Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Berne, 1er juin 2023

Modification de l'ordonnance du DFI sur le dossier électronique du patient

Révision annuelle 2023 (annexes 2 à 5, 8 et 9, y compris compléments 1 et 2.1 à 2.3 à l'annexe 5)

Rapport explicatif

BK-D-BF8A3401/507

1 Contexte

Le Parlement a adopté la loi fédérale sur le dossier électronique du patient (LDEP ; RS *816.1*, FF **2015** 4419) le 19 juin 2015. Loi-cadre, la LDEP régit les conditions auxquelles est assujetti le traitement des données du dossier électronique du patient (DEP).

Par sa décision du 22 mars 2017, le Conseil fédéral a fixé la date d'entrée en vigueur de la LDEP et de son droit d'exécution au 15 avril 2017. L'ordonnance du 22 mars 2017 sur le dossier électronique du patient (ODEP ; RS *816.11*) délègue au DFI les compétences législatives spécifiques pour définir les modalités des conditions de certification des communautés et des communautés de référence ainsi que des éditeurs de moyens d'identification.

2 Nécessité d'une révision

La présente révision porte sur les annexes 2, 3, 4, 5, 8 et 9 ainsi que sur les compléments 1, 2.1, 2.2 et 2.3 à l'annexe 5 de l'ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI ; RS *816.111*). Elle vise à clarifier des imprécisions techniques et à corriger des erreurs qui se sont fait jour dans les diverses spécifications lors des procédures de certification, ou ont été relevées par les spécialistes techniques des fournisseurs de plateformes et des systèmes primaires.

2.1 Plan de médication (Medication Card Document)

Dans le cadre du DEP, la disponibilité et l'échange des données concernant la médication sont un aspect essentiel de l'information, pour tous les patients comme pour les professionnels de la santé impliqués. Il est important que les patients et les professionnels de la santé aient accès en tout temps à un aperçu aussi à jour que possible de la médication. En outre, la motion Stöckli 18.3512 « Droit à un plan de médication en vue de renforcer la sécurité des patients » demande que le Conseil fédéral soumette au Parlement une base légale conférant aux patients qui doivent prendre au moins trois médicaments en même temps le droit d'obtenir un plan de médication sous forme électronique ou sur papier.

Le plan de médication (Medication Card Document) offre une vue d'ensemble aussi complète que possible des médicaments que le patient prend au moment considéré. Il sert de base à une anamnèse optimale de la médication et à un contrôle complet des interactions. Quant au patient, le plan de médication lui indique quand et comment il doit prendre quels médicaments et ce à quoi il faut prêter attention lors de ces prises.

2.2 OpenID Connect

Le protocole OpenID Connect (OIDC) est une norme moderne qui permet la communication entre plusieurs applications. Il est particulièrement bien adapté pour connecter un utilisateur sur différents services après une authentification unique sur un système central. Cette approche est également appelée « fédération d'identité » (*Identity Federation*), ou encore *Single-Sign-On (SSO)*. Elle simplifie considérablement l'utilisation d'un système complexe : l'utilisateur n'a besoin de s'authentifier que sur un seul système, sans devoir gérer les paramètres d'identification individuels sur chacun des différents services.

L'OIDC constitue ainsi une solution de rechange au Security Assertion Markup Language (SAML) déjà établi. Il couvre les mêmes fonctions que SAML avec le même niveau de sécurité, mais il est actuellement plus répandu sur le marché. L'intégration de l'OIDC dans les systèmes primaires, notamment, est plus simple que celle du SAML et peut donc potentiellement inciter davantage de fournisseurs de prestations à intégrer leurs systèmes primaires en profondeur.

Des mesures doivent être prises lors de l'utilisation du protocole OIDC afin de garantir la sécurité des données échangées. Il est important en particulier que les messages échangés entre les systèmes participants portent une signature cryptographique et que la signature soit vérifiée par le destinataire. Ces deux mesures sont prévues dans la version révisée de l'annexe 8.

L'implémentation du protocole OIDC requiert un travail important. Aussi, en concertation avec les fournisseurs d'identité, il a été décidé de la définir comme optionnelle dans la présente édition.

3 Commentaire des dispositions modifiées

3.1 Annexe 2 : Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence

Ch. 2.3.2 *Mise en œuvre des décisions d'accès*

Ce chiffre est abrogé. La vérification de l'exactitude des décisions d'accès est déjà suffisamment couverte par les spécifications énoncées à l'annexe 5 dans les profils techniques, avec le SIAS (Swiss Interoperability Conformity Assessment Scheme) et les tests approfondis qui doivent être menés dans les cas d'application complexes.

Ch. 2.6 *Destruction de données*

Cette modification ne concerne que le texte allemand (« Löschen » est remplacé par « Vernichtung »). Elle ne change rien au fond des spécifications.

