;

- Dans le degré de maturité 2, seules des unités d'information finalisées sont mises à disposition dans un DEP, tandis que le degré de maturité 3 permet aussi le traitement de données « librement disponibles » entre lesquelles des liens multidimensionnels peuvent être créés.

Les degrés de maturité 1 à 3 se succèdent dans cet ordre sur le plan technique et fonctionnel, mais peuvent coexister côte à côte au niveau du contenu d'informations, de l'utilisation de données et des conditions cadres régulatrices. Cela permet de supporter un plan de migration et d'adoption raisonnable, adapté aux besoins, qui répond aux défis sociaux et économiques. L'interopérabilité entre les différents degrés de maturité doit être garantie. Les recommandations I à IV de « eHealth Suisse » se limitent au degré de maturité 2. Il est impossible actuellement d'estimer à quel moment le degré de maturité 3 sera engagé. Si sa mise en place peut être constatée ponctuellement au sein de quelques institutions et organisations, elle reste encore confinée dans leurs limites.

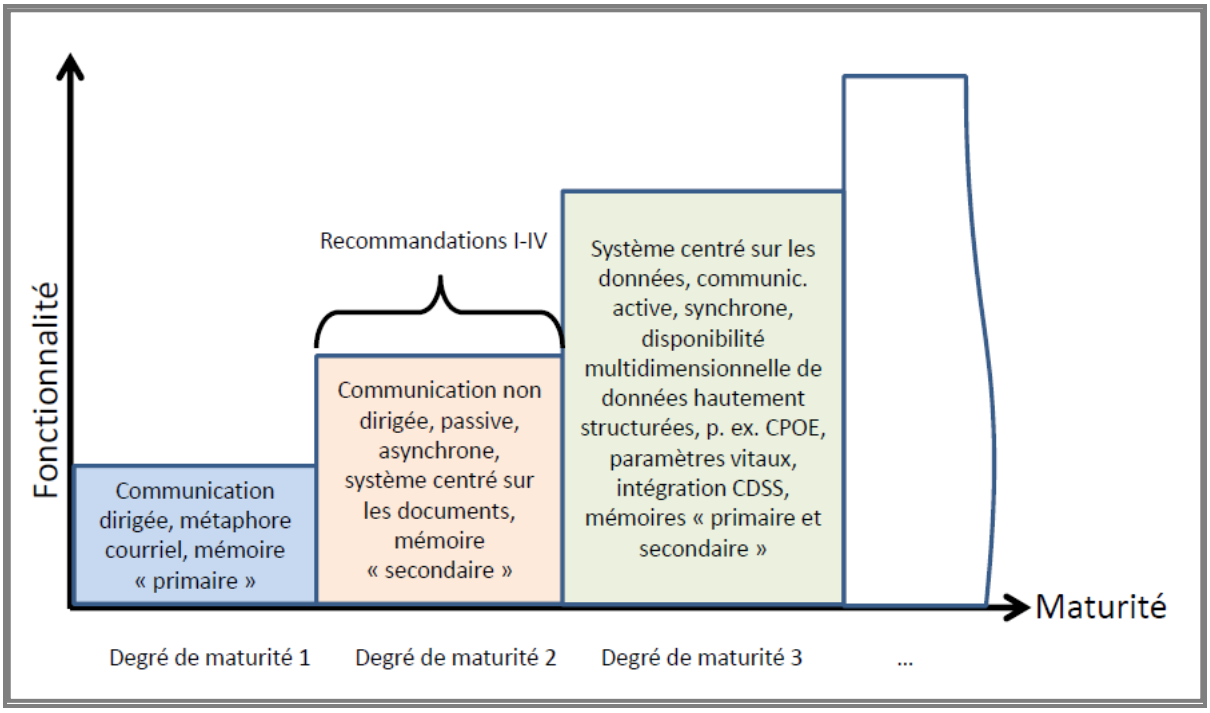

Figure 2 : Le modèle multi-phases de transition eHealth

1.3 Quelques définitions

Une communauté est une unité organisationnelle de professionnels de la santé qui Communauté

1. participe au traitement des patients,
2. génère et utilise des informations concernant le patient et
3. échange ces informations avec les autres communautés.

La collaboration au sein d'une communauté doit être réglée par contrat et revêtir une forme juridique. Un professionnel de santé peut faire partie de plusieurs communautés. La définition ne contient pas de spécifications concernant la taille, la délimitation géographique ou l'organigramme d'une communauté. La liste suivante donne quelques exemples possibles de communautés :

- Des groupements de professionnels de la santé de différentes catégories dans des réseaux de soins (p.ex. des cabinets médicaux, des physiothérapeutes, des hôpitaux) dans une région, au-delà des frontières cantonales ;
- Associations d'hôpitaux qui coopèrent étroitement et qui échangent des patients, p. ex. un centre hospitalier avec plusieurs petits hôpitaux ;
- Des réseaux de médecins, qui sont organisés à un niveau local ou régional et où les membres coopèrent étroitement, p. ex un réseau oncologique ;

- Association d'organisations d'un groupe de traitants pour des raisons synérgiques, p. ex. plusieurs laboratoires, qui veulent mettre à disposition des données médicales à d'autres communautés ou des pharmacies voulant offrir à leurs clients des services supplémentaires.

La communauté, en tant qu'entité, qui veut participer au système global « eHealth Suisse » doit faire certifier ses techniques, ses processus et son organisation.

Pour l'ensemble du document, les termes « communauté » et « portail d'accès » impliquent systématiquement une certification.

Communauté de référence

Chaque communauté de référence doit proposer des fonctions pour l'administration des déclarations de consentement et des autorisations. Les communautés qui ne proposent pas ces fonctions ne peuvent être choisies comme communautés de référence par les patients. Chaque communauté de référence doit offrir un portail d'accès interne pour permettre aux patients de définir les autorisations d'accès à leur dossier. Le patient qui change de communauté de référence doit pouvoir transférer les autorisations dans sa nouvelle communauté. La communauté de référence doit assurer cette possibilité (exportation et importation des données entre une ancienne et une nouvelle communauté de référence). A chaque identité de patient ne peut correspondre qu'une seule communauté de référence à un moment donné. Comme les communautés, les communautés de référence doivent être certifiées.

Portail d'accès

Le patient doit à tout moment pouvoir accéder à ses propres données. Une exigence essentielle de transparence des données et d'autonomie de décision des patients est ainsi remplie. Ce droit d'accès est protégé par des portails d'accès (internes ou externes) certifiés. Le portail d'accès interne doit en outre permettre aux utilisateurs l'administration des droits d'accès individuels.

Une communauté peut avoir comme élément intégral un portail d'accès « interne ». Des portails d'accès indépendants, « externes » à une communauté, sont également possibles, mais ils ne permettent que les accès en lecture seule et n'offrent pas la possibilité de sauvegarder des données ou de modifier des autorisations.

Par le portail d'accès interne, les patients doivent aussi pouvoir donner aux professionnels de la santé l'accès à des données qu'ils ont relevées eux-mêmes comme le relevé algique, les niveaux de glycémie ou les valeurs de tension artérielle.

En outre, les professionnels de la santé autorisés doivent aussi pouvoir utiliser les portails d'accès internes pour consulter ou saisir des données.

Le tableau suivant montre les deux types de portails d'accès et les fonctionnalités les plus importantes pour l'utilisateur potentiel. Tous les utilisateurs doivent être enregistrés dans une communauté ou au portail d'accès externe pour pouvoir participer au système. Ceci concerne aussi les professionnels de la santé qui n'appartiennent pas à une communauté ou qui ne veulent pas utiliser un portail d'accès externe.

Portail d'accès interne à la communauté de référence		Portail d'accès externe sans communauté, accès en lecture seule	
Patient	Professionnel de santé – sans intégration TI[2]	Patient	Professionnel de santé – sans intégration TI
-Administration de l'autorisation -Consultation données -Sauvegarde données	-Consultation données -Sauvegarde données	-Consultation données	-Event. consultation données

Point d'accès

Un point d'accès confère une vue *logique* sur une communauté depuis l'extérieur. Pour une communauté, le point d'accès est le canal de communication exclusif avec les autres communautés.

Nœuds passerelles

Un point d'accès doit remplir plusieurs fonctions. Celles-ci sont *techniquement* implémentées sous forme de nœuds dits « passerelles ». Un nœud passerelle effectue une certaine tâche en offrant ou en utilisant un service. Le point d'accès d'une communauté comprend ainsi plusieurs de ces nœuds, par exemple un nœud demandeur (initiating gateway) et un nœud répondeur (responding gateway). Tous les nœuds passerelles d'une communauté doivent être individuellement certifiés.

