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

Mobile Health et le dossier électronique du patient

Recommandations relatives à l'utilisation de normes et standards techniques

Adoptées par le comité de pilotage

Berne, le 27 septembre 2018

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

Centre de compétences et de coordination
de la Confédération et des cantons

Centro di competenza e di coordinamento
di Confederazione e Cantoni

Impressum

Auteurs *:* Christian Kohler, Oliver Egger, Martin Smock

Informations supplémentaires et diffusion :
www.e-health-suisse.ch

But et positionnement du présent document

Le présent document a pour but de préconiser des normes et des standards pour le domaine de la santé mobile permettant de faire communiquer différents systèmes moyennant un travail d'implémentation raisonnable. La priorité a été donnée aux normes et standards reconnus internationalement.

Pour faciliter la lecture, la forme générique est utilisée pour désigner les deux sexes.

Table des matières

Table des figures

Résumé

Contexte et mandat

Contexte

L'organe de coordination eHealth Suisse orchestre les travaux de mise en œuvre du dossier électronique du patient et de la cybersanté au niveau des cantons et de l'Office fédéral de la santé publique.

Le Parlement a adopté la loi sur le dossier électronique du patient (LDEP) le 19 juin 2015. Cette loi prévoit à l'art. 8, al. 2, que les patients peuvent saisir leurs propres données ou documents dans leur dossier électronique. Des instruments simples à utiliser, notamment des applications mobiles, doivent donc être proposés aux patients.

Objectif

La question de l'interopérabilité est de grande importance pour la santé mobile (mHealth), car la population enregistrera des données de santé ou des constantes vitales au moyen de divers appareils ou applications mobiles, ces données pouvant ensuite être versées au dossier électronique du patient sous forme de documents. eHealth Suisse entend recommander des standards et des normes permettant une communication intersystémique sans grand travail d'implémentation.

Mandat

Il s'agit d'élaborer un document proposant des recommandations sur l'utilisation de standards techniques en santé mobile, en mettant l'accent sur les normes reconnues au niveau international.

Procédure

L'enregistrement et la lecture de documents se fondent sur les transactions décrites dans la figure ci-dessous, publiée par eHealth Suisse dans « mHealth et le DEP – un cas d'application concret [1] ». Les initiatives et standards internationaux pertinents en lien avec ces transactions sont identifiés, expliqués et évalués ; l'élément le plus adéquat est proposé comme recommandation. Les transactions se rapportant au cas d'application portent la mention CAn (n = numéro de la transaction). Pour pouvoir catégoriser et évaluer les standards correspondants, le cas d'application a été complété de manière à permettre au patient, monsieur Winter, de visionner à nouveau le rapport initialement publié dans le DEP au moyen de l'application se trouvant sur son appareil mobile.

[1] https://www.e-health-suisse.ch/fr/mise-en-oeuvre-communautes/activites-ehealth/mhealth.html

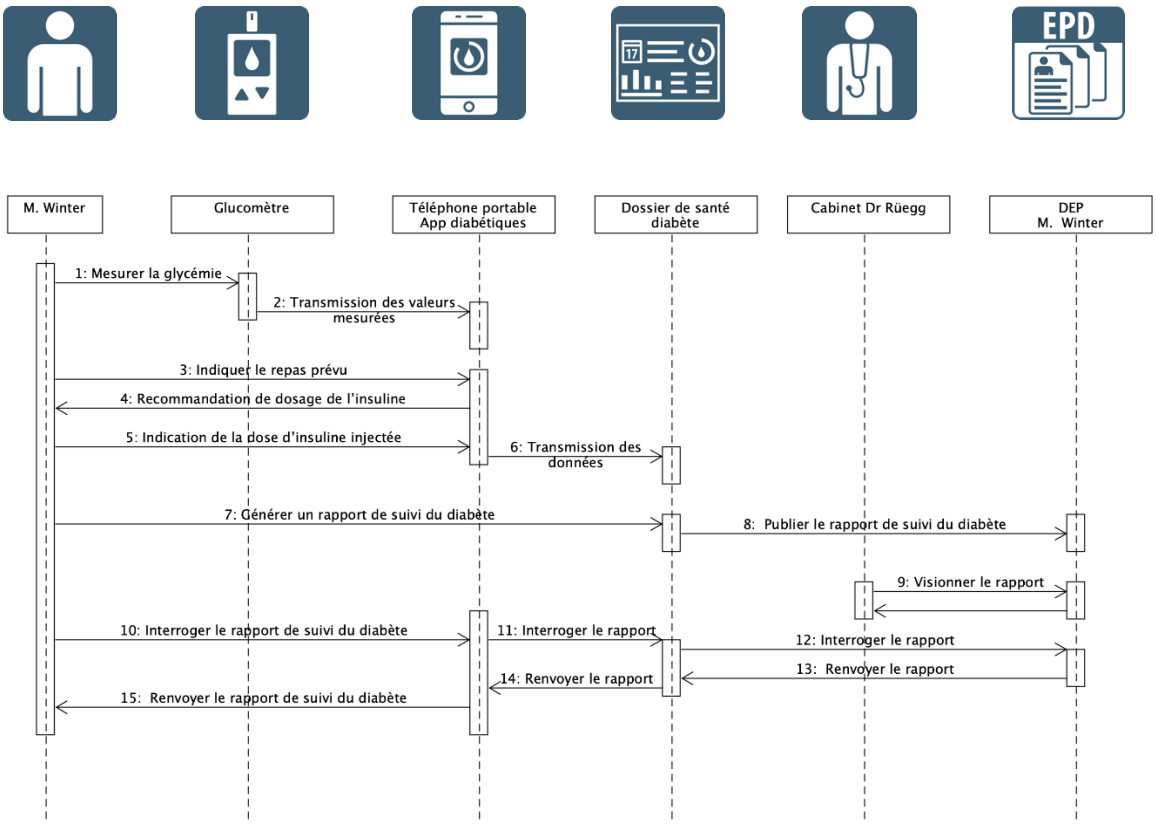

Figure 1-1: Aperçu du cas d'application et des transactions

Normes analysées

Continua Design Guidelines

IEEE 1073

IHE Patient Care Device (PCD)

Devices on FHIR

SMART on FHIR

Profils d'intégration mobiles (MHD, PIXm, PDQm, IUA, RESTFul ATNA)

Standard pour Mobile Health Data (IEEE-Project P1752)

Consumer Mobile Health Application Functional Framework (cMHAFF) Overview and Update (HL7)

Cross-Enterprise Document Data Element Extraction Profil (mXDE)

Défis et évaluation

Les données collectées par capteurs sont des données sensibles. Bien que les capteurs de données fitness ne collectent pas directement des informations médicales, la multitude de types de données différents qu'ils enregistrent permet de créer des profils de personnalité considérés comme des données sensibles par la loi sur la protection des données (LDP). Il en résulte des exigences particulières en matière d'utilisation, de consentement de la part des personnes concernées et de protection des données.	Défis
De manière générale, on observe que la santé mobile recourt à trois liaisons totalement différentes entre les capteurs et le DME/DEP, pour des cas d'application différents faisant l'objet d'une gestion dédiée. Il en découle qu'on ne trouve pas d'ensemble de normes complet dont on pourrait suivre les préconisations.	Appréciation
Les éléments et composants dont l'utilisation est recommandée sont nombreux. La Suisse a la possibilité d'observer et d'accompagner les démarches entreprises dans les pays nordiques et en Autriche. Dans le meilleur des cas, elle pourra avoir une influence sur les développements en cours et en venir à préconiser ou à rendre obligatoires les résultats de ces travaux pour les implémentations en Suisse.	
Alors que le DEP est régi par des dispositions exhaustives et contraignantes, la liaison entre les capteurs et les apps ou les services reste soumise aux mécanismes du marché, qui ne peuvent ni ne doivent être réglementés de manière exhaustive.	
Le cas d'application publié par eHealth Suisse est fourni à titre d'exemple et n'a pas été validé, ni sur le plan du contenu, ni sur le plan clinique. S'il ne couvre pas tous les scénarios mHealth possibles, il est suffisant pour situer les différents standards/normes dans le domaine de la santé mobile. En plus des standards mHealth évalués, d'autres normes doivent être prises en compte, comme celles relatives à l'accessibilité (standards W3C élaborés par la WAI).	Limitation
Le présent rapport se concentre sur l'action recommandée 7 du document « mobile Health (mHealth) Recommandations I ».	

Recommandations

Utiliser les directives Continua	Recommandation 1
Service Interface : utiliser H.812.5 FHIR Observation Upload	Recommandation 1.1
Gérer les consentements sur la base de XACML au lieu de Continua	Recommandation 1.2
Élaborer une technologie de formulaire élargie	Recommandation 1.3
Anticiper le format d'échange PHMR basé sur FHIR	Recommandation 1.4
Suivre une méthode SMART on FHIR	Recommandation 2
Étendre le droit d'exécution de la LDEP aux technologies Web mobiles	Recommandation 3
Utiliser les profils d'intégration mobiles de IHE	Recommandation 4

1 Introduction

1.1 Contexte et objectifs

Contexte

L'organe de coordination eHealth Suisse orchestre les travaux de mise en œuvre du dossier électronique du patient et de la cybersanté au niveau des cantons et de l'Office fédéral de la santé publique.

Le Parlement a adopté la loi sur le dossier électronique du patient (LDEP) le 19 juin 2015. Cette loi prévoit à l'art. 8, al. 2, que les patients peuvent saisir leurs propres données ou documents dans leur dossier électronique. Des instruments simples à utiliser, notamment des applications mobiles, doivent donc être proposés aux patients.

C'est dans ce contexte que l'organe de coordination eHealth Suisse a, dans un premier temps, commandé un état des lieux de la santé mobile dans le cadre du dossier électronique du patient. Sur la base de l'étude du même nom (*mHealth im Kontext des elektronischen Patientendossiers*), réalisée par la haute école spécialisée de Saint-Gall, le groupe de travail mHealth a élaboré des recommandations d'action pour répondre aux défis mis en évidence par l'étude. La priorité a été fixée de manière à ce que les professionnels de la santé puissent, eux aussi, utiliser des applications mobiles pour le dossier médical électronique. Les actions recommandées sont réunies dans le document « mobile Health (mHealth) – recommandations I ». L'action recommandée 7 aborde les thèmes de l'interopérabilité et des standards techniques et sémantiques.

Objectifs

La question de l'interopérabilité est de grande importance pour la santé mobile (mHealth), car la population enregistrera des données de santé ou des constantes vitales au moyen de divers appareils ou applications mobiles, ces données pouvant ensuite être versées au dossier électronique du patient sous forme de documents. eHealth Suisse souhaite recommander des standards et des normes permettant une communication intersystémique sans grand travail d'implémentation.

1.2 Mandat et procédure

Mandat

L'analyse se fonde sur les transactions décrites dans la figure ci-dessous, publiée par eHealth Suisse dans « mHealth et le DEP – un cas d'application concret[2] ». Les initiatives et standards internationaux pertinents en lien avec ces transactions sont identifiés, expliqués et évalués ; et l'élément le plus adéquat est proposé comme recommandation. Les transactions se rapportant au cas d'application portent les mentions CA1 à CA15 (numéro de la transaction selon la figure 1 ci-dessous). Pour pouvoir catégoriser et évaluer les standards correspondants (CA1 à CA15), le cas d'application a été complété de manière à permettre au patient, Monsieur Winter, de vi-

[2] https://www.e-health-suisse.ch/gemeinschaften-umsetzung/ehealth-aktivitaeten/mhealth.html

sionner à nouveau le rapport initialement publié dans le DEP par l'intermédiaire de l'application se trouvant sur son appareil mobile.