Ch. 2.9 *Prescriptions relatives à la gestion et au transfert des données du dossier électronique du patient*

Un grand nombre de dispositions dans cette section ont été biffées car leur contenu est suffisamment couvert par le renvoi à l'annexe 5 ODEP-DFI. Cela concerne les chiffres suivants : 2.9.4, 2.9.5, 2.9.5*a*, 2.9.6, 2.9.7, 2.9.7*b*, 2.9.7*c*, 2.9.8, 2.9.9, 2.9.10, 2.9.11, 2.9.12, 2.9.13, 2.9.13*a*, 2.9.14, 2.9.15, 2.9.16, 2.9.16*a*, 2.9.17, 2.9.18, 2.9.19, 2.9.19*a*, 2.9.20, 2.9.21, 2.9.22, 2.9.23, 2.9.24, 2.9.25, 2.9.27 et 2.9.28.

Ch. 2.9.3 *Profils d'intégration IHE, adaptations nationales des profils d'intégration IHE et profils d'intégration nationaux*

La disposition est complétée par la mention explicite des acteurs et des transactions des profils tels que définis à l'annexe 5 ODEP-DFI.

Ch. 2.9.7a *Communication d'identités attestées*

Cette disposition est biffée, les spécifications qu'elle contient étant déplacées dans le complément 1 à l'annexe 5.

Ch. 2.9.26a *Authentification avec des certificats valables*

Il est désormais question de points d'accès, et non plus de points de terminaison. Cela ne change rien au fond des spécifications.

Ch. 2.10 *Données historisées*

Par souci de clarté, il est précisé que les données historisées dont il est question dans cette disposition sont historisées avec les profils ATNA et C:ATC tels que définis à l'annexe 5 OPDE-DFI. L'ancienne formulation ne permettait pas de savoir clairement si cette disposition s'appliquait aussi aux journaux des systèmes.

Ch. 2.10.5 *Données historisées*

Cette disposition est biffée car l'étendue de l'historisation est déjà définie avec suffisamment de précision à l'annexe 5.

Ch. 2.10.7 *Données historisées*

Il est précisé à la *let. a* que la disposition vise les données historisées avec le profil CH:ATC. À la *let. e*, l'expression « administrateurs du système » est remplacée par « utilisateurs administratifs ». Cette catégorie d'utilisateurs inclut les administrateurs système, mais aussi tous les autres utilisateurs accomplissant des tâches administratives pour une communauté.

Ch. 3.1b *Fiabilité des portails d'accès*

Cette disposition dérogatoire est biffée car aucune communauté ne l'applique à ce jour. Les allégations d'attributs relatifs à la sécurité doivent toujours être vérifiées auprès d'une source de données fiable. Cela renforce la sécurité de l'infrastructure du DEP.

Ch. 3.4.2 *Exigences techniques*

Cette disposition est biffée, son contenu étant déplacé au ch. 4.4.3, let. d.

Ch. 4.2.1 *Système de gestion de la protection et de la sécurité des données*

La référence à la norme ISO/IEC 27002 est actualisée : la version de 2022, intitulée « Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité de l'information » remplace la version de 2017-06.

Ch. 4.4.3 *Gestion des failles de sécurité*

La *let. c* est reformulée de façon à viser tous les types connus d'attaque et de compromission, et non pas seulement un scénario d'attaque spécifique. Compte tenu en outre de la nouvelle *let. d*, ce chiffre remplace trois dispositions biffées : les ch. 3.4.2, 4.18, let. f, et 9.6.2.

Ch. 4.6.2 *Gestion des moyens informatiques et des recueils de données sensibles*

L'indication des acteurs IHE dans la liste des éléments de l'infrastructure informatique est supprimée. Cela ne change rien au fond des spécifications.

Ch. 4.6.5 *Gestion des moyens informatiques et des recueils de données sensibles*

La modification précise qu'à l'occasion de son réexamen l'« inventaire de l'infrastructure informatique » doit être actualisé.

Ch. 4.7.1 *Prescriptions relatives à la protection et à la sécurité des données imposées aux institutions de santé affiliées ainsi qu'à leurs professionnels de la santé et à leurs terminaux*

La disposition exige à présent que les communautés et les communautés de référence emploient la forme écrite pour astreindre les institutions de santé à leurs obligations en matière de protection et de sécurité des données.

Ch. 4.18 *Accessibilité*

Une nouvelle exigence est introduite à la *let. a*^{bis} : les données doivent rester disponibles lorsqu'une communauté cesse son activité. La nouvelle *let. a*^{ter} demande que les métadonnées, en particulier le rôle de la personne détentrice, soient conservées en cas de migration des données. La *let. f* est biffée, son contenu étant repris à la let. d du ch. 4.4.3.