L'annexe 2 décrit, pour chacun des quatre chapitres suivants, certains aspects importants concernant l'implémentation technique.

[2] Professionnels de santé, qui n'utilisent pas de dossier médical électronique ou qui n'ont pas de système TI intégré à l'infrastructure du dossier électronique du patient, p.ex. un logiciel pour les cabinets médicaux, qui ne soutient pas de profil IHE, ou un système TI d'hôpitaux qui ne peut pas enregistrer de documents médicaux soi-même.

2 Composantes et services centraux

Sécurité de l'espace de confiance par la certification

La communication électronique dans l'« Architecture eHealth Suisse » est caractérisée par :

- son déroulement dans le cyberespace, toutes les transactions numériques étant transmises via le réseau mondial qu'est Internet
- une authentification poussée des utilisateurs
- la sécurisation des voies de communication et des données transportées par cryptage
- une communication point à point entre les nœuds passerelles

Ces caractéristiques créent un espace de communication sécurisé sur Internet (espace de confiance du DEP). Peuvent y participer les communautés, portails d'accès et composantes centrales. L'accès à cet espace de confiance est assuré par les nœuds passerelles certifiés (voir figure 3).

Recommandation 1

Espace de confiance par certification

Les points d'accès des communautés et des portails d'accès ainsi que les composantes centrales constituent l'espace de confiance du DEP. Tous les points d'accès sont certifiés.

Recommandation 2

Interface externe identique de tous les portails (gateways)

L'interface externe des points d'accès à l'espace de confiance du DEP sont toutes identiques. Ceci est également vrai pour les portails d'accès externes.

Services « centraux »

Des services de registres « centraux » sont nécessaires pour une bonne communication entre communautés. Ils sont représentés schématiquement à la figure 3 :

- Un service de registre de communautés et de portails d'accès externes
  Service pour Community/ Portal Index (CPI-S) ;
- Un service de registre des professionnels de la santé
  Service pour Health Professional Index (HPI-S) ;
- Un service de registre des organisations de santé
  Service pour Healthcare Organisation Index (HOI-S) ;
- Un service de registre des rôles
  Service pour Role Index (RI-S) ;
- Un service de registre de métadonnées
  Service pour Metadata Index (MDI-S).

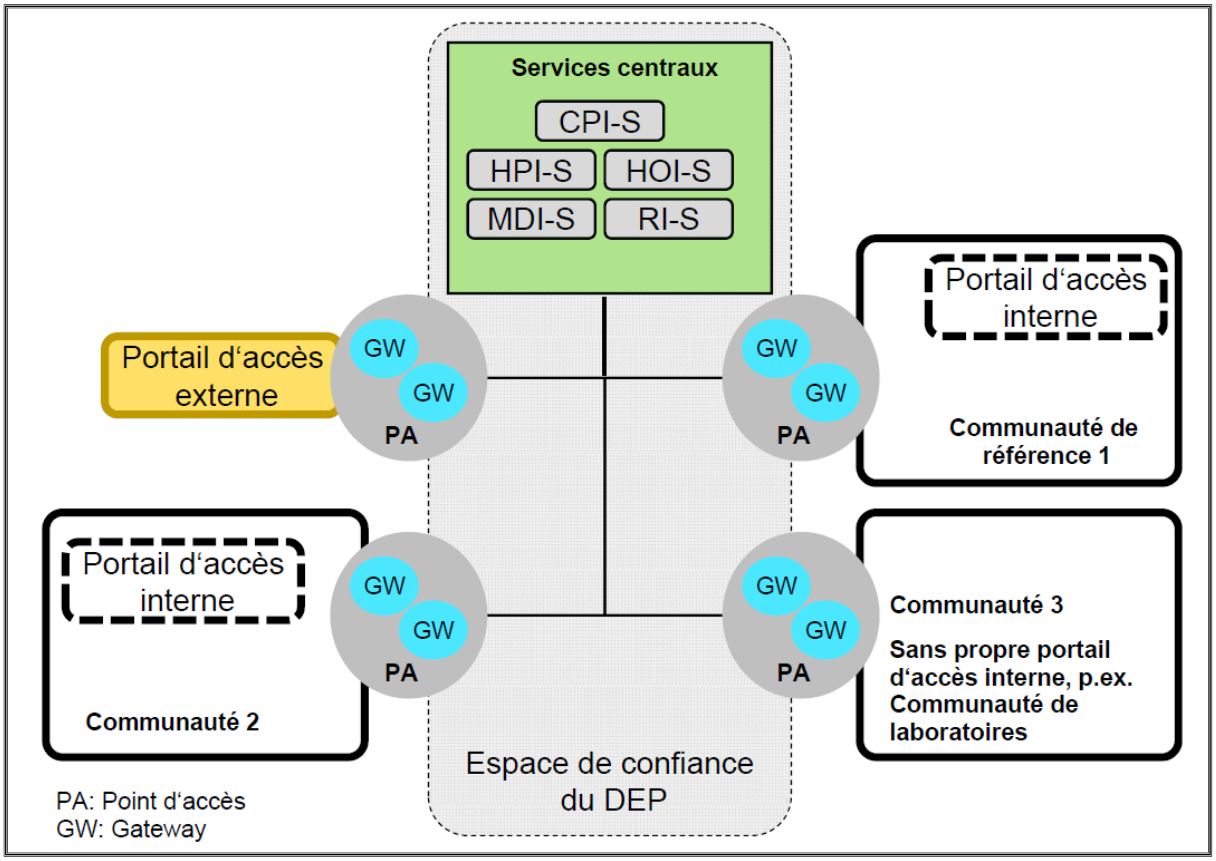

Figure 3 : Espace de confiance du DEP et composantes/services centraux

A la différence des Recommandations II (voir page 12, recom. 3), l'échange d'informations en lecture est aussi accordé aux portails d'accès externes. En outre, la configuration technique est définie de sorte qu'elle possède les attributs exigés. Les informations nécessaires sont énumérées dans l'annexe 3 « Attributs CPI-S ».

Toute communauté et chaque point d'accès externe est disponible par le service de registre central. Celui-ci ne répertorie que les communautés et les portails d'accès externes valablement certifiés. L'inscription au registre et la tenue à jour des entrées s'effectuent à l'échelle nationale.	Recommandation 3 Service central d'un registre des communautés et portails d'accès externes

Pour un contrôle effectif des accès aux données d'un patient, des professionnels de santé clairement identifiés doivent pouvoir se faire attribuer un ou plusieurs rôles autorisés. Pour une identification claire comprenant d'autres indications importantes comme le groupe professionnel et la qualification, un service d'index de professionnels de santé (service HPI) est indispensable avec les informations suivantes :

- GS1 GLN en tant qu'identificateur univoque
- données de base personnelles
- profession/qualification
- spécialisation (s'il y a lieu)
- autorisation de pratiquer avec mention de la date de validité et avec indication du lieu de délivrance (si connus)

Tout professionnel de santé faisant partie de l'espace de confiance du DEP est retrouvable et clairement identifiable via le service HPI-S. Les différents registres fournissent au service HPI-S les informations correspondantes et garantissent la fiabilité des données. Ce service est administré en coordination nationale.	Recommandation 4 Service central d'un registre des prestataires de soins
En plus de renseignements personnels spécifiques sur le professionnel de santé, il faut aussi une liste de toutes les institutions du système de santé (hôpital, service d'un hôpital, organisation de soins à domicile, cabinet médical, etc.) susceptibles d'être interrogées dans un service de registre des organisations de santé (service HOI-S). Outre les informations descriptives ci-dessus, cette liste doit aussi présenter des GS1 GLN univoques (cf. Recommandations II, métadonnée 2.5 : numéro d'identification de l'institution selon le GS1 GLN (GS1 Global Location Number). Dans le système des autorisations, l'indication de l'organisation peut être combinée avec des renseignements personnels - par exemple pour l'autorisation d'accès de membres d'un cabinet médical.	
Il est important de bien séparer les personnes et les institutions dans les services HPI-S et HOI. Ce n'est qu'ainsi que l'on peut, à partir de ces deux listes, décrire l'appartenance d'une personne à différentes institutions et garantir l'intégrité référentielle (p. ex. le médecin XY exerce au cabinet médical A et à l'hôpital B).	Interaction des services HPI et HOI
Un service de registre d'organisations de santé (service HOI) avec des entrées GS1 GLN est disponible en tant qu'entité centrale propre. Ce service est administré en coordination nationale.	Recommandation 5 Service central d'un registre d'organisations de santé
Un registre consultable des rôles autorisés (service de registre des rôles) est nécessaire à la mise en œuvre du système des autorisations. Le patient a toujours la possibilité de réattribuer les numéros d'identification de rôles aux identités des soignants et de contrôler ainsi l'accès aux données.	
Un service de registre de rôles est disponible en tant qu'entité centrale propre. Ce registre est administré en coordination nationale.	Recommandation 6 Service central d'un registre de rôles
L'utilisation de métadonnées IHE XCA homogènes est nécessaire pour l'échange d'informations entre communautés. Ce n'est qu'ainsi que l'on peut garantir une interopérabilité technique et sémantique. Certains attributs de métadonnées sont importants pour le contrôle des autorisations. D'autres sont descriptifs et servent au filtrage et au classement des données affichées.	