La présente analyse doit traiter des points suivants :

- État des lieux des standards et normes existant en matière de santé mobile
- Identification des avantages et des inconvénients ainsi que des domaines dans lesquels les standards et les normes indiquées s'appliquent
- Identification des défis qui se posent et des mesures possibles (par ex. mappage avec les formats d'échange)
- Définition et justification de recommandations pour des standards techniques
- Indications pour l'utilisation de standards sémantiques, dans la mesure où cela est pertinent et possible
- Évaluation du nouveau standard FHIR de HL7 également pour des actions effectuées via des appareils fixes. Les questions suivantes se posent :
    - Quel rôle joue le standard FHIR dans le dossier électronique du patient ?
    - Comment représenter des ressources FHIR dans des formats d'échange ?

Procédure

L'analyse se fonde sur les transactions selon la figure ci-dessous. Elle identifie, explique et évalue les initiatives et standards internationaux pertinents en lien avec ces transactions et recommande l'élément le plus adéquat.

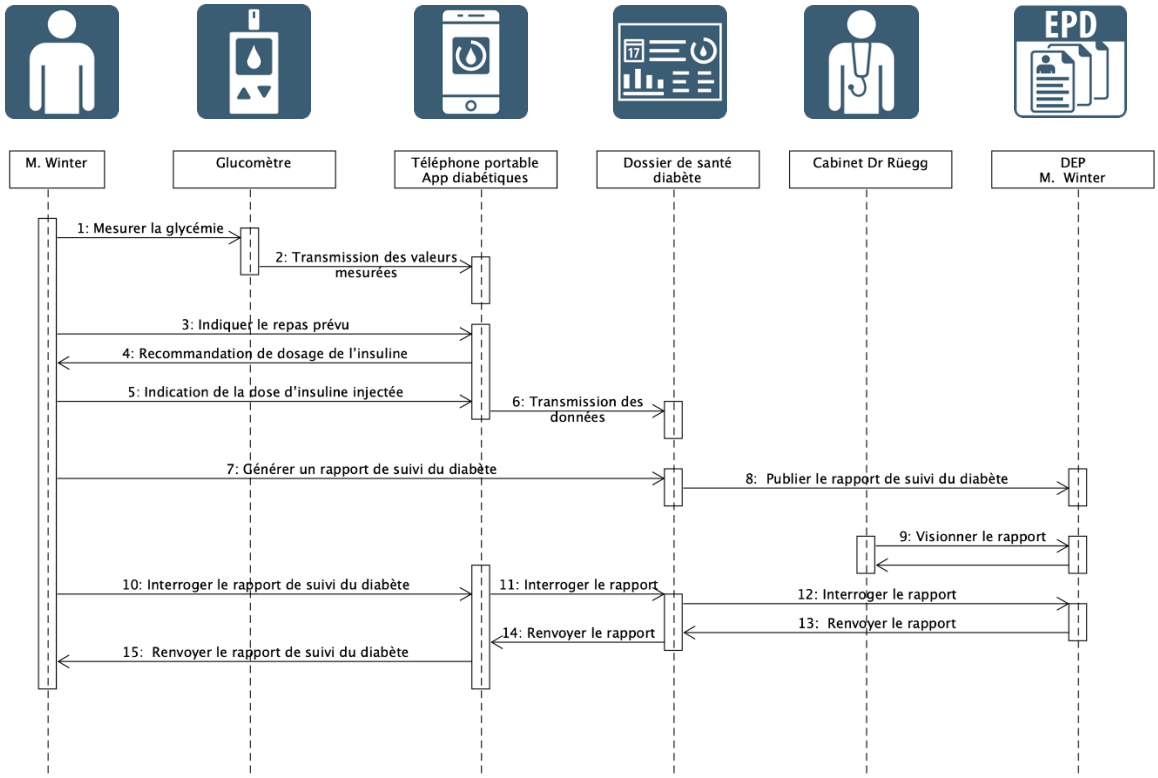

Figure 1-1: Aperçu du cas d'application et des transactions (identique à la figure 1-1)

Procédure

Les documents à la base de la présente analyse sont notamment :

- la LDEP et l'ordonnance y relative, en particulier les critères de certification techniques et organisationnels (CTO),
- « mobile Health (mHealth) – recommandations I » d'eHealth Suisse,
- l'étude « mHealth im Kontext des elektronischen Patientendossiers » de la HES de Saint-Gall (en allemand),
- le LIVRE VERT sur la santé mobile de la Commission européenne.

Sources des standards et initiatives internationaux :

- Continua Design Guidelines
- Consumer Mobile Health Application Functional Framework (cMHAFF) Overview and Update (HL7)
- Devices on FHIR (IHE-USA-Initiative avec Continua)
- Smart on FHIR
- IHE Patient Care Device (PCD)
- IHE MHD, PIXm, PDQm, XUA, IUA
- IEEE-Project P1752 – Standard pour données de santé mobile

Ces standards sont décrits sous forme résumée, évalués quant à leur impact et analysés sous l'angle de leur degré de maturité et de leur complexité.

Les défis particuliers et leur relation avec les exigences suisses en matière de protection et de sécurité des données sont également étudiés. Cet examen comporte une analyse des réglementations existantes (ODEP avec CTO), dans laquelle les experts recommandent d'autres dispositions utiles et se prononcent sur l'avancement du développement et la documentation.

Enfin, les experts se fondent sur leur analyse pour formuler des recommandations.

1.3 Le groupe d'experts

Groupe d'experts

L'équipe de mise en œuvre et formée des spécialistes suivants :

Christian Kohler, KDS GmbH, Herisau
(christian.kohler@kds-main.ch, 078 663 15 63),
directeur de projet et contact,
références particulières : spécification CDA CH-RESP, comités IHE et HL7

Oliver Egger, ahdis gmbh, Zurich (oliver.egger@ahdis.ch),
spécialiste en profils IHE DEP et guides d'implémentation,
références particulières : aide à la mise en œuvre pour le raccordement des systèmes primaires, cas d'application mHealth, IHE et FHIR HL7

Martin Smock, Poste CH SA, Zurich (martin.smock@post.ch),
spécialiste en matière de concepts et d'architectures,
références particulières : aide à la mise en œuvre pour le raccordement des systèmes primaires, IHE et FHIR HL7

2 État des lieux (éléments et normes analysés)Schéma général

Généralités

Le schéma ci-après représente le modèle sous-jacent à toutes les réflexions exposées ici : il reprend les transactions 1 à 15 du cahier des charges et les place dans un contexte technique. Les analyses et autres observations exposées dans le présent chapitre portent sur les liaisons entre les blocs de fonctions ; celles-ci sont représentées par des flèches numérotées qui servent de référence dans le texte.

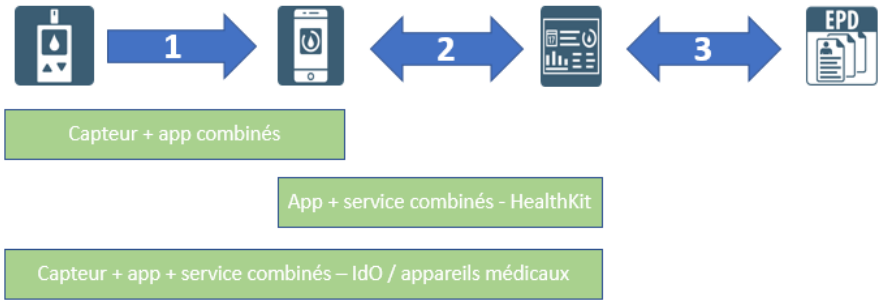

Figure 1: Représentation abstraite des normes et standards

Aperçu

Les composants représentés dans le schéma peuvent aussi être regroupés. Par exemple, un capteur peut fonctionner en combinaison avec une application (app) et une app en combinaison avec un service.

Le schéma explique ce fonctionnement en prenant l'exemple de différents types d'implémentation, comme l'Internet des objet (IdO), les appareils médicaux, l'app HealthKit d'Apple et des combinaisons quelconques de capteurs et d'apps.

Lorsque deux composants sont regroupés, ils constituent un méta-composant, dans lequel la communication est encapsulée. La liaison entre ces deux composants n'est donc plus prise en considération.

Le pictogramme du capteur désigne les composants logiques qui mesurent une valeur. Il s'agit en général de capteurs physiques, dans le cas d'application étudié ici, d'un tensiomètre.

Une app est une application que l'utilisateur fait fonctionner. C'est le composant qui attribue la valeur mesurée à une personne et la transmet au service. Selon les caractéristiques de l'app, il est possible à ce niveau de procéder à une première intervention en validant, en commentant ou en refusant la valeur mesurée. Dans le cas étudié ici, il s'agit d'une app de gestion du diabète sur smartphone.

Le service est le système qui récupère les valeurs attribuées par l'app (passerelle ou *gateway*) et qui les enregistre durablement. Le service peut proposer d'autres fonctions que la simple conservation de données, placer les

mesures effectuées dans un contexte plus large et, le cas échéant, déclencher une alarme. Il peut s'agir du service d'un fournisseur presque quelconque ou d'une application pour un domaine déterminé. Dans le cas étudié ici, il s'agit d'un dossier de suivi de diabète.

Le DME est le système mis en place pour un dossier médical électronique dans l'environnement d'un fournisseur de prestations ou pour le dossier électronique du patient (DEP) selon la législation fédérale. Le DEP est donc une forme de DME définie dans la législation suisse. Dans le présent document, il est question de dossier médical électronique (DME) à propos des généralités et de dossier électronique du patient (DEP) à propos des questions en rapport direct avec les prescriptions légales suisses. Le cas d'application étudié ici prend l'exemple du DEP.

2.2 Continua Design Guidelines

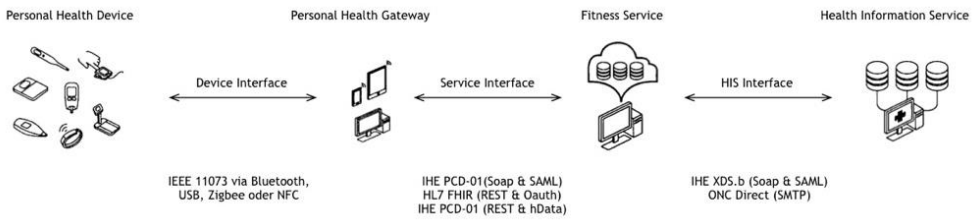

Figure 2: Acteurs de la transmission de données et normes applicables selon les Continua Design Guidelines

Les Continua Design Guidelines (directives Continua) sont publiées par l'organisation internationale à but non lucratif Personal Connected Health Alliance (PCHAlliance). Elles portent sur l'intégration de capteurs et d'autres appareils dans une infrastructure de cybersanté. L'accent est mis sur l'application à la télémédecine et au traitement des maladies chroniques.

Aperçu

1 2 3

Cas d'application

CA1 à CA15

PCHAlliance cherche à offrir une connectivité prête à l'emploi (*plug and play*) de bout en bout entre les appareils et les services utilisés pour la gestion personnelle de la santé et la fourniture de soins. Le but est de couvrir tout le spectre de la transmission de données depuis les capteurs et autres appareils mobiles jusqu'au dossier médical électronique.

Pour ce faire, les directives Continua n'élaborent pas de nouveaux standards, mais recommandent l'utilisation de standards existants pour la transmission de données, l'utilisation de formats de données existants ainsi que des bonnes pratiques d'implémentation. Ces directives rentrent donc dans la catégorie des cadres d'implémentation, tout comme les cadres techniques de l'initiative IHE.