Ch. 8.2.1 *Identification des patients*

Les prescriptions contenues au ch. 8.2.1. dans la précédente version de l'annexe 2 ont été réparties dans les ch. 8.2.1 à 8.2.1*b*. Le ch. 8.2.1 liste désormais seulement les possibilités d'identification des personnes qui, en vertu de l'art. 17, al. 1, let. b, ODEP, souhaitent ouvrir un DEP. Cette énumération explicite des moyens d'identification reconnus dans le processus d'ouverture d'un DEP remplace le renvoi à l'art. 24 ODEP qui figurait à la *let. a*.

Sur le plan matériel, les exigences en matière d'identification des personnes ont été étoffées. Selon la *let. d*, les passeports et les cartes d'identité suisses périmés sont reconnus à la condition qu'ils soient accompagnés d'autres documents ou complétés par une déclaration d'identification émise par des proches ou par une autorité. Il faut que la pièce d'identité périmée et les autres documents produits permettent d'identifier la personne de manière fiable. Il est envisageable de produire la carte d'assurance-maladie, un permis d'établissement et des cartes bancaires, par exemple. Les communautés de référence conservent la compétence de définir les modalités de détail et le processus d'identification des personnes qui souhaitent ouvrir un dossier électronique. Cela concerne aussi notamment les autres documents à produire pour pouvoir réaliser une identification sûre. Cette adaptation a en particulier pour but de faciliter l'ouverture d'un dossier électronique lorsque l'accès à une pièce d'identité valable est compliqué (p. ex. personnes en EMS ayant perdu toute mobilité).

La *let. m* introduit la possibilité d'ouvrir un DEP avec une carte d'identité étrangère, mais à la condition que celle-ci autorise l'entrée en Suisse et que son titulaire puisse apporter à la communauté de référence la preuve qu'il fait ménage commun avec le titulaire d'une carte de légitimation telle que définie à l'art. 17 de l'ordonnance sur le pays hôte.

Ch. 8.2.1a *Identification des patients (enfants jusqu'à 12 ans)*

Le ch. 8.2.1*a* introduit une règle spéciale pour les enfants de moins de 12 ans. Il permet d'identifier l'enfant au moyen d'une carte d'assurance-maladie suisse en combinaison avec l'acte de naissance ou un autre document approprié pour l'identification. Cette disposition a été formulée à dessein de manière ouverte afin que les communautés de référence puissent fixer elles-mêmes les exigences précises à respecter, comme dans le cas des passeports suisses périmés, et ainsi tenir compte des contraintes pratiques.

Ch. 8.2.1b *Identification des patients (autres processus)*

Cette disposition régit les autres exigences posées au processus d'identification, qui figuraient au ch. 8.2.1, let. b à e, dans la précédente version.

Ch. 8.6.3 *Gestion des autorisations*

La *let. c* précise que les informations sur l'intégration de professionnels de la santé dans les groupes autorisés ne sont à communiquer que si le patient en fait la demande.

Ch. 9.1a *Fiabilité des portails d'accès*

Cette disposition dérogatoire est biffée car aucune communauté ne l'applique à ce jour. Les allégations d'attributs relatifs à la sécurité doivent toujours être vérifiées auprès d'une source de données fiable, ce qui accroît la sécurité.

Ch. 9.6.2 *Exigences techniques*

Cette disposition est biffée car son contenu est déplacé à la let. d du ch. 4.4.3.

3.2 Annexe 3 : Métadonnées pour l'échange de données médicales

Ch. 1.1 *Rattachement des attributs des métadonnées visées à l'annexe 3 aux attributs des métadonnées des profils d'intégration visés à l'annexe 5*

La désignation de l'attribut « Spécialité de l'auteur » est adaptée selon la version 2.1 du manuel « IHE IT Infrastructure Handbook ».

Ch. 2.2 *Spécialité de l'auteur*

La modification du ch. 1.1 (voir ci-dessus) oblige à modifier le ch. 2.2. En outre, certains concepts ont été précisés et des corrections typographiques ont été apportées (emploi des majuscules et des minuscules).

Ch. 2.3 *Type organisationnel de l'institution de santé*

La liste comprend un nouveau type d'institution de santé : Free-standing birthing center (environment).

Ch. 2.4 *Spécialisation de l'institution de santé*

Quatre spécialisations ont été rajoutées : Obstetrics (qualifier value), Vascular surgery (qualifier value), Emergency medicine (qualifier value) et Dentistry (qualifier value).

Ch. 2.6 *Type du document*

Un nouveau type de document figure dans la liste : Digital representation of specimen (record artifact). De plus, diverses fautes d'orthographe ont été corrigées.

Ch. 2.7 *Types de documents autorisés par catégorie de documents*

La modification apportée au ch. 2.6 est reportée dans cette section afin d'associer le nouveau type de document à la catégorie correspondante. De plus, diverses fautes d'orthographe ont été corrigées.