Un service central d'un registre de métadonnées est disponible en tant qu'entité centrale propre. Ce service est administré en coordination nationale.	Recommandation 7 Service central d'un registre de métadonnées

3 Communication entre les communautés

3.1 Principes généraux

Comme le montre schématiquement la figure 3, la communication entre communautés n'est possible que par les points d'accès logiques ou les nœuds passerelles (gateways) techniques d'une communauté. Conformément au principe fondamental qui veut qu'un document enregistré dans le système soit clairement défini et ne puisse plus être modifié, une fonctionnalité d'écriture via ces nœuds passerelles n'est pas autorisée dans la phase 2 du modèle de transition. Cela vaut aussi pour les portails d'accès externes liés à ces gateways.

L'accès intercommunautaire via les portails (gateways) est autorisé uniquement en lecture seule. Chaque communauté conserve ainsi le contrôle sur l'ensemble des documents produits dans la communauté, avec tous les droits et obligations qui leur sont liés, et peut aussi à tout moment établir de façon incontestable le contenu original d'un document.	Recommandation 8 Accès intercommunautaires : en lecture seule
L'attribution univoque à des personnes dans le contexte de l'« Architecture eHealth Suisse » s'effectue au moyen d'identités électroniques. En principe, cela n'exclut pas la possibilité technique qu'une personne possède plusieurs identités électroniques de patient. La question si une personne physique peut avoir une ou plusieurs identités électroniques doit être réglée dans le cadre des projets législatifs.	Identités de personnes
L'office d'état-civil de la commune d'origine tient un registre des originaires de la commune et établit des certificats d'origine à des particuliers. Toute personne qui vient s'installer dans une commune doit déposer son certificat d'origine au contrôle des habitants. Par analogie avec le dépôt du certificat d'origine, un patient ne peut déposer qu'en un seul lieu par identité sa déclaration de consentement et ses attributs d'autorisation, et doit les transférer en un nouveau lieu s'il change d'identité. Pour que le consentement du patient et ses droits d'accès soient trouvés d'une manière univoque, une identité électronique de patient ne doit être déposée à tout moment qu'à une seule communauté de référence.	Analogie avec le certificat d'origine
Toute identité électronique de patient ,'est attribuée à tout moment qu'à une seule communauté de référence.	Recommandation 9 Une communauté de référence par identité
Des fonctionnalités d'exportation et d'importation sont requises dans certains scénarios, comme par exemple le passage d'un patient dans une autre communauté de référence, son départ d'une communauté (de référence) ou la fermeture de cette communauté. Il peut s'agir de données médicales et administratives, de fichiers journaux ou d'attributions de droits d'accès. Cela implique l'absence de toute fonctionnalité d'écriture via des nœuds passerelles (gateways) dans les espaces d'autres communautés et de toute copie inutile de données. Lors de la fermeture d'une communauté (de référence), l'accès aux données dans le DEP n'est plus possible. Les documents originaux des prestateurs de soins restent dans les systèmes sources qui les ont créés.	

Une communauté est en mesure d'importer et d'exporter tous les contenus appartenant à un patient. L'importation et l'exportation s'effectuent via la composante architecturale « Interface des processus médicaux et administratifs ». Cette capacité doit être certifiée.	Recommandation 10 Fonctionnalités pour l'importation/ exportation

3.2 Concept d'autorisation

En vertu des Recommandations II et III, le système d'autorisation de l'« Architecture eHealth Suisse » repose, d'une part, sur le rôle de l'utilisateur et des métadonnées d'un document, et d'autre part, sur les réglages individuels des attributs d'autorisation par le patient. L'élément décisif, en fin de compte, est toujours l'octroi explicite par le patient d'un consentement à la consultation de ses données selon une liste d'accès dynamique que le patient administre lui-même. Il peut le faire par exemple via le service HPI en désignant nommément des professionnels de la santé auxquels il attribue un rôle défini. Une autre voie concevable est l'octroi/la détermination explicites de niveaux de confidentialité des documents par le patient, par exemple la règle consistant à attribuer systématiquement le niveau de confidentialité « données stigmatisantes » à tous les documents d'un service psychiatrique. Dans tous les cas, le patient qui gère ses attributs de droits d'accès doit être suffisamment informé des conséquences de ses actes, ceci afin d'exclure que l'accès à ses données puisse être régi par des règles implicites et des automatismes à l'insu du patient. Les réglages de base mentionnés dans la Recommandation III (voir page 22, Recommandation 5) doivent donc être expliqués précisément au patient, tout comme son droit de modifier explicitement ces préréglages.

Le patient a le contrôle

Le concept global de contrôle des autorisations est fondé sur le principe de l'octroi explicite de droits d'accès par le patient. Cela peut se faire via les métadonnées des documents et par l'attribution de rôles à certains professionnels de la santé. C'est l'action consciente du patient informé qui est déterminante, et non les propriétés implicites du système, qui sont inconnues du patient.	Recommandation 11 Octroi explicite de droits par le patient

Les attributs de droits du patient doivent être évalués à chaque vérification d'accès. Le caractère univoque et actuel des attributs de droits peut être garanti au mieux si ces attributs sont uniques dans le système et qu'il n'en existe aucune copie. Le lieu d'enregistrement idéal est la communauté de référence, vu que toute identité de patient est attribuée à une communauté de référence bien précise (voir ci-dessus). Ainsi, chaque communauté de référence possède une banque de données d'attributs de droits (BDAD) dans lesquels sont enregistrés tous les jeux d'attributs de droits de leurs patients (cf. figure 4).

Les attributs d'autorisation d'une identité électronique de patient sont mémorisés uniquement dans la communauté de référence. L'administration des autorisations s'effectue uniquement dans la communauté de référence. Un changement de communauté de référence signifie un transfert du kit des attributs de droits d'un patient de l'ancienne communauté de référence à la nouvelle.	Recommandation 12 Attributs de droits et l'administration de droits dans une communauté de référence

Vérification des droits d'accès

Tout contrôle d'accès commence par une vérification d'identité effectuée par la communauté demandeuse (techniquement dans le nœud demandeur), la vérification des autorisations s'effectuant sous la responsabilité de la communauté répondeuse (techniquement dans le nœud répondeur). La vérification des autorisations requiert l'accès à la communauté de référence du patient pour une lecture et une évaluation de ses attributs de droits. La gestion des personnes et des accès est donc distribuée entre communautés, comme le montre la figure 4.