Acteurs

Les directives Continua définissent les acteurs suivants.

L'acteur « Personal Health Device » (PHD ; appareil personnel de santé) désigne tous les capteurs fonctionnant comme une source de données vitales.

Ce sont, par exemple, les podomètres et autres capteurs de fitness, mais aussi des appareils médicaux comme les tensiomètres et les glucomètres, les ECG de 24h et d'autres capteurs collectant des données de manière continue ou discontinue.

L'acteur « Personal Health Gateway » (PHG ; passerelle personnelle de santé) recouvre l'ensemble des appareils qui pilotent le flux d'informations entre les capteurs et les dispositifs de stockage des données situés en aval. Ce sont, par exemple, des smartphones munis d'apps propres à un capteur, mais aussi des ordinateurs appartenant à des particuliers et équipés de programmes spéciaux pour transmettre sur Internet les données collectées par les capteurs.

L'acteur « Health & Fitness Service » (service de santé et de fitness) englobe toutes les applications qui stockent et compilent des données pour l'utilisateur, par exemple, les services de cloud des fabricants de capteurs.

L'acteur « Healthcare Information Service » (HFS ; service d'informations médicales) correspond aux systèmes utilisés pour publier les données vitales pour d'autres acteurs et plus spécialement pour le dossier médical électronique.

Regroupements

Les combinaisons ou regroupements d'acteurs ne sont pas explicitement mentionnés dans les directives Continua, mais ils sont possibles et il en existe déjà sur le marché. On peut citer, par exemple, la combinaison entre un Personal Health Device et un Personal Health Gateway dans une voiture équipée d'un WLAN ou encore la combinaison appareil + passerelle + service de fitness dans un smartphone, avec capteur intégré et app mobile correspondante. Dans ce cas, les recommandations des directives Continua s'appliquent bien sûr uniquement à la communication entre les systèmes externes restants.

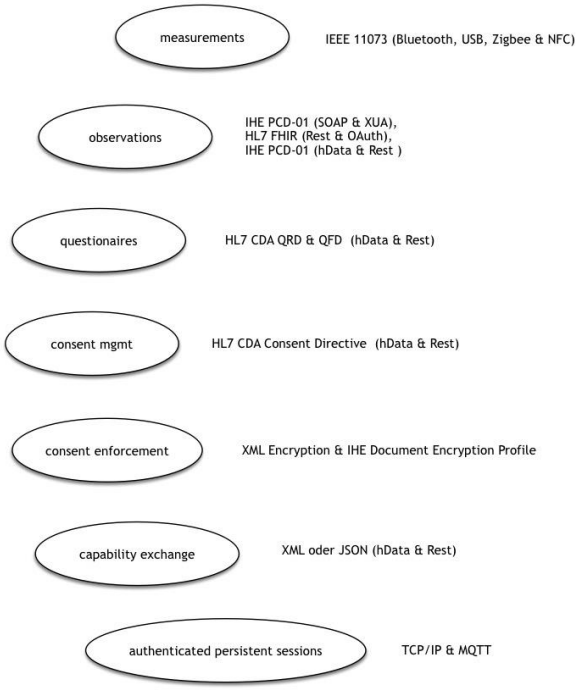

Figure 3: Catégories de cas d'application dans les directives Continua

Catégories

Les recommandations des directives Continua se rapportent majoritairement aux cas d'application (*use cases*) et aux standards d'échange de données entre les acteurs, et plus particulièrement aux protocoles techniques et médicaux utilisés pour implémenter les cas d'application.

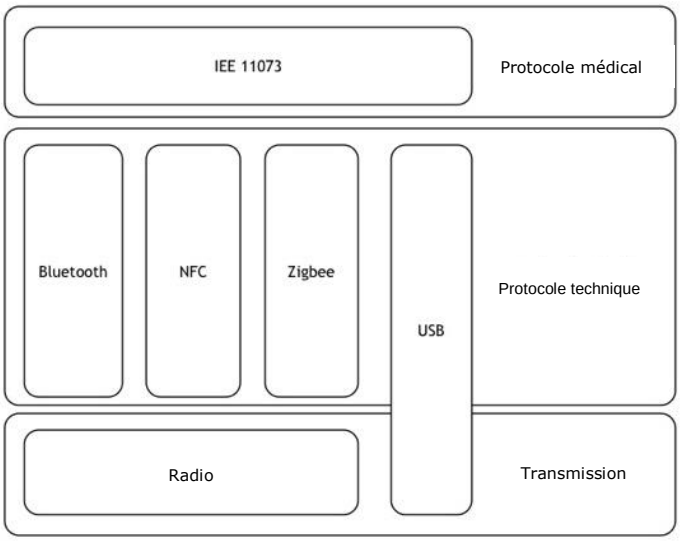

Figure 4: Pile de protocoles du Device Interface selon les directives Continua

CA2

Device Interface (interface avec l'appareil) : pour la transmission des données du capteur vers le Personal Health Gateway (par ex., un smartphone), les directives Continua préconisent d'utiliser les protocoles de la famille de

normes IEEE-11073 en passant par les protocoles techniques Bluetooth, USB, Zigbee et NFC.

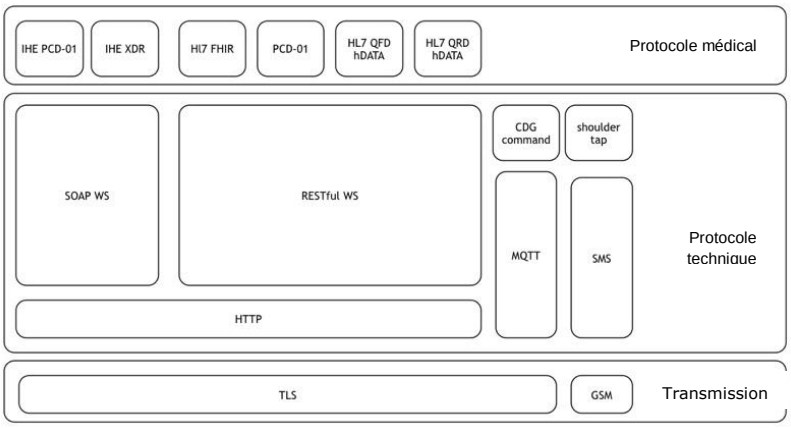

Figure 5: Pile de protocoles du Service Interface selon les directives Continua

CA6

Service Interface (interface avec le service) : pour la transmission des données de la passerelle (par ex. smartphone) vers le Fitness Service (par ex. app fitness sur le cloud), les directives Continua préconisent trois protocoles différents :

1. IHE PCD-01 via XML SOAP avec authentification SAML
2. HL7 FHIR avec autorisation OAuth
3. IHE PCD-01 avec REST Binding et OAuth ou OpenID Connect

Pour l'échange de questionnaires, les directives Continua préconisent les formats HL7 CDA QFD et QRD et leur transmission via les services Web hData et RESTful.

Pour le contrôle de l'accès aux données transmises par le Service Interface, les directives Continua préconisent une solution utilisant un cryptage individuel, spécifique au destinataire. Ce cryptage doit être configuré dans un document HL7 CDA R2 contenant les directives en matière de consentement et implémenté au moyen d'un procédé XML ou du profil IHE-DEN. Comme protocole de transfert, les directives Continua préconisent soit hData via REST, soit le profil IHE-XDR avec service Web XML SOAP.

Pour la synchronisation automatique des données au format hData Record, les directives Continua recommandent toujours des formats d'échange utilisant des services Web RESTful avec autorisation OAuth. Cela s'applique aux valeurs mesurées par les capteurs et proposées via la passerelle (par ex. app mobile) comme aux données vitales supportées par le Fitness Service (*capability exchange*).

En plus de ces protocoles HTTP, les directives Continua préconisent de recourir à des sessions persistantes avec authentification (*authenticated persistent sessions*) reposant sur le protocole MQTT. Cette technologie de trans-

fert de données, qui a été développée en lien avec l'IdO, supporte une transmission sûre et économe en énergie même lorsque la connexion au réseau est mauvaise.

Pour les sessions persistantes avec authentification, les directives Continua ne peuvent renvoyer à des normes établies. Elles définissent donc de nouveaux protocoles techniques, sans formuler de recommandations explicites concernant les informations et protocoles médicaux.

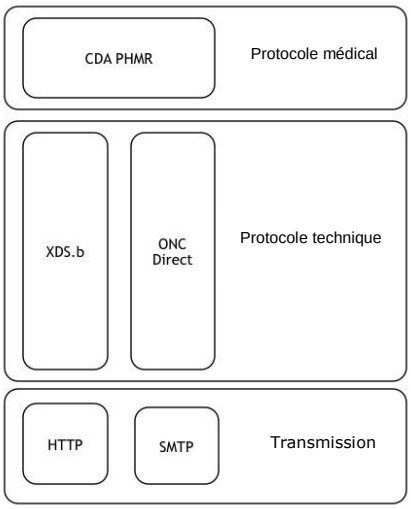

Figure 6: Pile de protocoles du Healthcare Information System Interface selon les directives Continua

CA8

Healthcare Information System Interface (interface avec le système d'information médicale) : pour la sauvegarde des données dans le dossier médical électronique, les directives Continua préconisent des documents CDA qui contiennent les données vitales au format PHMR (Personal Health Monitoring Report) et qui sont stockés au moyen des transactions de service Web du profil IHE-XDS.b ou par courriel via ONC Direct. Concernant les questions d'authentification, d'autorisation et de journalisation, les directives ne formulent pas de recommandations explicites, mais renvoient aux profils IHE correspondants (par ex. XUA, ATNA).

Degré de maturité et état de la documentation

Avec ses directives Continua, PCHAlliance s'efforce de couvrir tous les aspects des échanges de données en télémédecine. Les directives formulent donc des recommandations très variées. Comme elles se réfèrent presque exclusivement à des normes existantes, les protocoles techniques et médicaux recommandés présentent un degré de maturité et d'applicabilité très élevé.

Groupes cibles et domaines d'utilisation

Couvrant un large spectre de transactions, les directives Continua s'adressent à tous les intervenants sur la chaîne de traitement des données de santé mobile : fabricants de capteurs, développeurs d'apps mobiles, fournisseurs de services et surtout exploitants de DME ou de DEP.

Simplicité

Comme les directives Continua préconisent souvent plusieurs combinaisons de protocoles techniques et médicaux pour des cas d'application individuels sans toutefois les évaluer, l'évaluation et la sélection de protocoles adaptés incombent aux développeurs d'applications. Ces directives restent cependant une source importante pour eux car elles offrent une vue complète des variantes disponibles pour les échanges de données entre acteurs ou applications dans la télémédecine.

La forte variabilité des spécifications référencées, leur grand nombre et leur complexité sont autant d'obstacles à l'implémentation des applications. Il faut donc fixer des exigences appropriées.

Discussion

Alors que les standards applicables à la communication entre les appareils personnels de santé (Personal Health Devices, par ex. capteurs) et les passerelles personnelles de santé (Personal Health Gateways, par ex. smartphones) ainsi qu'à la connexion des services avec le DME ou de DEP sont désormais reconnus et admis internationalement, ce n'est pas le cas des normes applicables à l'implémentation de l'interface avec le service (Service Interface). Cela tient en partie au fait que les cas d'application correspondants ne sont pas encore au cœur des travaux d'implémentation (questionnaires, *capability exchange*, *authenticated persistent sessions*).