Ch. 2.12 *Format technique détaillé*

Un nouveau format a été introduit pour le plan de médication : CH EMED Medication Card document.

3.3 Annexe 4 : Formats d'échange

Ch. 3 *Informations administratives*

La version applicable de CH Core a été actualisée, la version 3.0.0 remplaçant la version 2.1.0. L'actualisation comprend des modifications techniques de la norme. Celles-ci concernent, par exemple, la vérification du numéro GLN, qui ne doit pas dépasser 13 chiffres. Par ailleurs, des adaptations ont été apportées aux spécifications pour améliorer leur lisibilité.

Ch. 4 *Format d'échange Dossier électronique de vaccination (CH VACD)*

La version du format d'échange CH VACD passe de 2.1.0 à 3.0.0. Cette actualisation comprend des adaptations techniques.

La version des ensembles de valeurs passe également de 2.1.0 à 3.0.0. Les modifications comportent des ajouts, concernant par exemple la vaccination contre la variole du singe (mpox), et des fautes d'orthographe ont été corrigées.

Ch. 5 *Format d'échange Cybermédication (CH EMED)*

Le format d'échange Cybermédication permet de saisir, d'administrer et de représenter les données de médication des patients. Sa mise en œuvre doit obéir aux spécifications détaillées CH EMED (ch. 5) pour les documents FHIR. La modification introduit d'abord le document Plan de médication (ch. 5.1) du format d'échange Cybermédication. Elle définit ensuite les métadonnées qui doivent impérativement être attribuées au plan de médication (ch. 5.1.1). Les métadonnées permettent entre autres de reconnaître les documents.

3.4 Annexe 5 : Profils d'intégration

Dans son annexe 5, l'ODEP-DFI fixe les profils d'intégration à utiliser dans le contexte du DEP. Le complément 1 à l'annexe 5 décrit les adaptations nationales des profils IHE standard. Le complément 2.1 définit les profils d'intégration nationaux CH:ADR et CH:PPQ, le complément 2.2 le profil d'intégration national CH:ATC et le complément 2.3 le profil d'intégration national CH:CPI. Ces spécifications doivent être adaptées aux évolutions techniques.

3.4.1 Annexe 5 (partie publiée au recueil officiel)

Ch. 1 et 2 *Profils d'intégration IHE et profils d'intégration nationaux*

La version 20.0 du document technique « IHE Radiology Technical Framework » a été publiée le 10 mars 2022 tandis que la version 19 du document technique « IHE IT Infrastructure Technical Framework » est parue le 17 juin 2022. Ces mises à jour contiennent de nouveaux profils ainsi que des changements pertinents pour le DEP proposés par la Suisse concernant les profils d'intégration Restricted Metadata Update (RMU) et Healthcare Provider Directory (HPD).

Les références aux documents techniques précités ont été adaptées dans les tableaux listant les profils d'intégration (ch. 1 et 2) ainsi que dans le complément 1.

3.4.2 Complément 1 à l'annexe 5 : Adaptations nationales des profils d'intégration selon l'art. 5, al. 1, let. b, ODEP-DFI

Ch. 1.3 *Requirements on XDS-I.b*

Depuis l'entrée en vigueur de la LDEP en 2017, il est prévu de raccorder des archives d'images radiologiques au DEP. L'ordonnance est précisée afin d'assurer la réalisation correcte des accès aux études DICOM dans les archives d'images radiologiques des hôpitaux au moyen de l'infrastructure du DEP et la prévention des utilisations abusives. Il est stipulé en particulier que seul l'utilisateur technique est autorisé à mettre à disposition des objets DICOM Key Object Selection (KOS) dans le DEP. On empêche ainsi que des patients ou des professionnels de la santé ne déposent dans le dossier des objets KOS manipulés pour obtenir un accès non autorisé aux études d'autres patients. Ce risque n'a cependant jamais existé dans la pratique, car il n'est pas encore possible de raccorder des archives d'images radiologiques.

Ch. 1.5.1 *Precisions on Authenticate Node [ITI-19]*

Dans la nouvelle version du document « IHE ITI Technical Framework » (cf. 3.4.1), plusieurs versions de TLS peuvent être utilisées pour la transaction Authenticate Node [ITI-19]. Les ch. 1.5.1 et 1.5.2 ont été rajoutés pour préciser qu'il faut utiliser au moins la version 1.2 de TLS (STX: TLS 1.2 floor using BCP195 Option).

Ch. 1.6.2 Actors / Transactions

Les acteurs IHE sont des composants logiciels qui communiquent entre eux via des interfaces standardisées (transactions). La convention IHE permet de regrouper des acteurs, ce qui implique qu'il faut toujours implémenter l'ensemble des transactions des acteurs regroupés. Les groupes existants ont entraîné l'obligation d'implémenter des transactions inutiles. La présente modification redéfinit le groupage des acteurs pour l'adapter à la réalité.