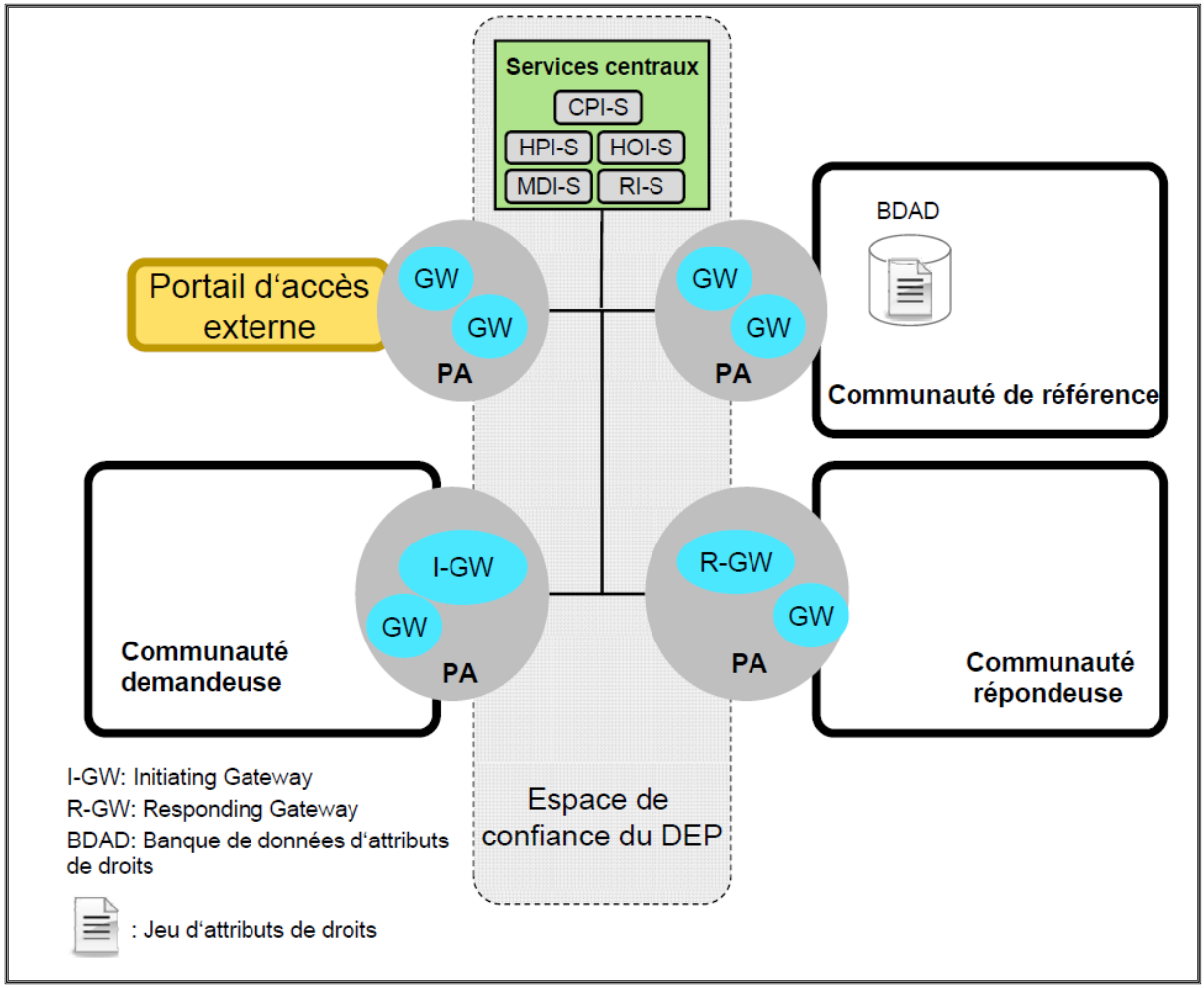

Figure 4 : Distribution de l'Identity and Access Management dans la communauté de référence

Une vérification des autorisations effectuée le plus tôt possible paraît judicieuse dans la mesure où elle permet d'éviter des actions inutiles en aval et qu'elle réduit les disséminations fautives de données dignes de protection. Tous les accès ne peuvent cependant pas être validés à l'avance.

Ainsi, lors d'un accès à un registre de documents, l'autorisation ne peut être accordée qu'une fois l'accès effectué parce que chaque résultat de recherche doit être vérifié séparément. Lors d'un accès à une archive de documents, par contre, la vérification doit avoir lieu avant l'accès proprement dit.

De manière générale, les accès sont toujours contrôlés le plus tôt possible au niveau des autorisations. En ce cas, le nœud passerelle répondant de la communauté ayant l'autorité sur les données vérifie et valide si les autorisations nécessaires sont données.	Recommandation 13 Vérification précoce des droits d'accès

3.3 Identification et authentification

Le profil d'intégration IHE:XUA n'a certes pas été développé pour une utilisation spécifique intercommunautaire, mais il peut toutefois être mis en œuvre sans modification par le positionnement ciblé des deux acteurs « User Authentication Provider » et « X-Assertion Provider ».	Recherche des identités entre communautés
Le profil d'intégration IHE:XUA doit être utilisé pour l'établissement fiable des identités dans les transactions intercommunautaires.	Recommandation 14 Utiliser également IHE:XUA pour l'identification intercommunautaire

4 Audit et notification

Objectif

L'audit (enregistrement des transactions) et la notification ont pour but de retracer fidèlement les accès et modifications au dossier du patient à l'attention de ce dernier.

La raison d'être de l'audit comme de la notification est de remplir les exigences de sécurité en matière d'intégrité et d'imputabilité. Leurs différences tiennent aux points suivants :

- Audit : Toutes les transactions relatives au DEP sont enregistrées dans un rapport d'événement. La création d'entrées ne peut être empêchée.
- Notification : permet de contacter le patient et de l'informer activement des transactions liées à son DEP. Les notifications peuvent être configurées et supprimées par le patient. Toute manipulation du DEP déclenche le processus.

Dispositions relatives à la protection des données

Les fichiers de procès-verbaux peuvent toutefois être consultés également par d'autres voies (p. ex. par des administrateurs), raison pour laquelle ces fichiers ne doivent contenir aucune donnée sensible telle que des contenus des documents médicaux. Les administrateurs ont cependant besoin d'un minimum d'informations comme certaines métadonnées des documents, pour faire leur travail. Comme ces métadonnées peuvent contenir des informations confidentielles, les administrateurs doivent être tenus à des règles et des processus définis.

Recommandation 15

Evénements d'accès seulement, pas de résultats

De manière générale, seuls les événements d'accès avec leurs paramètres de recherche sont à mémoriser dans les fichiers journaux du système. Les résultats même des recherches, p. ex. les contenus de documents, ne doivent pas être mémorisés.

Recommandation 16

Administrateurs dans les communautés

Il n'y a pas de rôles d'administrateurs préposés à plusieurs communautés. Un administrateur est responsable d'un seul système ou d'une seule communauté. Tous les accès, y compris ceux des administrateurs, sont consignés dans un fichier journal.

Standardisation des entrées d'audit

Pour être conçues d'une manière utile aux patients, les entrées techniques d'audits doivent être rédigées de manière uniforme et standardisée à l'échelle nationale. Ces entrées doivent être intelligibles pour les patients et présenter une granularité raisonnable. Elles doivent répondre au minimum aux questions suivantes :

- Quand l'événement est-il survenu (timbre horodateur)?
- Quelle communauté/quel système est concerné ?
- Qui a déclenché l'action (identification de la personne/du rôle/de la communauté) ?
- Quelle communauté/quel système est concerné ?
- Sur quel objet d'information (N° d'identification du document, son titre, sa date, type de document, auteur) l'accès s'est-il produit ?
- Quelle a été l'action effectuée? En lecture ou en écriture ?

- Si modification de consentements et de droits : quels droits a-t-on modifiés et comment ? Toute modification de la matrice des droits est inscrite dans un fichier procès-verbal.
- L'action a-t-elle réussi ? Les tentatives d'accès infructueuses sont également inscrites dans le fichier procès-verbal.

On peut également définir d'autres événements à inscrire obligatoirement au procès-verbal, par exemple la défaillance technique d'un système.

Les directives et réglementations pour les administrateurs du système et la durée de conservation des données de journal du système sont à définir juridiquement.

Faciliter au patient la consultation des entrées d'audit

Tout patient a en tout temps le droit de consulter les entrées d'audit qui le concernent en provenance de toutes les communautés, avec toutes les entrées d'audit à son dossier de patient. Il existe différentes variantes dans les manières de garantir ce droit :

1. La notification active par chaque communauté des événements locaux concernant le patient à sa communauté de référence (pull on notification).
2. L'attente passive par chaque communauté de la réception d'une demande de lecture d'audit. Pour afficher tous les accès, envoi de demandes aux communautés depuis un portail d'accès (externe et internes) et lecture ad hoc des entrées d'audit locales (pull on request).
3. Evaluation périodique des événements locaux par chaque communauté, laquelle intègre ensuite le résultat sous forme de document procès-verbal autonome dans le dossier du patient.

Pour les variantes 1 et 2, il n'existe actuellement aucun profil IHE approprié et il faudrait en définir de nouveaux. Dans la variante 2, au-delà d'une durée de conservation d'une année, la traçabilité d'accès plus anciens n'est plus assurée.

Des entrées d'audit sous forme de « document »

Dans la variante 3, que nous recommandons, les communautés analysent périodiquement les entrées d'audit à un rythme choisi par le patient (p. ex. quotidiennement). A l'aide des métadonnées, ce document est enregistré comme type de document propre (extrait d'audit) au plus haut niveau de confidentialité (secret) dans le registre de documents de la communauté, à l'instar d'autres documents médicaux. Tous les extraits d'événements système correspondant à une identification définie de patient sont automatiquement générés sous forme de documents structurés (CDA Body Level 3). Chaque extrait doit aussi être présenté sous forme de document indépendant utilisable par le lecteur. Le patient peut ainsi consulter à tout moment les entrées d'audit qui le concernent en provenance de toutes les communautés en recourant aux mécanismes d'interrogation ordinaires.