La dernière version des directives Continua intègre la norme HL7 FHIR pour la transmission des données collectées par des capteurs (observations) de la passerelle (par ex. smartphone) vers le service de fitness. Comme la norme HL7 FHIR utilise des techniques populaires de développement Web, les obstacles à l'implémentation de l'interface avec le service sont moins élevés qu'avec les autres protocoles.

À ce jour, les directives Continua ne définissent pas de protocole pour la consultation des données personnelles de santé conservées par le service d'informations médicales (DEP) ou le service de fitness. Il est facile cependant de transposer les protocoles des directives Continua à la consultation de données, car on peut utiliser les mêmes formats et protocoles que pour le transfert des données vers les services.

L'extension des cas d'application à la consultation des données collectées par les capteurs sur le service d'informations médicales ou le service de fitness accroît l'importance de la gestion du consentement et de l'exécution des directives en la matière (*consent management and enforcement*). Or, les ordonnances relatives à la loi sur le dossier électronique du patient régissent la gestion du consentement et l'exécution des directives en la matière en ce qui concerne la consultation de documents sur le service d'informations médicales, mais pas en ce qui concerne le téléchargement de données du service de fitness vers la passerelle personnelle de santé (Personal Health Gateway, par ex. smartphone).

Il faut en outre déterminer avec précision si les recommandations des directives Continua sur la gestion du consentement au moyen de la directive de consentement HL7 CDA R2 et sur son exécution au moyen d'un cryptage

spécifique au destinataire définissent des procédures appropriées pour consulter les données collectées par des capteurs ainsi que des questionnaires. Une autre solution consiste à utiliser XACML, qui est déjà prescrit pour le DEP.

2.3 IEEE 11073

Aperçu

1

CA2

ISO/IEEE 11073 Personal Health Data[3] (PHD) est une famille de normes permettant d'échanger des données vitales entre différents appareils médicaux, d'analyser les données et de commander les appareils à distance. Les appareils concernés sont par exemple des balances, des tensiomètres, des glucomètres et autres appareils similaires. Les directives Continua s'appuient sur ces normes pour la transmission entre l'appareil et l'app.

Architecture

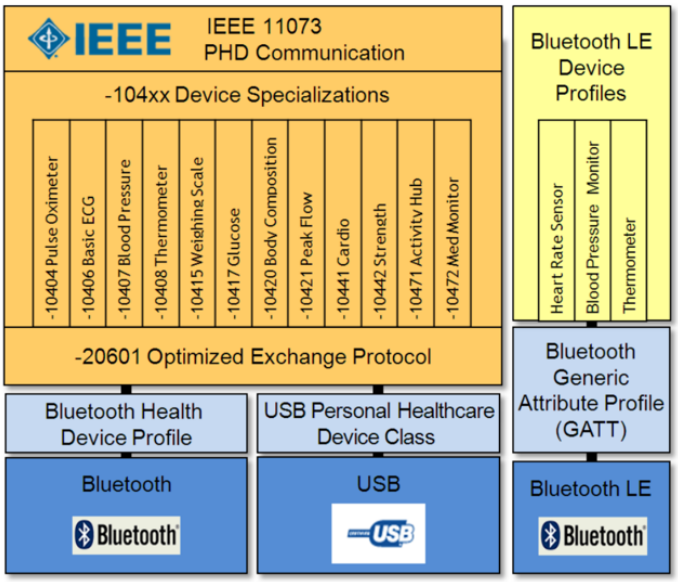

Figure 7: Schéma de l'IEEE 11073 PHD, source[4]

La norme de base définit un modèle d'informations de domaine (Domain Information Model, DIM), la nomenclature et le modèle de communication. Elle est déclinée en normes spécialisées pour chaque type d'appareil.

La famille de normes IEEE-11073 s'adresse aux fabricants d'appareils médicaux et aux fabricants de capteurs personnels de santé.

Groupes cibles et domaines d'utilisation

L'IEEE 11073 couvre la communication entre le capteur et l'app. En raison de leur format binaire, les messages ne peuvent pas être traités simplement avec d'autres normes IT, car il existe peu d'outils pour travailler avec ce format. Il faut donc recourir à d'autres solutions pour assurer l'interopérabilité des flux de l'app vers le service, telles que celles décrites par IHE ou dans les directives Continua. Les appareils à la norme IEEE-11073 ne sont pas encore très répandus alors qu'il existe 23 modèles d'appareils basés sur les directives Continua (chiffre d'octobre 2017)[5]. En outre, la norme

Discussion

[3] http://www.11073.org/

[4] http://www.who.int/medical_devices/global_forum/Sun_pm_SAF_3_ZHONG.pdf?ua=1

[5] http://www.pchalliance.org/product-showcase?title=&field_manufacturer_tid=All&field_product_type_tid=All&field_transport_type_tid=All&field_product_capability_tid=All&field_product_category_tid=1140&field_design_guidel

IEEE 11073 ne couvre pas tous les capteurs. Il faut donc se demander dans quelle mesure les données provenant de capteurs non couverts peuvent être mappées sur le modèle d'informations IEEE-11073.

2.4 IHE Patient Care Device (PCD)

Aperçu

CA2

Le cadre technique Patient Care Device (PCD) est édité par l'initiative IHE comme cadre d'implémentation pour les échanges de données entre et avec des appareils médicaux. Conçu principalement pour connecter des appareils médicaux dans les hôpitaux et les cabinets médicaux, il porte avant tout sur des cas d'application dans le domaine clinique concernant la gestion des appareils médicaux, le traitement des alarmes ainsi que les échanges de données de mesure et de fonctionnement produites par des stimulateurs cardiaques, des appareils respiratoires, encore des appareils d'anesthésie, etc.

Dans le cadre technique PCD, IHE ne définit pas de nouvelles normes mais préconise d'utiliser des normes établies dans le secteur médical pour la transmission et les formats de données et recommande des bonnes pratiques d'implémentation.

Profils PCD

Le cadre technique PCD définit les profils suivants :

- Device Enterprise Communication (DEC), avec des acteurs et des transactions pour gérer les données du patient et la communication des données de mesure ;
- Point-of-Care Infusion Verification (PIV), avec des acteurs et des transactions pour piloter les appareils de perfusion ;
- Implantable Device Cardiac Observation (IDCO), avec des acteurs et des transactions pour surveiller à distance les stimulateurs cardiaques par exemple ;
- Alert Communication Management (ACM), avec des acteurs et des transactions pour assurer la transmission et la gestion des alarmes.

Protocoles

Les transactions des profils PCD utilisent des formats de données à la norme HL7 V2. Le cadre technique PCD ne formule pas de recommandations ou de prescriptions explicites concernant les protocoles de transfert, mais renvoie aux protocoles de transfert des cadres techniques ITI.

Groupes cibles et domaines d'utilisation

Le cadre technique PCD s'adresse principalement à tous les fabricants d'appareils médicaux destinés au domaine clinique. Il met à disposition un guide d'implémentation pour une communication standardisée dans les cas d'application considérés.

Simplicité

Le cadre technique PCD est basé directement sur la norme HL7 V2, déjà très répandue chez les fabricants d'appareils médicaux. Son implémentation est donc assez simple. Il propose en outre, grâce à la cartographie terminologique Rosetta (Rosetta Terminology Mapping, RTM)[6], des outils de conversion terminologique d'IEEE 11073 en PCD.

Discussion

Le cadre technique PCD est assez largement répandu chez les fabricants d'appareils médicaux destinés à l'usage clinique et donc bien accepté. On

ine_version_tid=All&field_health_category_tid=All&field_certified_date_value[value][date]=&field_certified_date_value_1[value][date]=&field_countries_value=All&field_commercially_available_value=1&order=field_manufacturer_1&sort=asc

[6] https://rtmms.nist.gov/rtmms/index.htm

ne sait pas ce qu'il en est chez les fabricants de capteurs de télémédecine. On peut toutefois préciser que les directives Continua préconisent la transaction PCD-01 de communication des observations, combinée aux protocoles de transfert par service Web XML SOAP et RESTful hData.

2.5 Devices on FHIR

Aperçu

Devices on FHIR est une initiative qui a pour but d'améliorer la communication basée sur HL7 FHIR à la fois pour les appareils médicaux en milieu hospitalier et pour les capteurs de télémédecine. Elle est le fruit d'une collaboration entre plusieurs autres initiatives, notamment IHE, HL7 FHIR et PCHAlliance.

CA2

Cette initiative s'efforce de développer l'utilisation de la nouvelle norme HL7 FHIR pour les échanges de données entre appareils médicaux ou capteurs ainsi qu'entre ces appareils et les systèmes d'information médicale.

À cet effet, elle élabore les bases requises pour représenter les appareils et les capteurs au moyen d'objets FHIR et plus spécialement le modèle de données et de communication de l'IEEE 11073 avec les ressources FHIR et les extensions FHIR requises.

Protocoles

Devices on FHIR reprend à la fois les formats de données (XML, JSON,etc.) et les protocoles de transfert (RESTful Web Service) de HL7 FHIR.

Groupes cibles et domaines d'utilisation

Devices on FHIR s'adresse donc aux fabricants d'appareil médicaux pour le milieu hospitalier comme aux fabricants de capteurs personnels de santé et aux développeurs d'applications dans les domaines de la médecine et de la santé personnelle.

Simplicité

HL7 FHIR repose sur des technologies (RESTful, JSON, XML, etc.) actuellement employées par presque tous les concepteurs de logiciels et fabricants d'appareils, y compris dans d'autres cas d'application. Son implémentation technique, qui est donc déjà relativement simple, est facilitée par l'ouverture de FHIR, la multiplicité des exemples et la grande disponibilité de serveurs de test ouverts. Le mappage sémantique et la conversion des unités de mesure (UOM) restent un défi de taille pour tous les fabricants.

Discussion

HL7 FHIR est un standard émergent, qui doit encore évoluer et qui est actuellement dépourvu de valeur normative. Il est donc difficile d'estimer à quelle vitesse le marché acceptera les résultats de l'initiative Devices on FHIR et implémentera les interfaces proposées.

2.6 Smart on FHIR

Figure 8: SMART on FHIR, http://docs.smarthealthit.org/

Aperçu

SMART (Substitutable Medical Applications, Reusable Technologies) est une série de spécifications ouvertes pour l'intégration d'apps dans les systèmes primaires, les portails, les dossiers électroniques et d'autres systèmes informatiques de santé.

CA6

(CA8 à CA14)

SMART définit, d'une part, un mécanisme permettant aux systèmes primaires de sélectionner des patients et de démarrer une application Web à partir de ce contexte. L'application Web peut alors accéder aux données du patient. D'autre part, SMART définit un modèle d'autorisation et d'authentification pour des apps.

Ces spécifications couvrent les domaines app, service et DME. Le terme app désigne non seulement des app mobiles mais aussi des applications Web.