Ch. 1.6.3 Actor Grouping

La modification du ch. 1.6.2 (voir ci-dessus) oblige à modifier le ch. 1.6.3 : le tableau 7 est complété avec les groupes d'acteurs corrects.

Ch. 1.6.4 Transactions

L'édition 3 de l'annexe 8 ODEP-DFI donne un ancrage légal au protocole OpenID Connect, en plus du protocole SAML, afin qu'il soit possible de se connecter DEP avec des appareils mobiles, en utilisant des interfaces mobiles.

Pour que le protocole OpenID Connect fonctionne aussi dans les communautés et les communautés de référence ainsi que dans les systèmes primaires, il est rajouté en option dans le profil XUA (sous-rubriques du ch. 1.6.4).

Ch. 1.6.4.3.4.2 Message Semantics

Dans les spécifications de la transaction Provide X-User Assertion du profil XUA, nécessaire par exemple pour déterminer les droits d'accès lors d'une recherche de documents, des corrections ont été apportées aux dispositions relatives à la structuration des attributs des éléments « organization » et « organization-id » afin d'empêcher des implémentations erronées et d'améliorer l'interopérabilité.

Ch. 1.11.5.1.2 Attribute

Des précisions sont apportées aux prescriptions suisses relatives au profil Health-Provider-Directory (HPD) : dans l'élément « prefix », l'Assigning Authority est la communauté ou la communauté de référence et, de manière générale, il faut employer uniquement des doubles points afin de ne pas contrevenir à la norme ISO 21091. Par ailleurs, seuls les caractères suivants sont autorisés dans le champ UID du profil HPD : caractères alphanumériques moins (-), double point (:), point d'exclamation (!), barre verticale (|), tiret bas (_), point (.). Il est arrivé que l'emploi de caractères non autorisés crée des problèmes et empêche de retrouver une entrée HPD lors de recherches.

Ch. 1.14 Requirements on Medication Card document

Les ch. 1.13 et 1.14 contiennent la description des acteurs IHE requis pour afficher et valider le plan de médication. Les acteurs IHE *Content Consumer* et *Content Creator* ont été rajoutés dans le complément 1 à l'annexe 5 ODEP-DFI.

3.4.3 Complément 2.1 à l'annexe 5 : Profils d'intégration nationaux selon l'art. 5, al. 1, let. c, ODEP-DFI – Authorization Decision Request (CH:ADR) and Privacy Policy Query (CH:PPQ)

Ce complément contient les spécifications techniques applicables à la gestion des autorisations d'accès au DEP. Ces spécifications évoluant au fil du temps, elles ont été complètement remaniées en tenant compte d'enseignements remontés de la pratique, qui ont été collectés en continu. Ces enseignements ont ainsi désormais un caractère obligatoire, ce qui aura un impact positif sur la sécurité et sur la protection des données. Les spécifications énoncées dans le complément ont été réduites à l'essentiel et les exemples de code ont été déplacés dans un autre document. En outre, les schémas XML pour la définition des droits d'accès au DEP ont été développés et l'obligation de les utiliser a été inscrite dans un texte normatif, alors qu'elle ne l'était pas auparavant. Dans ce contexte, un schéma de contrôle a été développé et mis en référence dans l'annexe (ch. 4.1). Ces nouvelles dispositions ont pour but d'empêcher les indications non autorisées lors de l'octroi ou de la modification de droits d'accès.

Par ailleurs, la modification précise les dispositions de détail relatives au raccordement d'archives d'imagerie à l'infrastructure DEP d'une communauté ou d'une communauté de référence. Cela garantit que seuls les utilisateurs autorisés du DEP peuvent débloquer des contenus provenant de ces archives. En particulier, seul l'utilisateur technique est désormais autorisé à mettre à disposition des DICOM Key Object Selection (KOS). On empêche ainsi que des patients ou des professionnels de la santé ne déposent dans le dossier des objets KOS manipulés pour avoir un accès non autorisé aux études d'autres patients.

Enfin, de multiples adaptations de moindre envergure ont été apportées au texte, par exemple pour supprimer les complexités inutiles du système ou permettre une meilleure gestion des erreurs. Le tableau de concordance ci-dessous donne un aperçu de la nouvelle structure du complément 2.1 à l'annexe 5.