Les communautés évaluent périodiquement les rapports d'événement et génèrent automatiquement des documents journaux centrés sur le patient au format CDA Body Level 3. Ils sont traités comme des documents médicaux.	Recommandation 17 Documents journaux centrés sur les patients dans chaque communauté

Le patient peut choisir le rythme (quotidien, hebdomadaire, mensuel) auquel le rapport d'événement est généré. Il peut aussi modifier le niveau de confidentialité préréglé et étendre aux professionnels de la santé le droit de consulter ses données d'audit. Les entrées d'audit (p. ex. modification de droits, annonce de départ) doivent être maintenues dans un souci de traçabilité. Elles peuvent être requises pour les besoins de la médecine légale ou à d'autres fins juridiques plusieurs années après l'événement. Le patient peut cependant aussi exiger en tout temps que des documents d'un certain type ne soient plus affichés.

Le délai de conservation des documents centrés sur le patient et des entrées audit est défini par le droit.

5 Portail d'accès

Le portail d'accès est un élément fondamental de l'« Architecture eHealth Suisse » (cf. définition page 7f). Il permet aux patients d'accéder, en tout lieu et à toute heure, aux données de leur propre dossier électronique du patient (DEP), sans l'aide d'un tiers, et ceci de manière sécurisée et traçable. En outre, le patient peut régler l'accès aux données à l'aide de consentements individuels et d'octroi de droits. Il s'agit de la seule composante de l'architecture qui s'adresse directement au citoyen ou au patient. Grâce à sa forte visibilité, il contribuera de manière déterminante à l'acceptation et à la réussite du système « Cybersanté » Suisse.

Elément central de l'« architecture Cybersanté Suisse ».

Les portails d'accès permettent l'interaction entre les utilisateurs, tel que le patient et les professionnels de santé, avec l'espace de confiance du DEP. Au point d'accès, ils sont techniquement identiques aux communautés. En d'autres termes, tous les nœuds passerelles (gateways) fonctionnent de manière identique dans leur interface extérieure, qui doit être certifiée. Il n'existe pas de cas particulier concernant les portails d'accès.

Les portails externes se comportent comme les communautés

Les portails d'accès existent en deux variantes :

- Des portails d'accès internes peuvent être placés *à l'intérieur* d'une communauté et communiquer via le point d'accès de cette communauté.
- Des portails d'accès externes peuvent aussi, *indépendamment* d'une communauté, communiquer directement avec d'autres points d'accès de communautés via leurs propres points d'accès.

Recommandation 18

Deux variantes de portails d'accès

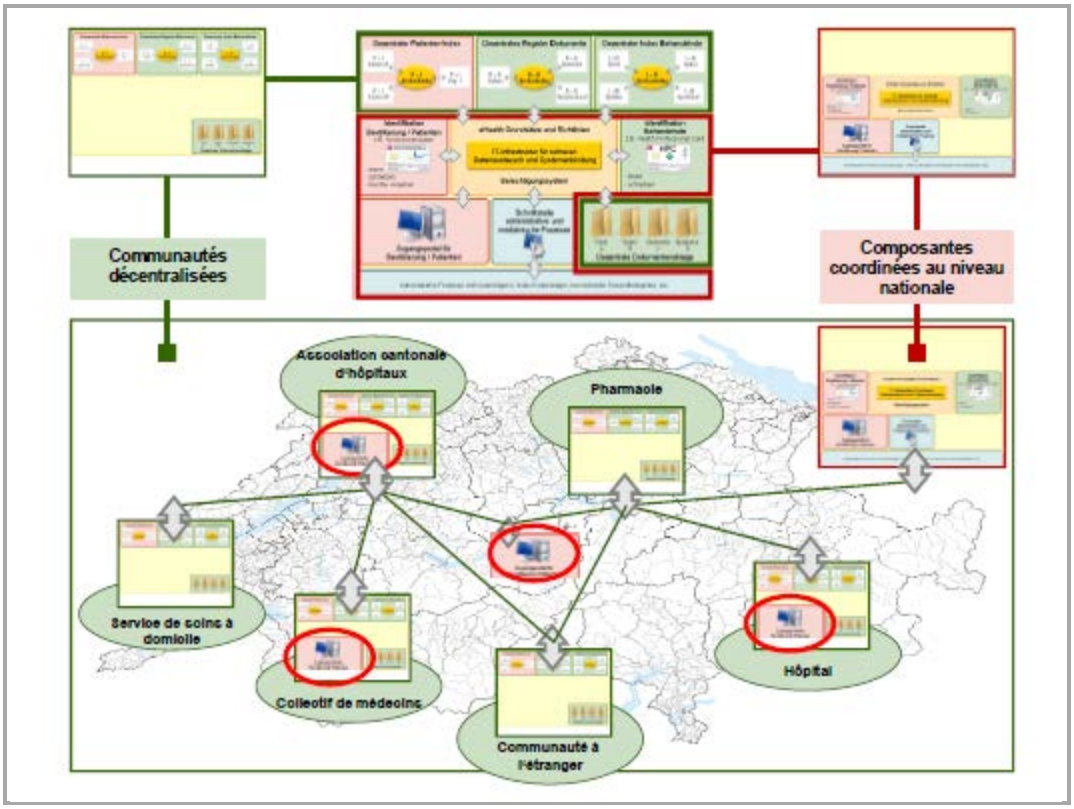

Figure 5 : Deux variantes de portails d'accès, interne et externe

Lors de la communication entre les communautés, il existe une limitation réciproque, à savoir, l'accès ne se fait qu'en lecture seule. Les professionnels de santé ne peuvent donc publier des documents que dans la communauté dont ils sont membres. Les patients peuvent uniquement publier leurs propres données via le portail d'accès interne de la communauté de référence qu'ils ont choisie. La gestion des autorisations par le patient intervient exclusivement dans la communauté de référence (voir le tableau du chapitre 1.3).

Accès en lecture seule uniquement entre les communautés

Pour une diffusion plus rapide et pour favoriser l'acceptation de la « cybersanté », il pourrait être judicieux de permettre un accès facile et sécurisé au DEP pour les professionnels de la santé qui ne sont pas (encore) membres d'une communauté. Ainsi, il serait technique-ment possible de concéder un accès en lecture seule aux professionnels de la santé en tant qu'utilisateurs tiers d'un portail d'accès externe, sous réserve d'obtention du consentement explicite du patient. Par cette option d'accès « facile » au système DEP, la motivation des professionnels de santé de devenir membre d'une communauté risque de diminuer. Le projet législatif devra clarifier si un tel accès en lecture seule et éventuellement sa durée sera concédé aux professionnels de santé non membres d'une communauté.

Portail d'accès externe à un accès plus large

Par les portails d'accès externes, les patients ont un accès en lecture à leurs données du dossier électronique du patient.

Les professionnels de la santé, qui ne sont pas membres d'une communauté ont par des portails d'accès externes seul un accès en lecture sur le dossier électronique du patient. L'autorisation d'accès doit être attribuée d'une manière explicite par le patient.

Recommandation 19

Portail d'accès externe pour patients et professionnels de la santé

Les patients doivent pouvoir eux-mêmes rendre accessibles des données via le portail d'accès (interne), par exemple leurs disponibilités ou les données d'évolution de leur poids ou de leur tension artérielle	Documents des patients
La publication de documents est possible par des portails d'accès internes au sein de la communauté. En outre, d'autres services (p. ex. webservices) peuvent être utilisés au sein de la communauté. Les portails d'accès *externes* indépendants qui ne font pas partie d'une communauté ne permettent que l'accès intercommunautaire en lecture seule.	Recommandation 20 Publication de documents
Les portails d'accès internes des communautés, qui supportent le téléchargement de documents sur le réseau, sont tenus d'enregistrer, dans les métadonnées du document, l'identité et le rôle (patient ou professionnel de la santé) de l'utilisateur procédant au téléchargement. Afin de permettre l'évaluation de la validité des données, il doit exister, dans la présentation des documents, une distinction visuelle claire entre les documents envoyés par un professionnel de la santé ou par un patient (p.ex. en séparant visuellement les différents domaines).	Obligation de contrôle de l'identité
Le portail d'accès (interne ou externe) met à disposition des afficheurs appropriés pour visualiser les types de documents définis dans les métadonnées. L'interface d'utilisateur doit démontrer d'une manière visible si les données ont été téléchargées par des professionnels de la santé ou par le patient.	Recommandation 21 Affichage de données
La gestion des identités numériques revêt un rôle particulièrement important dans l'échange intercommunautaire de données. Les portails d'accès (internes ou externes) prennent en charge ces responsabilités en attribuant des identités de manière autonome ou par le biais d'un service d'identité (Identity Service). Tant que la question de l'identificateur national des patients / personnes n'est pas clarifiée, le portail d'accès attribue les identifications selon ses propres règles. La condition de validité dans ce contexte repose sur le caractère univoque des identifications au sein du lieu de délivrance. Pour cela, on peut avoir recours au concept OID, qui garantit, avec le Root-ID et le Child-ID, le caractère absolument univoque de tous les identificateurs.	Rôle du portail dans l'identification
Chaque communauté et chaque portail d'accès externe doit vérifier, lors de l'inscription des utilisateurs, l'attribution des bonnes métadonnées à leur identité (par exemple le nom, le prénom, le sexe, la date de naissance et les différentes identifications issues des autres communautés). Ces attributs seront fournis lors des consultations intercommunautaires - par exemple les consultations du service HPI, les demandes de documents, les demandes d'autorisations à la communauté de référence. Les moyens d'authentification des utilisateurs supportés par les portails d'accès doivent être enregistrés et actualisés en interne. Ils doivent contenir, pour l'enregistrement (login), toutes les métadonnées pertinentes de l'identification de la personne. Chacun de ces utilisateurs valables, enregistrés en tant que patient ou professionnel de la santé, peut ainsi se connecter au portail d'accès. Plusieurs moyens d'authentification, légalisés dans la loi future, peuvent être utilisés - par exemple les Smartcards (carte d'accès électronique), les clés USB avec signature, procédés smsTAN, etc.	Enregistrement