Architecture

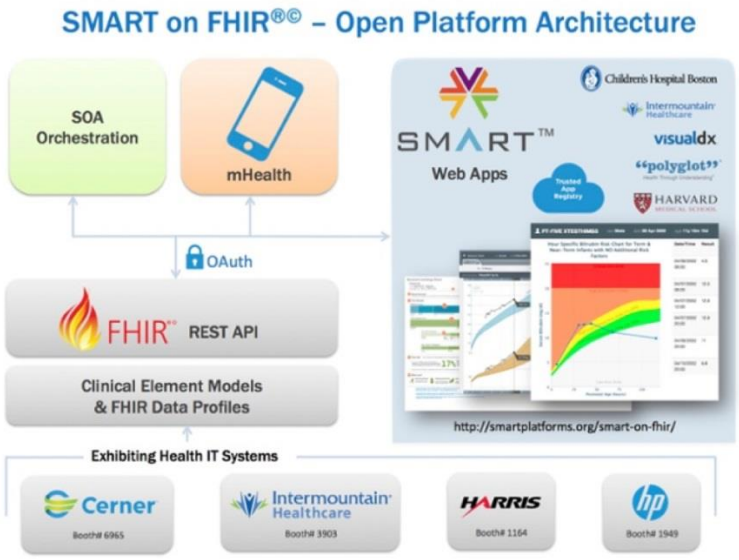

Figure 9: Architecture SMART on FHIR ; source : https://www.healthcare-guys.com/2015/11/18/whats-the-deal-with-smart-on-fhir/

Normes utilisées

SMART se base sur la norme FHIR de HL7 pour proposer une API unique pour les interfaces. L'autorisation et l'authentification des apps sont basées sur les normes OAuth 2.0 et OpenID Connect. Les spécifications SMART sont intégrées dans la norme FHIR. SMART on FHIR devient ainsi *de facto* la norme de sécurité de FHIR.

Discussion

Pour pouvoir appliquer la méthode SMART on FHIR aux apps en Suisse, il faut adapter les ressources créées aux États-Unis aux spécificités suisses en recourant à des profils. Comme, en Suisse, les documents utilisés pour les formats d'échange dans le DEP sont basés sur la norme CDA, il faut définir des profils FHIR correspondants afin de pouvoir les décrire dans les formats d'échange du DEP.

2.7 Profils d'intégration mobiles IHE (MHD, PIXm, PDQm, IUA, RESTFul ATNA)

Aperçu

CA8 à CA14

IHE[7] est une initiative internationale visant à améliorer les échanges de données sur le plan technique et l'interopérabilité des systèmes informatiques dans le secteur de la santé. IHE s'est basé sur la nouvelle norme FHIR de HL7 pour élaborer de nouveaux profils d'intégration[8], parmi lesquels MHD, PIXm, PDQm, RESTful ATNA et IUA concernent la santé mobile.

Ces profils d'intégration couvrent l'interaction entre l'app et le service combiné avec le DME (cf. schéma général). Dans le contexte du DEP suisse, les profils d'intégration mobiles sont applicables à la partie app/passerelle, avec le regroupement des profils d'intégration non mobiles utilisés dans le DEP entre service et DME (DEP).

IHE ITI TF Suppl MHD

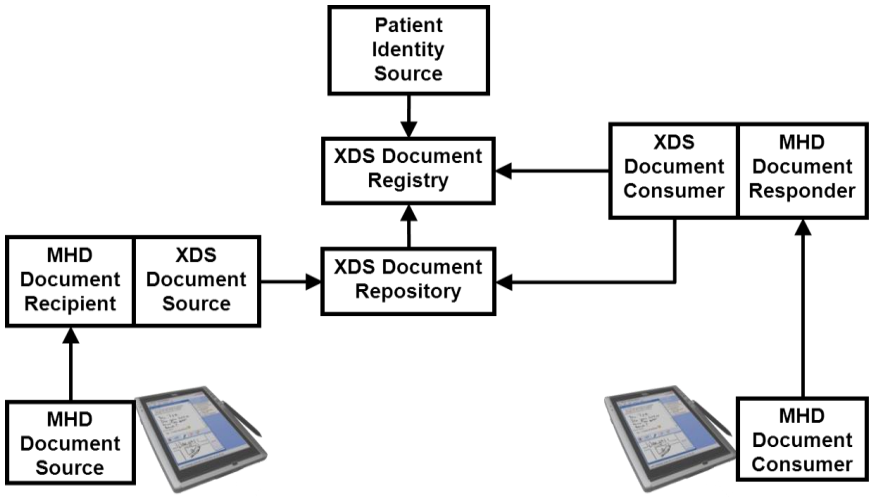

Figure 10: Acteurs MHD combinés avec acteurs XDS (source : IHE MHD)

Le profil MHD (Mobile access to Health Documents) permet d'accéder à une infrastructure XDS au moyen d'une API RESTful, comme cela est prévu pour le dossier médical électronique. Parmi les exemples mentionnés explicitement dans le profil figure l'intégration d'appareils de mesure basée sur IHE PDC/Continua pour publier des documents dans l'infrastructure XDS.

IHE ITI TF Suppl PIXm, PDQm

IHE PIXm et PDQm sont des profils permettant d'établir la correspondance entre le portail et le dossier médical électronique en ce qui concerne les patients. PDQm est utilisé pour rechercher les données démographiques des patients et PIXm pour mettre en corrélation leurs identités sur différents systèmes. Ces profils d'intégration mobiles peuvent être combinés aux profils IHE PIX et PDQ, qui sont basés sur HL7 V3.

IHE ITI TF Suppl

Add RESTful Query to ATNA

Ce complément actualise le profil ATNA (Audit Trail and Node Authentication), qui définit une méthode standardisée pour établir et envoyer des entrées d'audit. Il permet de rechercher et de consulter des entrées d'audit journalisées en utilisant la norme FHIR.

[7] http://www.ihe.net/
[8] https://wiki.ihe.net/index.php/Category:FHIR

Le profil IUA (Internet User Authorization) supporte l'autorisation de transactions dans les interfaces HTTP RESTFul. IHE a déjà le profil XUA pour les services Web et les transactions basées sur SOAP. Le profil IUA le complète pour les interfaces HTTP basées sur le Web. L'autorisation repose sur la norme OAuth 2.0 et utilise des jetons JWT (JSON Web Token). Les jetons OAuth Bearer ou SAML Token peuvent également être utilisés en option.

IHE ITI TF Suppl IUA

Les profils d'intégration mobile de IHE offrent une interface simplifiée basée sur FHIR, dont la fonctionnalité par rapport aux profils sous-jacents est partiellement réduite elle aussi. Les acteurs des profils d'intégration mobiles peuvent cependant être combinés avec les profils sous-jacents, comme le montre la figure 12 Acteurs MHD combinés avec acteurs XDS (source : IHE MHD).

Architecture

Les communautés du DEP sont tenues de supporter les profils IHE sous-jacents à XDS, PIX, PDQ et XUA définis dans la loi et les ordonnances qui s'y rapportent. Mais celles-ci ne régissent pas les profils d'intégration mobiles décrits ici. Il n'est pas facile d'estimer dans quelle mesure il est intéressant pour les communautés de mettre à disposition une interface simplifiée pour l'accès mobile. De plus, il faut notamment trouver une solution pour assurer l'authentification complète lors des accès et, à l'heure actuelle, ces profils doivent être implémentés en l'état par chaque communauté. L'accès technique au dossier médical électronique serait certainement plus facile à implémenter au niveau des apps.

Discussion

2.8 Standard for Mobile Health Data (IEEE-Projekt P1752)

L'Institute of Electrical and Electronics Engineers (IEEE) a lancé un projet (P1752[9]) de normalisation des données de santé mobile (Mobile Health Data). Le but est d'élaborer une interface de programmation applicative (API) pour les données de santé mobile et de standardiser la représentation et les métadonnées des données de santé. Les données de santé visées sont les données recueillies par les capteurs et les apps. Les responsables du projet ont annoncé une première esquisse pour janvier 2018. Elle reposera sur les normes IEEE-11073, auxquelles se réfèrent également les directives Continua. Ce nouveau standard est élaboré par un groupe de travail de l'IHE (Open Mobile Health Work Group).

Aperçu

CA6

Selon les responsables du projet, il concernera les capteurs et les apps en combinaison avec le service.

Aucune information n'a encore été publiée au sujet de ce futur standard norme. Il est donc impossible de décrire son architecture. Pour en savoir plus :

Architecture

[9] https://standards.ieee.org/develop/project/1752.html

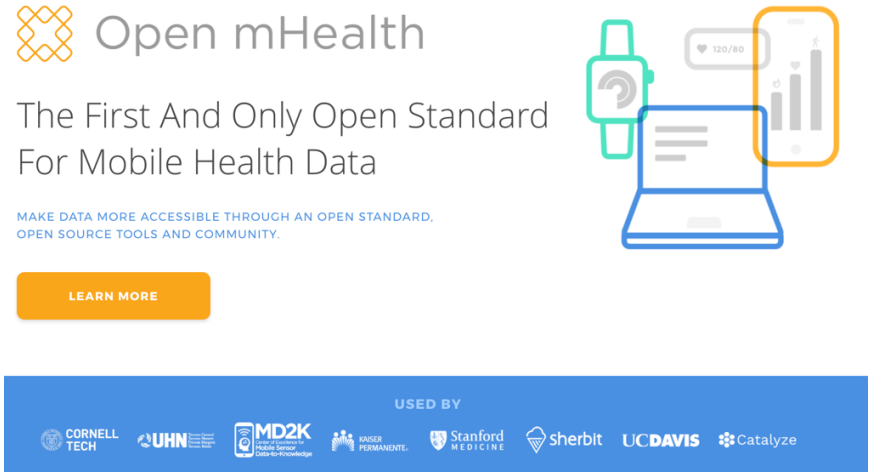

Figure 11: Open mHealth, http://www.openmhealth.org/

Discussion

L'adresse électronique de la personne à l'origine du projet laisse penser qu'il existe un lien entre le groupe de travail Open Mobile Health Work Group et le site Internet Open mHealth. Ce dernier expose plusieurs scénarios relatifs au partage de données de santé, allant du traitement des données à leur importation et à leur exportation en passant par leur visualisation et leur agrégation. Cette initiative est soutenue par plusieurs organisations américaines, mais les dernières informations concernant le protocole publiées sur son blog remontent à septembre 2016. Il faut donc attendre pour voir si une nouvelle norme est effectivement élaborée et dans quelle mesure elle sera interopérable avec d'autres normes. Le meeting de lancement a eu lieu le 6 février 2018 (cf. diapositives)[10]. Les responsables prévoient d'élaborer d'ici octobre 2018 un guide d'implémentation indiquant comment la norme ouverte Open mHealth Standard pourra être représentée dans FHIR.

2.9 Consumer Mobile Health Application Functional Framework (cMHAFF) Overview and Update (HL7)

Aperçu

Le cadre Consumer Functional Framework (cMHAFF)[11] de HL7 propose un standard pour les applications de santé mobile grâce auquel on peut évaluer les caractéristiques fondamentales d'une app mobile, c'est-à-dire en particulier la sécurité, la protection des données, l'accès aux données, l'exportation de données et la transparence (informations sur les conditions).

Le but est de mettre à disposition des directives sectorielles et des méthodes communes afin de permettre le développement d'apps de santé mobile centrées sur le patient/citoyen qui utilisent les informations de santé ainsi que des données personnelles. Ce cadre ne couvre pas les fonctionnalités cliniques des apps (par ex. recommandations, diagnostics), mais

[10] http://sites.ieee.org/sagroups-1752/meeting-agenda-minutes/

[11] http://wiki.hl7.org/index.php?title=MHWG_Consumer_Mobile_Health_Application_Functional_Framework

offre une structure pour la sécurité, la protection des données et l'intégration de données provenant d'applications situées sur un portail ou dans un dossier électronique.

Un groupe de travail de HL7 (Mobile Health Workgroup) est en train d'élaborer le cadre cMHAFFD[12]. Une phase de consultation est prévue pour janvier 2018.

Si l'on se rapporte au schéma général, le cadre cMHAFF porte uniquement sur l'app proprement dite, mais seulement si elle ne rentre pas dans la catégorie des apps médicales.

Ce cadre s'adresse en premier lieu aux développeurs d'apps mobiles, mais aussi aux organisations qui souhaitent tester, certifier ou préconiser ces apps.