Sections et sous-sections	Ch. dans l'édition 4	Correspondance dans l'édition 5
Introduction	1	1
Definitions of terms	1.1	-
EPR circle of trust	1.1.1	-
Patient Identifiers (EPR-SPID, MPI-PID)	1.1.2	-
Terminology	1.1.3	-
Volume 1 - Integration Profiles	2	2
Overview	2.1	-
Authorization Decision Request (CH:ADR)	2.2	2.1
Motivation	2.2.1	-
Objectives and Constraints	2.2.2	-
Actors / Transactions	2.2.3	-
Privacy Policy Query (CH:PPQ)	2.3	2.2
Motivation	2.3.1	-
Objectives and Constraints	2.3.2	-
Actors / Transactions	2.3.3	-
Volume 2 - Transactions	3	3
Ancienne désignation : Authorization Decision Request (CH:ADR) *Nouvelle désignation :* Authorization Decision Request [CH:ADR]	3.1	3.1
Scope	3.1.1	3.1.1
Referenced Standards	3.1.2	3.1.2
Nouveau chiffre : XML Namespaces	-	3.1.3
Interaction Diagram	3.1.3	3.1.4
Ancienne désignation : XACMLAuthzDecisionQuery Request *Nouvelle désignation :* CH:ADR Request	3.1.4	3.1.5
Trigger Events	3.1.5	
Message Semantics	3.1.6	-
Expected Actions	3.1.7	-
Ancienne désignation : XACMLAuthzDecision Response *Nouvelle désignation :* CH:ADR Response	3.1.8	3.1.6
Nouveau chiffre : Indirect decision queries	-	3.1.7
Trigger Events	3.1.9	-
Message Semantics	3.1.10	-
Expected Actions	3.1.11	-
Enforcement of XDS Retrieve Document Set transactions	3.1.12	-
Enforcement of XDS-I.b "Imaging Retrieve" transactions	3.1.13	-
Security Considerations	3.1.14	3.1.8
Authorization Decision Consumer Audit Message	3.1.15	-
Authorization Decision Provider Audit Message	3.1.16	-
Cross-Community Authorization Decision Request (CH:XADR)	3.2	-
Ancienne désignation : Privacy Policy Feed (PPQ-1) *Nouvelle désignation :* Privacy Policy Feed [PPQ-1]	3.3	3.2
Scope	3.3.1	3.2.1
Use Case Roles	3.3.2	-
Referenced Standards	3.3.3	3.2.2
Nouveau chiffre : XML Namespaces	-	3.2.3
Interaction Diagrams	3.3.4	3.2.4
Message Semantics	3.3.5	-
Ancienne désignation : EPR AddPolicyRequest and EPR UpdatePolicyRequest *Nouvelle désignation :* AddPolicyRequest and UpdatePolicyRequest	3.3.6	3.2.5
Ancienne désignation : EPR AddPolicyRequest Response and EPR UpdatePolicyRequest Response *Nouvelle désignation :* AddPolicyRequest Response and UpdatePolicyRequest Response	3.3.7	3.2.6

Sections et sous-sections	Ch. dans l'édition 4	Correspondance dans l'édition 5
Ancienne désignation : EPR DeletePolicyRequest *Nouvelle désignation :* DeletePolicyRequest	3.3.8	3.2.7
Ancienne désignation : EPR DeletePolicyRequest Response *Nouvelle désignation :* DeletePolicyRequest Response	3.3.9	3.2.8
Security Considerations	3.3.10	3.2.9
Ancienne désignation : Privacy Policy Retrieve (PPQ-2) *Nouvelle désignation :* Privacy Policy Retrieve [PPQ-2]	3.4	3.3
Scope	3.4.1	3.3.1
Use Case Roles	3.4.2	-
Referenced Standards	3.4.3	3.3.2
Nouveau chiffre : XML Namespaces	-	3.3.3
Interaction Diagrams	3.4.4	3.3.4
Ancienne désignation : XACMLPolicyQuery *Nouvelle désignation :* Policy Query Request	3.4.5	3.3.5
Ancienne désignation : XACMLPolicyQuery Response *Nouvelle désignation :* Policy Query Response	3.4.6	3.3.6
Security Considerations	3.4.7	3.3.7
Volume 3 - Content Profiles	4	4
XACML EPR Access Policies	4.1	-
EPR Access Policy Stack	4.2	-
Entry Policies for the Evaluation of Access Decisions	4.2.1	-
Access Constraints	4.3	-
Read and Write Access Rights Overview	4.4	-
Enforcement of EPR transactions	4.4.1	-
Read EPR	4.4.2	-
Write EPR	4.4.3	-
Detailed Privacy Policy Format definitions	4.4.4	-
Value-Sets	4.4.5	-
Nouvelle section : Submission Rules for Policies and Policy Sets	-	4.1
Nouveau chiffre : Base Policies and Base Policy Sets	-	4.1.1
Nouveau chiffre : Patient Bootstrap Policy Sets and Patient User Assignment Policy Sets	-	4.1.2
Figures	5	5
Tables	6	6
Listings	7	-

3.4.4 Complément 2.2 à l'annexe 5 : Profils d'intégration nationaux selon l'art. 5, al. 1, let. c, ODEP-DFI – Audit Trail Consumption (CH:ATC)

La norme Fast Healthcare Interoperability Resources (FHIR) prescrite pour le profil CH:ATC, utilisé pour les données historisées du portail destiné aux patients, passe de la version STU3 à la Release 4. Comme les prochains formats d'échange seront basés sur cette version 4 de la norme FHIR, conserver une ancienne version de la norme aurait rendu le système inutilement complexe et aurait obligé à assurer la maintenance de deux versions. Cette modification s'applique à l'ensemble du document.