Le fournisseur de portail choisit les moyens d'authentification légalement autorisés qu'il propose sur son portail à ses utilisateurs.	Recommandation 22 Choix des moyens d'authentification
Les principaux cas d'utilisation des portails d'accès concernent les données administratives et médicales d'un patient. Cependant, d'autres informations « tierces » peuvent en principe être également intégrées dans le portail, à condition d'être clairement séparées du dossier électronique du patient - il peut par exemple s'agir d'informations externes sur les maladies ou les traitements, de liens vers des forums médicaux ou d'informations publicitaires déclarées. Afin de renforcer la transparence et la crédibilité, il est recommandé : ➢ de proposer sur le portail un moteur de recherche renvoyant uniquement à des informations transparentes et dignes de confiance, par exemple des sites Internet certifiés HONcode ; ➢ de n'indiquer que des liens vers des sites relatifs à la santé dignes de confiance, en d'autres termes des pages respectant le code de conduite HONcode ou certifiées HONcode ; ➢ de mettre à disposition des registres de partenaires et de prestataires de santé (services d'urgences, hôpitaux, cliniques, médecins, assurances) ; ➢ d'informer clairement l'utilisateur final sur les sources des informations, de sorte à renforcer la confiance accordée au portail ; ➢ d'expliquer à tous les groupes cibles la façon d'utiliser le portail ; Des certifications complémentaires par des labels de qualités sont possibles.	Transparence et confiance
Les portails d'accès remplissent le HONcode de la Fondation Health on the Net: Les normes, principes et recommandations relatives à la qualité des informations de santé, à l'accès et à la convivialité du portail d'accès sont prises en considération dans tous les processus.	Recommandation 23 Certification HONcode
Les portails d'accès sont utilisables sans restriction par tous les patients, quelles que soient leurs ressources physiques ou techniques. Pour optimiser l'accès sans barrière au portail, comme l'exige la certification HONcode, il est recommandé de suivre les directives du Consortium World Wide Web (W3C) pour des contenus Web sans barrière (WCAG) 2.0 ainsi que les recommandations pour l'accessibilité des contenus (User Agent Guidelines) des navigateurs Web et lecteurs de médias. L'absence de barrière peut être utilisée comme caractère distinctif par les fournisseurs de portails.	Recommandation 24 Absence de barrières

6 Conclusions

En bref

Les présentes Recommandations IV fournissent les définitions et spécifications manquantes des composantes et services généraux à régler au niveau central. Ainsi, il devrait être possible de commencer à mettre en œuvre de manière concrète des mesures de niveau de maturité 2 dans le contexte documentaire central et d'aborder les thèmes importants, tels que le contrôle des accès et l'audit/enregistrement au niveau intercommunautaire. Sans description plus détaillée des composantes au niveau suisse, l'échange de données entre les communautés est impossible.

Etapes

Pour la prochaine étape qui débutera en 2013, il est prévu que les travaux dans le domaine de « Normes et architecture » se concentrent sur trois dimensions. D'une part, il est nécessaire de démontrer de manière approfondie, dans le contexte du démarrage de projets conformes à la stratégie, comment les recommandations actuelles I à IV peuvent être mises en œuvre dans la pratique. D'autre part, les connaissances acquises jusqu'ici doivent être élargies et complétées afin qu'elles puissent servir à soutenir de manière optimale les projets de mise en œuvre. Enfin, Il est également nécessaire de concevoir comment il est possible de continuer à développer le concept actuel afin qu'il ne tienne aussi compte des futures exigences. La priorisation des thèmes présentés ci-dessous sera réalisée dans le cadre des travaux de planification.

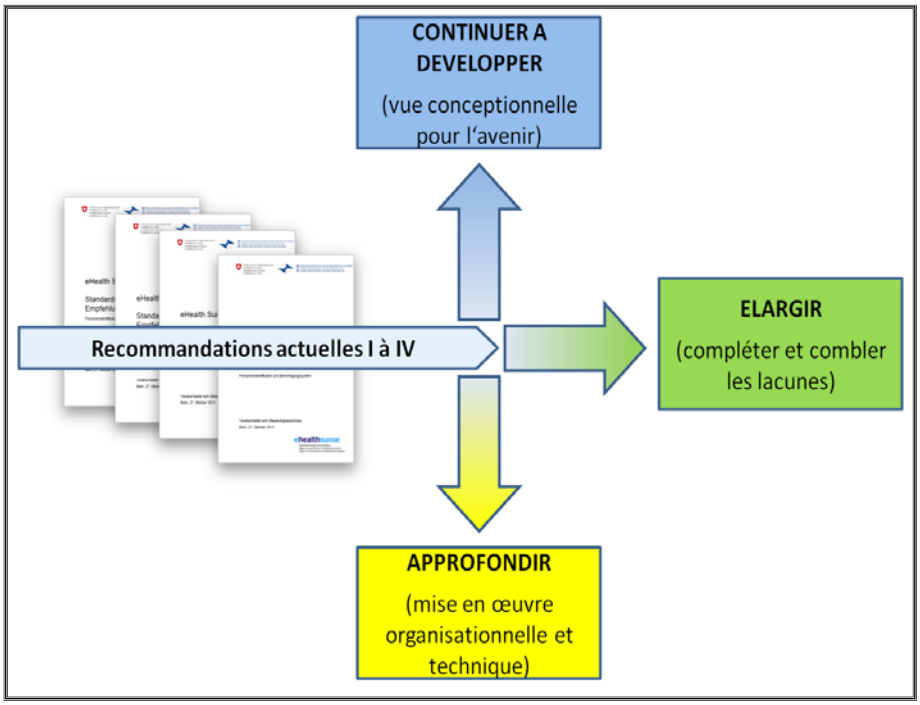

Figure 6: Dimensions de planification pour les futurs travaux

Description détaillée de la mise en œuvre organisationnelle et technique des recommandations actuelles:

- Guide pour la constitution de communautés (description conceptuelle de la mise en commun des recommandations I à IV);
- Instructions techniques pour la mise en œuvre des recommandations I à IV (guide pour l'implémentation technique).

1ère Dimension :

Approfondir

APPROFONDIR

(mise en œuvre organisationnelle et technique)

Complément des éléments nécessaires et comblement des lacunes dans les travaux conceptuels existants:

- Définition de la procédure pour l'élaboration du contenu du DEP, en particulier la coordination des experts en charge de définir ce contenu ;
- Contexte de traitement et d'autorisation: pour une gestion des droits d'accès proche de la pratique, qui utilise des caractéristiques d'identification et des métadonnées de documents. Le contexte de traitement doit être saisi de manière correcte, comme le choix des plages de valeurs des métadonnées et des listes d'attributs des services centraux ainsi que définition des métadonnées XCA pour une « configuration initiale »;
- Test d'une solution technique et organisationnelle intermédiaire pour les services centraux, en particulier le HPI-S et le HOI-S;
- Définition des composantes d'architecture « interface des processus médicaux et administratifs », en particulier, les fonctionnalités d'exportation et d'importation pour les documents du DEP, les attributs de droits d'accès et les déclarations de consentement.

2ee Dimension :

Elargir

ELARGIR

(compléter et combler les lacunes)

Poursuite des développements conceptuels des bases existantes de « Normes et architecture » :

- Perspective en vue du degré de maturité 3 (voir pages 5 à 7), en particulier l'utilisation des informations médicales structurées, qui sont actualisées par plusieurs professionnels de la santé au-delà des limites de la communauté ("shared documents");
- Concept pour la suppression de données: que se passe-t-il si un patient décède ou s'il quitte une communauté? Il est nécessaire de fixer une réglementation unique tenant compte des directives de protection des données et de définir sa mise en œuvre technique.