Il aborde, par exemple, les sujets suivants :

- L'app contient-elle des informations permettant d'identifier le patient ?
- Des données sont-elles stockées ou transmises hors de l'appareil ?
- L'app est-elle associée à des capteurs qui mesurent les valeurs du patient ?
- Y a-t-il des envois d'avertissements ou de notifications ?

Architecture

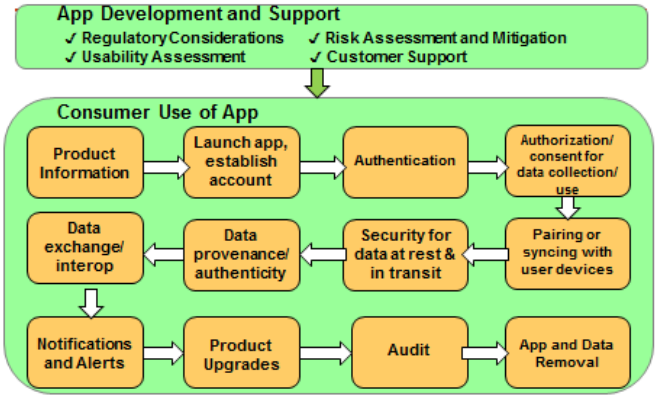

Figure 12: cMHAFF Sections and Mobile App Life Cycle (source : HL7, CMHAFF_STU_Ballot_Draft.docx)

Le cadre cMHAFF définit des critères pour les différents segments du cycle du vie d'une app, mais pas d'architecture à proprement parler.

Normes utilisées

Il n'utilise ou ne préconise pas directement des normes, mais intègre des préconisations ou des référentiels issus de projets nationaux.

Discussion

Le cadre cMHAFF n'est pas une norme technique permettant de développer une app, mais il permet de se familiariser rapidement avec les défis que pose une app de santé mobile ne rentrant pas dans la catégorie des apps médicales.

[12] http://wiki.hl7.org/index.php?title=File:CMHAFF_STU_Ballot_Draft.docx

2.10 Profil Cross-Enterprise Document Data Element Extraction (mXDE)

Le profil mXDE (Cross-Enterprise Document Data Element Extraction)[13] offre la possibilité d'accéder à des éléments de données extraits de documents structurés communs.

Aperçu

(CA13, CA14)

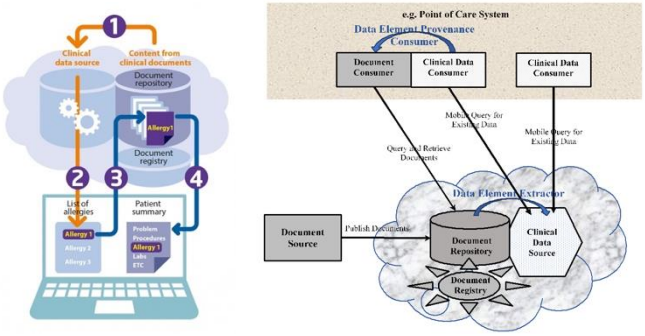

Figure 13: Profil d'intégration mXDE[14]

Ce profil permet de consulter non seulement des documents, mais aussi directement, via une infrastructure basée sur des documents, des éléments de données comme les signes vitaux ou les allergies. Le lien contextuel entre l'élément de données et le document dont il est extrait est conservé, ce qui permet de retrouver le document à partir de l'élément de données. Le profil utilise le profil d'intégration QEDm (PCC Query for Existing Data for Mobile)[15]. Les éléments de données sont représentés avec les ressources FHIR correspondantes et ils peuvent être réalisés avec les profils IHE-XDS ou MHD.

Discussion

Lorsque les éléments de données doivent être extraits de différents documents HL7 CDA PHMR, le profil peut établir la liaison à partir d'éléments de données stockés dans le contexte du DEP. Ce profil en est au stade de l'essai d'implémentation (*trial of implementation*). Les éléments de données sont représentés sous la forme de ressources FHIR ; le mappage est à définir.

Dans le cas d'application étudié, ce profil pourrait être utilisé lorsque le dossier de santé veut extraire directement des éléments de données (par ex. précédentes mesures de glycémie) d'un document figurant dans le DEP plutôt que consulter le rapport *in extenso* (CA13, CA14).

[13] https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_mXDE.pdf
[14] http://wiki.ihe.net/index.php/Mobile_Cross-Enterprise_Document_Data_Element_Extraction
[15] https://www.ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_Suppl_QEDm.pdf

3 Défis fondamentaux

3.1 Protection et sécurité des données

Protection et sécurité des données

Les données collectées par capteurs sont des données sensibles. Bien que les capteurs de données fitness ne collectent pas directement des informations médicales, la multitude de types de données différents qu'ils enregistrent permet de créer des profils de personnalité considérés comme des données sensibles par la loi sur la protection des données (LDP). Cela pose des exigences particulières en matière d'utilisation, de consentement de la part des personnes concernées et de protection des données.

Sécurité des capteurs

Les capteurs appartiennent généralement aux personnes dont ils recueillent les données ; ils n'enregistrent que peu d'informations, limitées la plupart du temps à une seule activité. Sous l'angle de la protection et de la sécurité des données, le risque est relativement faible, à la condition que les capteurs aient été implémentés conformément à l'état actuel de la technique.

Sécurité des apps

En termes de sécurité, le traitement des données au moyen d'apps est déjà plus critique. Les applications exploitées sur des équipements mobiles (par ex. smartphones) mémorisent généralement des informations relevant de plusieurs catégories de données médicales et de fitness, dont certaines requièrent un niveau de protection élevé. L'équipement mobile appartient généralement à son utilisateur ; c'est donc lui qui contrôle la protection et la transmission de ses données de santé, à la condition que les mécanismes de sécurité des applications aient été implémentés conformément à l'état actuel de la technique.

Sécurité du service

C'est au niveau du service dans lequel les données de santé sont mémorisées en nombre, accessibles à des tiers et placées sous le contrôle de l'exploitant que la protection et la sécurité des données deviennent très critiques. En principe, ces services ne sont pas soumis à des dispositions légales particulières, excepté celles régissant le traitement des données visé par la loi sur la protection des données. Un traitement de données à des fins particulières requiert le consentement éclairé de la personne concernée.

La loi sur la protection des données prévoit que des mesures appropriées doivent être prises pour assurer la sécurité des données. De manière générale, pratiquement toutes les mesures visant à garantir la sécurité des données prises conformément à l'état actuel de la technique sont considérées comme appropriées. Le catalogue de mesures de la famille de normes ISO-27001 ou de la protection de base IT, par exemple, indique comment interpréter cette disposition.

Protection et sécurité des données du DME

En revanche, le droit d'exécution de la LDEP définit explicitement les mesures destinées à assurer la protection et la sécurité des données et précise les dispositions de mise en œuvre dans les CTO. Il impose parfois des exigences très strictes aux systèmes raccordés, que l'application du service doit satisfaire.

Discussion

Du capteur au DME en passant l'app et le service, les exigences de protection et de sécurité des données s'accroissent fortement et doivent recevoir l'attention nécessaire.

Ces aspects ont été abordés sous un angle technique, en lien avec les normes étudiées. La réflexion n'a pas été poussée pour englober des aspects plus généraux.

Nous rappelons qu'une expertise juridique est en cours d'élaboration.

3.2 Authentification et autorisation

Authentification et autorisation d'un capteur

Les capteurs sont généralement individualisés et recueillent les données d'un seul utilisateur. En principe, l'appareil s'authentifie au moyen d'un identifiant ID que le capteur d'un fabricant reconnaît de manière univoque. L'autorisation s'effectue généralement par appairement, une technique courante avec des équipements Bluetooth par exemple. L'utilisateur accorde des droits d'écriture, éventuellement aussi de lecture, par un consentement explicite en enregistrant un code propre à l'appareil.

Authentification et autorisation d'un service

L'authentification d'un end point de service par rapport au DME et les autorisations d'accès sont définis dans les ordonnances relatives au DEP. Le droit d'exécution de la LDEP recommande les profils IHE ATNA, XUA et Authenticate User pour l'authentification du service, l'exécution des droits d'accès et l'authentification de l'utilisateur. Pour cette dernière, le DEP a retenu une procédure avec SAML 2 Token, SAML Artifact Binding et SAML Artifact Resolution via le service Web XML SOAP. Cette procédure garantit que les attributs d'identité de l'utilisateur sont exclusivement communiqués par un end point de service Web unique, crypté et authentifié par des certificats client et serveur.

Authentification et autorisation d'apps

En matière d'authentification et d'autorisation, le développement d'apps privilégie actuellement surtout la famille de protocoles OAuth-2.0 et le protocole OpenID-Connect basé sur ceux-ci. Ces protocoles passent pour être moins compliqués aux yeux des développeurs et permettent généralement d'implémenter plus rapidement l'authentification et l'autorisation que les procédures avec SAML, par exemple.

Authentification d'une app OpenID-Connect

Alors que le protocole SAML 2 fournit uniquement un cadre et laisse les développeurs de l'app et les services s'entendre sur l'implémentation proprement dite, l'appairement et les attributs d'identité sont prédéfinis sous OpenID Connect et peuvent être implémentés par les deux parties sans concertation. Dans une app OpenID Connect, l'authentification se déroule pour l'essentiel comme dans SAML Artifact Binding. Là aussi, les attributs d'identité sont exclusivement transmis par un canal dûment crypté et authentifié. Sous OpenID Connect, et contrairement à ce que prévoit le DEP (ATNA), l'application ne s'authentifie pas au moyen d'un certificat, mais à l'aide d'un code (secret) préalablement attribué et échangé de manière sécurisée.

Autorisation d'apps

La procédure OAuth d'autorisation se distingue nettement du modèle préconisé pour le DEP. Plutôt que d'attribuer préalablement des droits d'accès à certains utilisateurs, l'utilisateur permet explicitement à une application ou à certains utilisateurs d'obtenir un accès à des données. OAuth utilise à

cet effet une procédure de demande de consentement qui se déroule comme suit : l'app envoie une demande d'accès, l'utilisateur se connecte à son compte sur l'application du service, puis valide ou refuse explicitement l'accès à ses données.

Par contre, la procédure OpenID-Connect basée sur OAuth communique des attributs de l'identité des utilisateurs ; par conséquent, elle supporte aussi une gestion et une application centralisées des droits d'accès dans l'application de service, par ex. avec XACML, également exploité dans le cadre du DEP.

Discussion

Ces considérations montrent qu'à chaque niveau, l'authentification et l'autorisation sont des procédures largement indépendantes l'une de l'autre. Les capteurs s'authentifient généralement par reconnaissance d'appareil et les utilisateurs les autorisent par un mécanisme d'appairement ; s'agissant de l'authentification et de l'autorisation d'accès au DME, ce sont les dispositions légales de l'espace juridique concerné qui s'appliquent. Dans le cas particulier du DEP, l'enregistrement et l'interrogation des données sont régis par les dispositions d'exécution de la LDEP. Le service de communication doit gérer les attributs nécessaires à cet effet en fonction des utilisateurs ou les interroger explicitement juste avant l'accès.