Ch. 1.1 Definitions of terms

Le ch. 1.1 est abrogé car il est identique à la même section du complément 1 à l'annexe 5.

Ch. 3.1.4 Security Considerations

Dans la révision 2.1 du supplément au profil d'intégration IHE IUA, l'attribut « type de jeton » dans le HTTP Header « Authorization » a été modifié. Cette modification a été transposée au profil CH:ATC : dans le HTTP Header, le type de jeton « Bearer » remplace « IHE-SAML ». Elle permet de s'adapter aux normes internationales, sans pour autant modifier le niveau de sécurité.

Ch. 4.1 Audit Trail Consumption Event Types

La recherche de documents dans un DEP est enregistrée dans les données historisées techniques (ATNA), mais elle ne s'affiche pas dans les données historisées sur le portail destiné aux patients. Pour améliorer la traçabilité, la spécification a été adaptée afin que la recherche de documents soit également enregistrée dans les données historisées sur le portail destiné aux patients.

Les accès dans des situations d'urgence sans consultation de documents seront eux aussi clairement affichés dans les données historisées sur le portail destiné aux patients.

L'art. 9, al. 2, let. f, ODEP dispose que les communautés doivent informer les patients, à leur demande, lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé. Pour simplifier la traçabilité, les communautés souhaitent que ces événements soient également enregistrés dans les données historisées du portail destiné aux patients. Les spécifications techniques relatives à ce processus, accompagnées d'exemples, ont donc été rajoutées (nouveaux ch. 4.5 et 4.5.1).

Ch. 4.2 Document Audit Event Content Profile

Lors de la consultation ou du traitement de documents ou de leurs métadonnées, le journal ATC-Log indiquera leur titre en plus de leur identificateur, lequel est peu parlant.

Ch. 4.2.1 Example of a Document Audit Event: Document upload

Dans l'exemple d'entrée dans le journal ATC-Log présenté au ch. 4.2.1, le titre du document a été complété.

3.4.5 Complément 2.3 à l'annexe 5 : Profil d'intégration nationale selon l'art. 5, al. 1, let. c, ODEP-DFI – Community Portal Index (CH:CPI)

Ch. 1.1 Definitions of terms

Le ch. 1.1 est abrogé car il est identique à la même section du complément 1 à l'annexe 5.

Ch. 3.1.4.2 Message Semantics

Les fournisseurs de plateformes DEP demandent que toutes les informations nécessaires du profil CH:CPI puissent être lues afin qu'une communauté certifiée puisse se raccorder automatiquement à toutes les autres communautés certifiées dans le profil CH:CPI, par tous les points d'accès. La présente modification rajoute au modèle de données du CH:CPI l'élément *CH:ATC Patient Audit Consumer*, une information pertinente qui manquait jusqu'ici. Il ne sera donc plus nécessaire d'échanger des certificats pour cet élément hors de l'espace confidentiel, ce qui améliore la sécurité. La modification concerne également les ch. 3.1.5.2.3, 4.1.3.2 et 4.1.3.3.9, qui contiennent les spécifications techniques applicables. Pour le reste, des fautes d'orthographe sont corrigées.

Ch. 3.1.8 Security Considerations

La nouvelle version du document technique « IHE ITI Technical Framework » (cf. ch. 3.4.1) permet d'utiliser plusieurs versions de TLS pour la transaction Authenticate Node [ITI-19]. La modification précise qu'il faut utiliser au minimum la version 1.2 (STX: TLS 1.2 floor using BCP195 Option).

3.5 Annexe 8 : Critères techniques et organisationnels de certification applicables aux moyens d'identification et à leurs éditeurs (profil de protection pour moyens d'identification)

L'annexe 8 a été remaniée en deux étapes.

Dans un premier temps, l'annexe a été restructurée. Sans cette restructuration, les modifications et les compléments requis pour tenir compte des retours d'information de l'organisme de certification et des fournisseurs d'identité ainsi que pour rajouter le protocole OpenID Connect auraient été impossibles à apporter, ou seulement moyennant un travail excessif. Lors de cette première étape, l'annexe 8 n'a pas été modifiée sur le fond ; seules ses sections ont été restructurées, ce qui a permis de corriger des incohérences et des imprécisions.