3e Dimension :
Continuer a developper

CONTINUER A DEVELOPPER

(vue conceptionnelle pour l'avenir)

D'autres thèmes, tels que les conditions de certification et la définition des exigences non fonctionnelles pour les communautés et des portails d'accès seront traités dans le cadre de la loi fédérale sur le dossier électronique du patient.

Responsabilités dans le contexte du projet de loi LDEP

Dans l’intérêt de la protection des investissements, le Comité de pilotage de « eHealth Suisse » recommande à tous les acteurs qui procèderont à des investissements nouveaux ou de remplacement dans le domaine informatique, de garantir à leurs niveaux de responsabilité respectifs l’observation des solutions et les approches techniques recommandées dans le projet partiel « Normes et architecture ».

Respect des recommandations dans l'intérêt de la protection des investissements

Annexe 1 : Principes architecturaux pertinents

Les recommandations I-III du projet partiel « Normes et architecture », citées ci-dessous, sont consultables à l'adresse suivante : http://www.e-health-suisse.ch/umsetzung/00146/00148/index.html?lang=fr

1. La standardisation est axée sur les processus, les cas d'utilisation étant basés sur l'initiative IHE (Integrating the Healthcare Enterprise), avec notamment les profils d'intégration du domaine de l'infrastructure TI
   [Recommandations I], p.7
2. Eléments de base de l'« Architecture eHealth Suisse » [Recommandations I], p.6
3. L'échange de documents en Suisse repose sur des communautés jouissant des mêmes droits qui communiquent via un ou plusieurs points d'accès.
   [Recommandations II, Recommandation 1, p. 10)
4. Un registre national des communautés sera tenu. Seules celles-ci auront la possibilité de participer à l'échange de documents.
   [Recommandations II, Recommandation 3, p. 12)
5. Tous les rôles autorisés seront consignés dans un registre national. Chaque rôle sera caractérisé par un code d'identification univoque.
   [Recommandations II, Recommandation 5, p. 16)
6. L'autorisation est octroyée par le patient pour un temps déterminé à une personne désignée assumant un certain rôle, et elle lui permet d'accéder à une partie spécifique de ses documents. Cette procédure s'effectue sous la forme d'un « consentement ».
   [Recommandations II, Recommandation 6, p. 17)
7. Les listes d'inclusion (appelées aussi « whitelists » ou listes blanches) contiennent l'identité de personnes qui ont le droit d'accéder aux documents d'un patient, comme par exemple une personne de confiance. Les listes d'exclusion (encore appelées « blacklist » ou listes noires) mentionnent l'identité de personnes auxquelles l'accès aux documents du patient est interdit. A cet effet, il faut pouvoir attribuer une identité à ces personnes.
   [Recommandations II, Recommandation 7, p. 17)
8. Configuration initiale des métadonnées
   [Recommandations II], Recommandation 9, p. 21
9. L'identification unique de personnes entre communautés sera assurée par le recours à un identifiant univoque à l'échelle nationale, qui pourra être utilisé en association avec d'autres caractéristiques à des fins d'identification des personnes entre communautés. Ceci est valable pour les professionnels de la santé et les patients.
   [Recommandations III, Recommandation 1, p. 17)
10. Il y a lieu d'assurer un processus d'authentification fort en recourant à une combinaison appropriée de connaissance, de possession d'un moyen d'identification et de caractéristiques biométriques.
    [Recommandations III, Recommandation 2, p. 17)
11. Consentement et droits d'accès
    [Recommandations III], recommandation 3, p. 19
12. Définition des niveaux de confidentialité
    [Recommandations III], recommandation 4, p. 20
13. Droits régissant le consentement de principe
    [Recommandations III], recommandation 5, p. 22
14. Autorisations par recours aux rôles
    [Recommandations III], recommandation 6, p. 23
15. Détermination individuelle des droits d'accès
    [Recommandations III], recommandation 7, p. 24
16. Tous les consentements, de même que les droits octroyés par un patient seront gérés dans une même communauté. Cette communauté sera désignée par le terme de « communauté de référence ». Il devra s'agir impérativement d'une communauté certifiée. Le patient pourra choisir librement de définir l'une des communautés certifiées comme sa communauté de référence. Il ne sera pas tenu de registre central dans lequel l'appartenance des patients à leur communauté

de référence sera mentionnée.
[Recommandations III, recommandation 8, p. 24)

17. Traçabilité, historisation et audit
[Recommandations III], recommandation 9, p. 25

Annexe 2 : Indications techniques

Indications techniques « Composantes et services centraux »

Système de gestion univoque du service de registre des communautés et des portails d'accès externes

Pour une communication digne de confiance entre les communautés, il est nécessaire que les composantes et les services centraux satisfassent également à des critères de qualité élevés. A cette fin, ceux-ci devront aussi faire l'objet de vérifications techniques. Un système de gestion univoque des versions de tous les services et registres est nécessaire pour toutes les demandes et réponses du système. Le service de registre des communautés et les portails d'accès extérieurs (CPI-S) contiennent un système de gestion univoque avec toutes les versions intermédiaires.

Registre des communautés et des portails d'accès externes notifiés

Les communautés doivent être informées en cas de modifications dans la liste des communautés certifiées. Ainsi seulement, elles pourront exploiter toutes les sources d'informations disponibles sur un patient lors d'une consultation. Toutes communautés sont activement informées de la part du registre des communautés et des portails d'accès externes concernant les changements. Ceci doit servir de déclencheur pour une mise à jour de la liste des communautés certifiées et des portails d'accès externes.

Indications techniques « Identification et authentification »

Identification des participants du système selon le concept OID

Afin de permettre une utilisation à bon escient des déclarations de consentement et des autorisations, une identification internationale univoque des participants au système doit être mise en place. Dans la mesure où il existera toujours des instances organisationnelles différentes, identifiant les participants à leur système, seule une combinaison de l'identification de la personne et du lieu de délivrance permettra de garantir le caractère non équivoque à l'échelle internationale (p. ex. GS1 GLN d'un médecin et OID pour le GLN 7601234567890 et 1.3.88 ou 2.51.1.3). Le concept OID pour la Suisse a été adopté en 2010 par le Comité de pilotage d'« eHealth Suisse ».

Pointeur sur fournisseurs X-Assertion dans CPI-S

Pour une mise en œuvre durable du profil d'intégration IHE:XUA au-delà des limites communautaires, il faut prévoir l'insertion d'une information supplémentaire dans le service de registre des communautés (CPI-S). Les nœuds passerelles répondeurs pourront ainsi déterminer la manière de retrouver le fournisseur d'assertion (Assertion Provider) dans le nœud passerelle demandeur. Le registre des communautés administre ce qu'on appelle des pointeurs (indicateurs) sur un fournisseur X-Assertion d'accès et les met avec les service Web à disposition des noeuds passerelles répondeurs.

Indications techniques « Concept d'autorisation »

D'après les Recommandations II et III, une interaction est nécessaire entre les différentes composantes du système et objets d'information afin de satisfaire à toutes les exigences en matière de contrôle des autorisations. Conformément à la description fournie dans le chapitre 3.2 précédent, on prévoit un système de distribution de Management de personnes et d'accès. La succession des étapes pour une recherche intercommunautaire de données est décrite ci-après.

1. Vérifier l'identité du professionnel de la santé demandant ans la communauté demandeuse ;
2. Une assertion SAML contient un identificateur des professionnels de la santé (p.ex. le numéro GS1 GLN) ;
3. Rechercher dans la communautés de référence et consulter de l'attribution des droits;
4. Compléter l'assertation SAML avec l'attribution de droits d'accès (incl. ID du patient) ; Vérifier auprès du nœud demandeur, si la demande est admissible (demande à un archive de documents (repository) ;
5. Vérifier dans le Initiating Gateway, si la demande est autorisée (demander au repository) ;
6. Compléter tous les identificateurs des patients des autres communautés ;
7. Envoyer la demande à tous les nœuds repondeur pour lesquels ;il existe un identificateur du patient :
8. Le nœud repondeur transfère la demande à la propre communauté ;
9. La communauté traite la demande et vérifie l'autorisation de tous les résultats. Dans le cas normal, la vérification des droits est un élément intégral du registry et du repository ;
10. La réponse arrive chez le nœud repondeur et est transmise au nœud demandeur si l'autorisation existe ;
11. Le nœud demandeur vérifie pour sa propre communauté la réponse (demande registry) ;
12. Le nœud demandeur attend que toutes les réponses soient de retour ou qu'un limite de temps soit signalisée ;
13. Le nœud demandeur combine toutes les réponses et les livre au point demandeur.