Alors que les applications de service autonomes (par ex. portails Web) parviennent relativement facilement à satisfaire les exigences élevées du droit d'exécution de la LDEP, il en va différemment des apps mobiles qui réunissent les acteurs app et service sur un smartphone et veulent accéder directement au DEP. SAML 2 et les protocoles basés sur ce standard pour se raccorder à des IdP certifiés selon les dispositions d'exécution de la LDEP ne sont pas courants dans le développement d'apps destinées à des équipements mobiles et le support par des bibliothèques tierces (*3rd party libraries*) est de ce fait insuffisant. Le rajout d'OpenID Connect dans le droit d'exécution simplifierait fortement l'accès au DEP pour les apps mobiles en particulier et augmenterait le degré d'acceptation parmi les développeurs d'apps. Cela simplifierait beaucoup l'authentification via des fournisseurs d'identité certifiés et l'utilisation de JSON Web Token pour l'autorisation en combinaison avec les profils d'intégration mobiles.

L'exploitant peut librement choisir les procédures d'authentification dans le service, dans le cadre du droit applicable. D'après les auteurs, les deux méthodes couramment utilisées, à savoir SAML et Open ID Connect (OAuth), offrent le même niveau élevé de sécurité si elles sont implémentées correctement, sachant que la seconde est plus facile à mettre en œuvre et que les développeurs lui accordent leur préférence.[16]

La norme XACML d'OASIS est actuellement largement répandue pour formuler le consentement et exécuter les droits d'accès. Elle est d'ailleurs prescrite dans le droit d'exécution de la LDEP. Cette norme se prête également très bien à l'autorisation des accès par app en raison de sa flexibilité, de son large domaine d'application et, aspect non négligeable, des activités de développement dynamiques du comité OASIS.

Recommandation

Afin de rendre le DEP attrayant pour les apps mobiles, il faut inclure OpenID

[16] La simplicité est un critère de sécurité important car elle permet d'éviter des erreurs d'implémentation susceptibles d'entraver, voire de paralyser les mécanismes de sécurité des applications.

Connect dans le droit d'exécution de la LDEP. Cela simplifiera l'authentification via des fournisseurs d'identité certifiés, l'utilisation de JSON Web Token pour l'autorisation et l'utilisation de profils d'intégration mobiles IHE et entraînera aussi une plus grande acceptation de la part des développeurs d'apps.

3.3 Medical Devices

Les Medical Devices désignent l'ensemble des composants qui collectent les données en première ligne et alimentent le processus. Les normes d'élaboration d'interfaces géolocales ne sont pas l'objet de la présente analyse. Nous les considérons comme faisant partie intégrante des produits qui, par leur conception et leur fonctionnalité, sont susceptibles de séduire les utilisateurs et de les inciter à les utiliser. Il s'agit donc d'exploiter le marché au moyen de ces produits et de fidéliser la clientèle. Pour ces produits, la qualité et la fonctionnalité, qui pourraient être mises en avant par leur certification en tant que dispositifs médicaux, peuvent réellement faire la différence. La présente étude s'intéresse à la transmission de données au niveau suivant (app ou service), aux interfaces nécessaires à cet effet et à leur standardisation.
Cela offre une marge de manœuvre pour d'autres types de mesures et de transmissions, comme dans le cas de mesures uniques ou continues.

Medical Devices

3.4 Rapport avec des formats d'échange et mappage

Le dossier médical électronique enregistre des documents médicaux pertinents et les met à la disposition d'autres professionnels de la santé. La santé mobile enregistre et contrôle cependant aussi des données spécifiques. Le service (Healthcare Information System Interface dans le langage Continua) convertit les données en un document. Les directives Continua ont développé le document CDA PHMR[17] à partir de HL7 à cet effet. Ce document peut enregistrer les données de mesure en conséquence, mais suppose l'exploitation de capteurs basés sur IEEE 11073. Les codes/valeurs correspondants sont enregistrés en format IEEE. Le document fait une distinction entre les signes vitaux (*vital signs*) et d'autres valeurs. Si ce type de document est repris dans le DEP, il doit être défini en tant que format d'échange.
Pour revenir aux éléments de données à partir des documents enregistrés dans le DEP, il faut utiliser le nouveau profil IHE mXDE.

Rapport avec des formats d'échange

IHE mXDE

3.5 Premières expériences et approches nationales et internationales

3.5.1 Base de l'étude de l'architecture de référence nordique

La Norvège, la Suède, le Danemark et la Finlande élaborent actuellement une base commune pour une stratégie « Personal Connected health and care Technology » et ont publié un premier rapport à ce sujet en mars 2017[18].

Vue d'ensemble

[17] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=33
[18] http://www.hl7.fi/wp-content/uploads/Nordic-Reference-Architecture-for-Personal-Connected-Health-Technology-2017-03-19.pdf

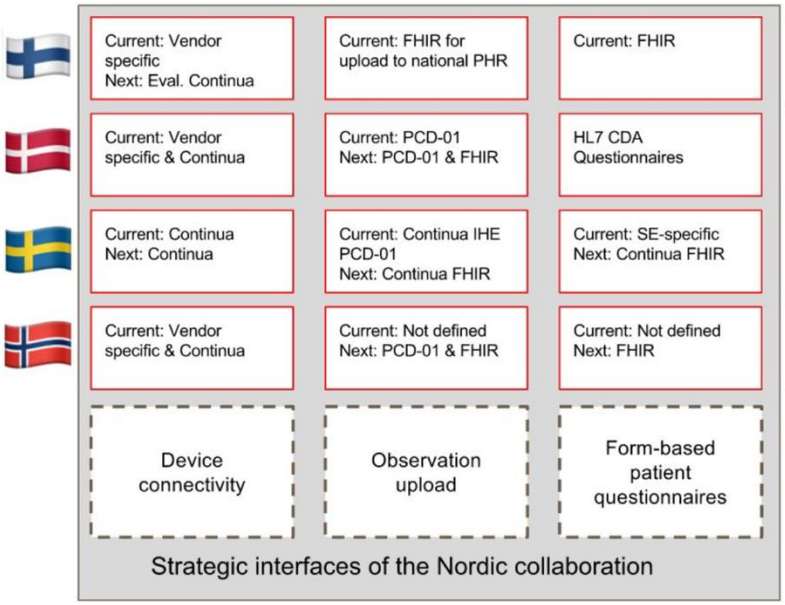

Figure 14: Strategic Interfaces Towards a Nordic Reference Architecture for Personal Connected health and care Technology

Aux yeux des fournisseurs qui opèrent à l'échelle mondiale, le domaine de la santé des pays nordiques constitue un petit marché. Le défi qui se pose est le suivant : les solutions globales doivent être adaptées aux solutions existantes au prix d'efforts considérables. Cette charge peut être allégée si l'on se fonde sur des normes et des profils internationaux dans le domaine de la santé, comme le proposent HL7, IHE et Continua. Même ainsi, la charge peut rester considérable car ces normes et profils ne sont pas forcément faciles à utiliser ou à développer. Les pays nordiques se sont regroupés pour établir les similitudes entre les cas d'application et élaborer un modèle de référence. Ils ont choisi les Continua Design Guidelines comme base de leur stratégie en matière de santé personnelle connectée. Le modèle doit cependant se fonder sur une architecture plus moderne et plus facilement implémentable, elle-même basée sur FHIR et OAuth, comme pour l'*Observation Upload* et la technologie de formulaire, par exemple.

Appréciation

Cela constitue une avancée considérable dans le domaine en question, dont la Suisse peut profiter.

Conclusion

Pour pouvoir exploiter les synergies existantes et introduire des éléments qui nous sont propres, une manière de procéder identique est recommandée pour la Suisse.

3.5.1.1 Directive cadre applicable à l'infrastructure IT des applications de télémonitoring : Autriche

Vue d'ensemble

Une directive cadre est mise en consultation jusqu'en novembre 2017 en Autriche. Elle doit ensuite être soumise pour adoption à la commission fédérale concernée (Zielsteuerungskommission).[19]

La directive concerne uniquement le télémonitoring de patients désireux de disposer d'un outil supplémentaire pour le traitement et la surveillance de leur maladie.

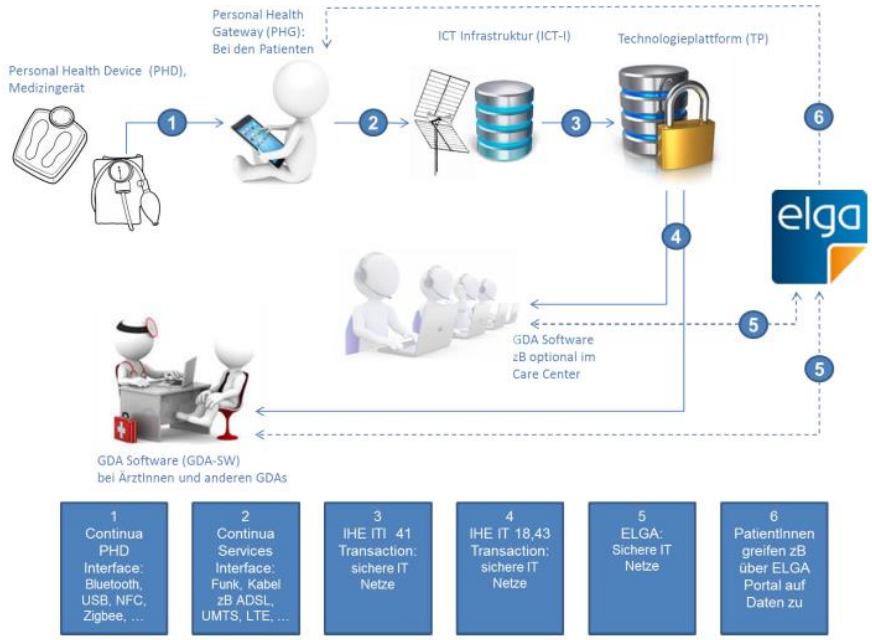

Figure 15: Raccordement de fournisseurs de prestations de santé à la plateforme technologique de télémonitoring et à un domaine ELGA (source : directive cadre)

L'architecture s'inspire de la terminologie et des normes des Continua Design Guidelines et de IHE/HL7 et fixe les standards à appliquer à chaque transaction :

1. Transmission de données de mesures PHD vers PHG : TAN/PAN/LAN Interface selon les Continua Design Guidelines
2. Transmission de données de mesures PHG vers l'infrastructure ICT (ICT-I) : transactions PCD-01 et PCD-09 selon le cadre technique PCD IHE
3. Transmission de données de mesures ICT-I vers la plateforme technologique (TP) : transaction ITI-41 selon l'IHE IT Infrastructure Technical Framework, les données étant codées comme HL7 CDA, par analogie à HL7 CDA PHMR
4. Transmission de données de mesures TP vers le logiciel GDA : transaction ITI-18 et ITI-43 selon l'IHE IT Infrastructure Technical Framework, les données étant codées comme HL7 CDA par analogie à HL7 CDA PHMR

[19] https://www.bmgf.gv.at/home/Rahmenrichtlinie_IT-Infrastruktur-Telemonitoring_Messdatenerfassung

5. La communication entre le logiciel GDS et la solution ELGA s'effectue selon les spécifications ELGA.

Cette architecture ne prévoit pas d'échange direct de données entre la plateforme technologique et ELGA. La plateforme est toutefois basée sur les services centraux d'ELGA.

La directive cadre mentionne également que de nombreux projets de standardisation se déroulent actuellement dans ce domaine et que ceux-ci doivent contribuer activement aux activités internationales. Par ailleurs, les critères et les approches de l'Autriche relatives à Continua, IHE, HL7 et IEEE doivent venir renforcer la coordination internationale.