La nouvelle version de l'annexe 8 est structurée ainsi :

1. Introduction
2. Exigences concernant le service aux utilisateurs (patients, professionnels de la santé et leurs auxiliaires)
3. Exigences concernant le fonctionnement opérationnel du fournisseur d'identité
4. Exigences techniques applicables à l'interface et aux protocoles

Toutes les modifications en vue de la restructuration comme de la correction d'incohérences et d'imprécisions ont été présentées et discutées au sein d'un groupe d'accompagnement temporaire (le groupe de travail Moyens d'identification, réunissant des représentants des communautés, des plateformes, de l'organisme de certification et des fournisseurs d'identité). Après évaluation, le groupe d'accompagnement a salué et soutenu cette restructuration. Le tableau de concordance ci-dessous donne une vue générale de la nouvelle structure de l'annexe 8 :

Section	Ch. dans l'édition 2.1	Correspondance dans l'édition 3
PP Reference	1	3
TOE Definition	1.2.1	3.1.1
Operational Environment	1.3	3.1.1
Physical Protection of the TOE	1.4	3.1.3
Assets	1.5	3.1.4
External Entities and Subjects	1.6	3.1.5
Conformance Claims	2	obsolet
Security Problem Definition	3	3.2
Assumptions	3.1	3.2.1
Organizational Security Policies	3.2	3.2.2
Threats	3.3	3.2.3
Security Objectives	4	3.3
Security Objectives for the TOE	4.1	3.3.1
Security Objectives for the operational environment	4.2	3.3.2
Security Objectives rationale	4.3	3.3.3
Countering the threats	4.3.2	3.3.3.1
Security Requirements	5	3.4
Overview	5.1	3.4.1
Security Functional Requirements for the TOE	5.2	3.4.2
Security Requirements rationale	5.3	3.4.3
Security Assurance Requirements Rationale	5.4	3.5
Appendix	6	5
Identity Proofing Requirements	**6.1**	**2.5**
Authentication Sequences (v2), SAML2.0 Binding (v3)	6.2	4.1
SAML Assertion Renewal	Tab. 12	4.1.1.2
Logout Sequence	6.2a	v.1.1.3
SAML Recommendations (v2), Protocol Requirements (v3)	6.3	4.1.2/.3
Open ID Connect	**n/a**	**4.2**
Protocol Requirements for Open ID Connect (v3)	**n/a**	**4.2.2**
WS Trust Recommendations	6.4	4.1.3.6, 4.1.3.7

Dans un deuxième temps, l'annexe 8 a été révisée pour préciser ou ajouter les spécifications suivantes :

1. Les exigences applicables aux certificats X.509 des systèmes Relying Party (c.-à-d. les portails et les systèmes primaires) pour l'authentification et le chiffrement sur la couche de transport TLS ont été mises en conformité avec les critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (annexe 2 ODEP-DFI).
2. Les exigences applicables aux certificats X.509 utilisés pour la signature numérique des messages échangés entre fournisseurs d'identité et Relying Parties (portails et systèmes primaires) ont été précisées.
3. Afin de permettre l'intégration de plusieurs Service Providers (p. ex. la page d'enregistrement de nouveaux membres de la communauté de référence ou le portail d'accès au DEP) dans une même communauté ou communauté de référence, l'utilisation des identificateurs NameID (*ch. 4.1.3.5*) et Subject Identifier (*ch. 4.2.3.5*) ont été autorisés pour les Services placés sous l'autorité de la communauté ou de la communauté de référence, dans la mesure où les Service Providers utilisés sont inscrits sur une liste.

Enfin, la révision a été mise à profit pour procéder à des corrections formelles en divers endroits (les renvois et les références à des sources ont été harmonisés et complétés si nécessaire).

3.6 Annexe 9 : Métadonnées pour le service de recherche des institutions de santé et des professionnels de la santé

Ch. 2.2 *Spécialisation des professionnels de la santé*

La rectification des majuscules et des minuscules au ch. 2.2 de l'annexe 3 ODEP-DFI a été répercutée dans le ch. 2.2 de l'annexe 9.

Annexes

- Projet de modification de l'ODEP-DFI (RS *816.111*)
- Projet d'annexe 2 à l'ODEP-DFI, édition 6
- Projet d'annexe 3 à l'ODEP-DFI, édition 5
- Projet d'annexe 4 à l'ODEP-DFI, édition 2
- Projet d'annexe 5, complément 1, à l'ODEP-DFI, édition 6
- Projet d'annexe 5, complément 2.1, à l'ODEP-DFI, édition 5
- Projet d'annexe 5, complément 2.2, à l'ODEP-DFI, édition 4
- Projet d'annexe 5, complément 2.3, à l'ODEP-DFI, édition 5
- Projet d'annexe 8 à l'ODEP-DFI, édition 3
- Projet d'annexe 9 à l'ODEP-DFI, édition 3
- Courrier d'accompagnement