La communauté répondeuse n'étant pas systématiquement la communauté de référence, un mécanisme de délégation est nécessaire entre les communautés pour les attributs d'octroi de droits d'un patient. Par conséquent : si la communauté de référence n'est pas disponible dans le système « Cybersanté » Suisse, et que l'on ne peut donc pas accéder aux attributs d'octroi de droits du patient, on obtiendra en réponse une liste de résultats vide.

Attributs d'octroi de droits en tant que partie de l'assertion SAML

Avant leur transmission, les attributs d'octroi de droits sont préparés et signés numériquement sous forme de fichier XML (jeu d'attributs) par l'office compétent de la communauté de référence du patient. Ce jeu d'attributs d'octroi de droits est intégré en tant qu'attribut dans l'assertion SAML pour la transmission intercommunautaire.

Vérification des droits par le portail répondeur (responding gateway)

Le nœud passerelle répondeur vérifie le contenu de l'identification et des attributs fournis (via l'assertion SAML d'IHE:XUA) en les comparant avec les autorisations actuellement en vigueur et peut décider sur cette base d'accorder ou de refuser l'accès. Ceci fait du nœud passerelle répondeur un « Access Enforcement Point » qui décide de permettre ou non une transaction entre les communautés.

Le lien entre le système de distribution de l'Identity and Access Management (IAM) et le Access Enforcement Point est schématisé dans la figure 7.

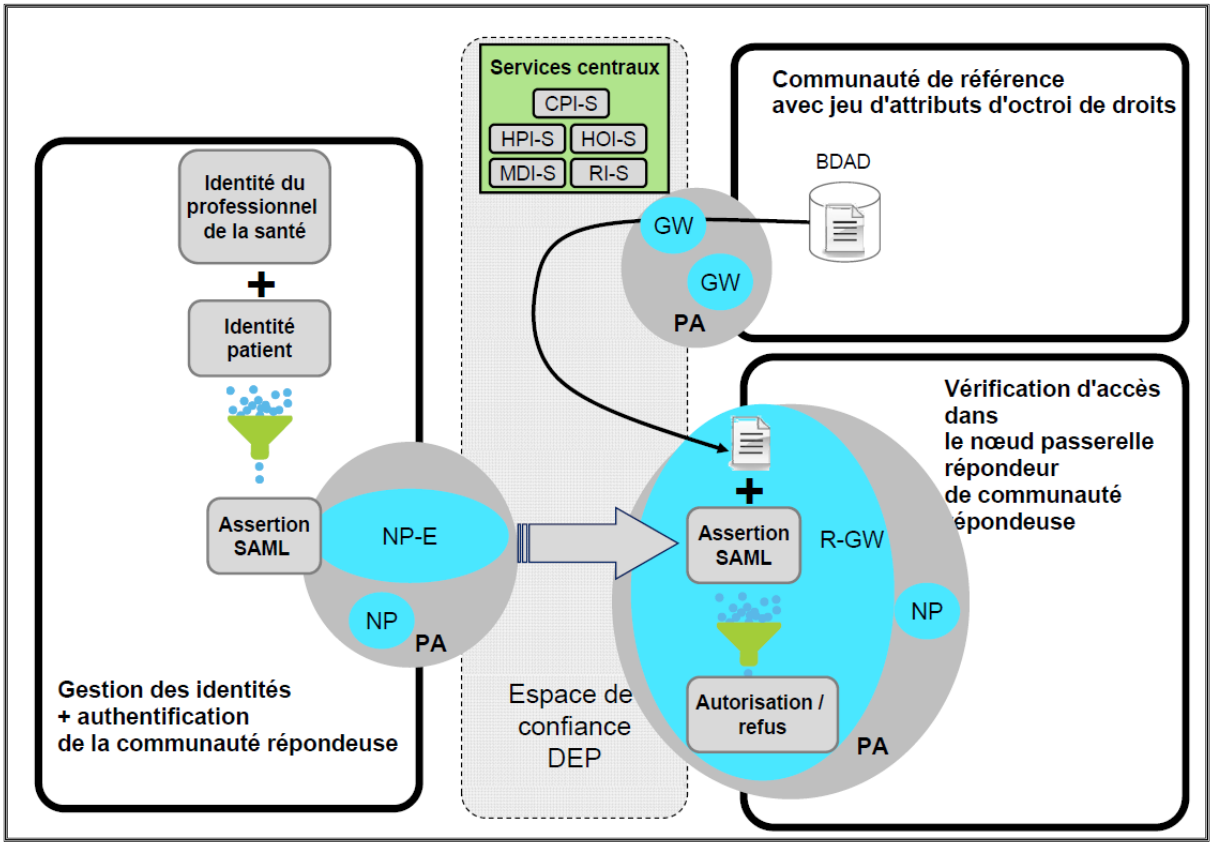

Figure 7 : Interactions au sein du concept d'autorisation

Indications techniques « Audit et notification »

Le profil IHE ATNA (Audit Trail and Node Authentication) définit la manière dont les ordinateurs centraux (Hosts) sont protégés, de même que le type d'informations et la manière dont elles sont consignées. Les journaux d'audit (Audit Logs) créés dans le cadre de l'ATNA présentent une granularité fine et sont très techniques. L'ATNA se limite à un « IHE affinity domain » et ne définit pas d'accès intercommunautaire.

Mise en œuvre avec les profils IHE

L'ensemble des systèmes et applications participants présentant des dépendances temporelles et leurs événements devant être consignés avec un horodatage fiable, leurs horloges doivent être synchronisées.

Les communautés synchronisent leurs systèmes selon le profil d'intégration IHE Consistent Time (CT).

Synchronisation selon IHE:CT

Les communautés consignent les événements déclencheurs dans un journal système local selon le profil d'intégration IHE Audit Trail and Node Authentication (ATNA).

Evénements déclencheurs selon IHE:ATNA

Annexe 3 : Attributs services CPI-S (Registre des communautés)

Attribut	Nom complet	Explication
ComName	Nom de la communauté	Nom de la communauté. Cette désignation doit être univoque et explicite. Elle est employée pour nommer la communauté sur le portail et peut être utilisée par les patients ou les professionnels de la santé lors du choix de leur communauté de référence ou de la définition des attributs d'octroi de droits.
ComInfo	Informations sur la communauté	Informations descriptives générales sur la communauté (texte libre, 500 caractères max.)
ComLogo	Logo de la communauté	Logo graphique de la communauté au format .JPG
ComLegal	Bases juridiques de la communauté	Texte libre décrivant les bases juridiques de la communauté, en renvoyant p. ex. à la Loi cantonale sur la santé ou à la Loi Fédérale relative au dossier électronique du patient, ou encore à des conventions privées au niveau de la communauté
ComContact	Coordonnées de la communauté	Les coordonnées de la communauté sont consignées dans CPI-S , permettant de prendre contact directement avec la communauté. Ces informations sont transmises par les autres communautés aux professionnels de la santé et aux patients. Pour la collaboration intercommunautaire, on consignera les coordonnées d'un autre interlocuteur (technique), qui ne sera sollicité que pour des questions internes. Pour chaque interlocuteur, il faut enregistrer au moins deux méthodes de contact (adresse postale, E-mail et téléphone).
ComOID	OID de la communauté	Chaque communauté doit recevoir un OID univoque qui l'identifie sans équivoque à l'échelle internationale. Celui-ci doit figurer dans le Registre suisse des OID.
ComAuthN	Fournisseur de l'authentification de la communauté	Chaque communauté doit avoir au moins un fournisseur d'authentification, qui signe les assertions SAML au nom de la communauté. Tous les certificats X.509 en cours de validité sont enregistrés dans cet attribut.
ComAssert	Autorité d'assertion de la communauté	Pour remplir son rôle de communauté de référence, chaque communauté doit utiliser un service d'assertion qui procède à la signature numérique des attributs d'octroi de droits. Les informations nécessaires pour la vérification de ces signatures sont enregistrées dans CPI-S.
ComXPoint	Pointeur sur un fournisseur d'accès X-Assertion	Information consultable par les nœuds passerelles répondeurs voulant contacter les nœuds passerelles demandeurs.
ComGW	Point d'accès de la communauté	Chaque communauté doit posséder au moins un nœud passerelle qui traite la communication entre les communautés. Les URLs du nœud passerelle sont enregistrées dans cet attribut.

Attribut	Nom complet	Explication
ComVersion	Version de la communauté	Version du nœud passerelle pour laquelle la communauté a reçu sa certification
ComZert	Date de certification	Date de l'obtention de la certification ou de la recertification