L'Autriche mise résolument sur les Continua Design Guidelines en matière de télémonitoring. — Appréciation

Pour pouvoir exploiter les synergies existantes et introduire de propres éléments, une manière de procéder identique est recommandée pour la Suisse. — Conclusion

3.5.2 Review of useful Information a Patient can provide Concept of Structuration of mHealth Data (MAS BFH, Cédric Michelet)

Ce travail considère et évalue les données collectées, leur importance et leur disponibilité dans les services les plus divers (*measurements store*) et cherche dans quelle mesure elles peuvent être exploitées dans le cadre du DEP. Il analyse les standards proposés par les services et s'intéresse en particulier à l'utilisation de HL7 CDA comme format cible pour le mappage de la communication des services vers le DEP. — Aperçu

En résumé, l'auteur de la recherche constate qu'aucun des services n'exploite un standard pour valider les données, mais que toutes les interfaces d'exportation peuvent être mappées sur HL7 CDA. Certaines limitations découlent d'exigences spécifiques des services à l'égard de l'environnement (l'app Healthkit d'Apple requiert le système d'exploitation iOS).

On peut déduire de cette étude les points suivants pour les recommandations à formuler dans la présente analyse : — Appréciation

- Aucun standard supplémentaire ne doit être pris en compte dans la présente analyse.
- HL7 CDA est approprié comme format cible pour enregistrer des données de santé mobile dans le DEP.
- La démonstration de faisabilité (*proof of concept*) de l'exportation a était fait sur eHealth Connector et CDA; l'étude n'analyse donc pas de variantes, comme HL7 FHIR.

Les deux recherches ne se recoupent pratiquement pas. Lorsque cela se produit, les considérations et thèses formulées dans l'un des travaux corroborent celles de l'autre. — Conclusion

4 Appréciation des normes et standards étudiés

Discussions Synthèse

De manière générale, on observe que la santé mobile recourt à trois liaisons totalement différentes entre les capteurs et le DME/DEP, pour des cas d'application différents faisant l'objet d'une gestion dédiée. Il en découle qu'on ne trouve pas d'ensemble de normes complet dont on pourrait suivre les préconisations.

Les éléments et composants dont l'utilisation est recommandée sont nombreux. La Suisse a la possibilité d'observer et d'accompagner les démarches entreprises dans les pays nordiques et en Autriche. Dans le meilleur des cas, elle pourra avoir une influence sur les développements en cours et en venir à préconiser ou à rendre obligatoires les résultats de ces travaux pour les implémentations en Suisse.

Alors que le DEP est régi par des dispositions exhaustives et contraignantes, la liaison entre les capteurs et les apps ou les services reste soumise aux mécanismes du marché, qui ne peuvent ni ne doivent être réglementés de manière exhaustive.

Protection et sécurité des données

Du capteur au DME en passant l'app et le service, les exigences de protection et de sécurité des données s'accroissent fortement et doivent recevoir l'attention nécessaire.

Ces aspects ont été abordés sous un angle technique, en lien avec les normes étudiées. La réflexion n'a pas été poussée pour englober des aspects plus généraux.

Nous rappelons qu'une expertise juridique est en cours d'élaboration.

Authentification et autorisation

L'authentification et l'autorisation à chaque niveau sont presque entièrement indépendantes les unes des autres.

L'alimentation et la consultation du DEP sont régies par le droit d'exécution de la LDEP. Le service qui sert d'intermédiaire doit gérer les attributs requis en fonction de chaque utilisateur ou les rechercher explicitement juste avant l'accès.

Le rajout d'OpenID Connect dans les dispositions d'exécution de la LDEP simplifierait fortement l'accès au DEP pour les apps mobiles en particulier et augmenterait le degré d'acceptation parmi les développeurs d'apps. Cela simplifierait beaucoup l'authentification via des fournisseurs d'identité certifiés et l'utilisation de JSON Web Token pour l'autorisation en combinaison avec les profils d'intégration mobiles.

À la connaissance des auteurs, les deux méthodes couramment utilisées, à savoir SAML et Open ID Connect (OAuth), offrent le même niveau élevé de sécurité si elles sont implémentées correctement, sachant que la seconde est plus facile à mettre en œuvre et que les développeurs lui accordent leur préférence[20].

Concernant la formulation du consentement et l'application des droits d'accès, la norme XACML d'OASIS est largement répandue à l'heure actuelle. Elle est d'ailleurs prescrite dans le droit d'exécution de la LDEP, par exemple.

[20] La simplicité est un critère de sécurité important car elle permet d'éviter des erreurs d'implémentation susceptibles d'entraver voire de paralyser les mécanismes de sécurité des applications.

5 Recommandations

Utiliser les directives Continua	Recommandation 1
Les directives Continua couvrent la totalité du champ technologique allant du capteur jusqu'au dossier basé sur des documents. C'est pourquoi la Suisse doit impérativement adopter l'architecture des directives Continua. Elle pourra ainsi participer aux évolutions internationales en exerçant une influence. Cela installera la Suisse dans une démarche proche de celle des pays nordiques et de l'Autriche tout en créant un potentiel de synergies pour toutes les parties prenantes. Mais les directives Continua ayant une portée très large, les recommandations suivantes ont été élaborées pour l'application de ces directives dans le contexte de la santé mobile et du DEP (cf. recommandations 1.1 à 1.4).	Explication
Service Interface : utiliser H.812.5 FHIR Observation Upload	Recommandation 1.1
La transmission entre l'app et le service ne se déroulera pas au sein d'une institution, ce qui signifie qu'il n'est pas facile d'appliquer le protocole IHE-PCD-01 basé sur HL7 V2. Malgré son approbation par Object Management Group (OMG) et HL7, hData ne s'est pas répandu aux États-Unis en dehors des directives Continua. FHIR Observation Upload couplé à OAuth est la méthode la plus simple à implémenter. Elle permet d'intégrer l'architecture SMART on FHIR pour les apps dans une interface avec le service.	Explication
Gérer les consentements sur la base de XACML au lieu de Continua	Recommandation 1.2
La norme XACML d'OASIS est actuellement très répandue pour formuler le consentement et exécuter les droits d'accès. Elle est d'ailleurs prescrite dans le droit d'exécution de la LDEP, par exemple. Cette norme se prête également très bien à l'autorisation des accès par app en raison de sa flexibilité, de son large domaine d'application et, ce qui n'est pas négligeable, des activités de développement dynamiques du comité OASIS.	Explication
Élaborer une technologie de formulaire élargie	Recommandation 1.3
La technologie CDA, prévue par les directives Continua pour les formulaires, n'est pas encore très utilisée et semble trop lourde pour le domaine de la santé mobile. Les pays scandinaves préfèrent recourir à des variantes basées sur des formulaires utilisant des ressources FHIR (trois pays sur quatre). En Suisse, une technologie IHE Proposal ORF (Order & Referral by Form) reposant également sur des ressources de formulaire FHIR, est en cours de développement et promet des synergies.	Explication
Anticiper le format d'échange PHMR basé sur FHIR	Recommandation 1.4
Hospital Interface : les transactions XDS pour l'enregistrement de documents sont obligatoires dans le contexte du DEP. Pour le contenu du document, les directives Continua prévoient le format CDA PHMR. Comme la norme HL7 FHIR est préconisée pour l'interface avec le service, il serait plus simple d'enregistrer dans le DEP un document constitué à partir de ces ressources FHIR (*bundle*) plutôt que de le convertir en document CDA PHMR. Selon des responsables, il est envisagé de définir un document FHIR PHMR pour la version 2019 des directives Continua. En ce qui concerne les formats d'échange, nous recommandons d'attendre pour voir si les choses évoluent dans cette direction.	Explication

Suivre une méthode SMART on FHIR	Recommandation 2
La méthode SMART on FHIR permet de développer des apps découplées du système primaire. Quelques projets en Suisse ont commencé à travailler sur cette méthode. Pour pouvoir la réaliser, il faut adapter les ressources FHIR aux prescriptions suisses (profilage). Il est également important dans ce cadre que la description dans les formats d'échange du DEP soit définie afin de ne pas créer d'obstacles à l'intégration entre la santé mobile et le DEP.	Explication
Étendre le droit d'exécution de la LDEP aux technologies Web mobiles	Recommandation 3
Pour rendre le DEP attractif pour les apps mobiles, il faut inclure OpenID Connect dans le droit d'exécution de la LDEP. Fondé sur OAuth 2.0, OpenID Connect simplifiera l'authentification via des fournisseurs d'identité certifiés, l'utilisation de JSON Web Token pour l'autorisation et l'utilisation de profils d'intégration mobiles IHE. Cela améliorera l'acceptation des développeurs d'apps.	Explication
Utiliser les profils d'intégration mobiles de IHE	Recommandation 4
Pour rendre le DEP attractif pour les apps mobiles, il faut inclure dans le droit d'exécution de la LDEP les profils d'intégrations mobiles de IHE (MHD, PDQm, PIXm). Cela améliorera l'acceptation des développeurs d'apps.	Explication

Annexe 1 : Glossaire

Abréviation	Signification
ACM	Alert Communication Management
API	Application Programming Interface
CDA	Clinical Document Architecture (format d'échange basé sur HL7 V3.0)
cMHAFF	Consumer Mobile Health Application Functional Framework
CTO	Critères techniques et organisationnels (ODEP)
DEC	Device Enterprise Communication
DEP (L)	Dossier électronique du patient, dossier médical électronique selon la législation fédérale suisse
DME	Dossier médical électronique
ELGA	Elektronische Gesundheitsakte (DME autrichien)
FHIR	Fast Healthcare Interoperability Resources (basé sur HL7)
hData	Service Web de spécification pour l'échange de données de santé électroniques
HL7	Health Level 7 (norme pour l'échange de données dans le domaine de la santé, V2.0 et V3.0)
HTTP	Hypertext Transfer Protocol
IDCO	Implantable Device Cardiac Observation
IdO	Internet des objets
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating Healthcare Enterprises (définit des profils de communication pour l'échange de données dans le domaine de la santé)
JSON	JavaScript Object Notation
LPD	Loi sur la protection des données
MHD, PIXm, PDQm, XUA, IUA, ATNA	Profils IHE (m = extension à la communication mobile), ne sont pas décrits ici.
mHealth	Mobile Health (santé mobile = domaine de la santé utilisant des capteurs et des appareils mobiles)
MQTT	Protocole de message ouvert pour la communication de machine à machine (M2M)
NFC	Near Field Communication
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Protocole assurant une gestion standardisée et sûre des autorisations par API pour les applications de bureau, en ligne et mobiles
ODEP	Ordonnance sur le dossier électronique du patient
OpenID Connect	Couche d'authentification basée sur le protocole d'autorisation OAuth 2.0
PCD	Patient Care Device (basé sur IHE)
PHD	Personal Health Device
PHG	Personal Health Gateway
PHMR	Personal Health Monitoring Report
PIV	Point-of-Care Infusion Verification (point de vérification de la perfusion)
QFD	Quality Function Deployment
QRD	Quality Review of Documents
RESTful	Méthode pour faire communiquer un client basé sur le Web et un serveur

RTM	Rosetta Terminology Mapping
SAML	Security Assertion Markup Language
SMART	Substitutable Medical Applications, Reusable Technologies
SOAP	*Simple Object Access Protocol*
UOM	Conversion d'unités
USB	Universal Serial Bus
WAI	La *Web Accessibility Initiative* (WAI) fait partie du W3C. Elle se compose de plusieurs groupe d'intérêts et groupes de travail consacrés à l'accessibilité du Web et de ses contenus aux personnes handicapées.
W3C	Le *World Wide Web Consortium* (W3C) est le comité dédié à la normalisation des technologies du Web.
XACML	eXtensible Access Control Markup Language
XML	Extended Markup Language
Zigbee	Protocole basé sur IEEE pour les réseaux sans fil transportant de faibles volumes de données