Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Commentaires relatifs à

la révision de l'ordonnance du DFI du 24 juin 2019 sur le dossier électronique du patient (ODEP-DFI)

Modification des prescriptions concernant les métadonnées (art. 3), la collecte de données pour l'évaluation et la recherche (art. 6), les exigences minimales applicables au personnel des organismes de certification (art. 7) et les données à enregistrer dans le service de recherche des institutions de santé et des professionnels de la santé (art. 8*a*)

ainsi que

- **nouvelle version de**
  - l'annexe 2 – Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence
  - l'annexe 7 – Exigences minimales applicables à la qualification du personnel des organismes de certification
- **nouvelle version de**
  - l'annexe 3 – Métadonnées utilisées pour l'échange de données médicales
  - l'annexe 5 – Profils d'intégration
  - l'annexe 6 – Évaluation et recherche
- **nouvelle annexe 9 – Métadonnées utilisées pour le service de recherche des institutions de santé et des professionnels de la santé**

1 Situation initiale

La LDEP est entrée en vigueur le 15 avril 2017, suite à la décision du Conseil fédéral du 22 mars 2017.

2 Contexte des modifications

2.1 Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (annexe 2)

L'art. 30, al. 2, de l'ordonnance sur le dossier électronique du patient (ODEP, RS *816.11*) délègue au DFI la compétence de définir les critères de certification dans la législation. L'annexe 2 de l'ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI, RS *816.111*) règle les critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence. Dans le cadre du processus de certification, il incombe aux organismes de certification accrédités d'attester que les communautés ou communautés de référence concernées remplissent ces critères.

Les adaptations prévues dans la présente révision de l'annexe 2 de l'ODEP-DFI concernent deux domaines essentiels des critères techniques et organisationnels de la certification : d'une part, la protection et la sécurité des données, domaine dans lequel les exigences sont concrétisées et précisées (ch. 4 de l'annexe 2 de l'ODEP-DFI) et, d'autre part, l'interopérabilité technico-sémantique, où il s'agit de reprendre des prescriptions modifiées dans l'annexe 5 de l'ODEP-DFI et dans spécifications techniques définies dans les suppléments à cette dernière (cf. ch. 2.3 des commentaires).

Les adaptations proposées dans le domaine de la protection et de la sécurité des données visent principalement à compléter et à préciser les exigences compte tenu de l'expérience acquise à ce jour avec l'accréditation d'organes de certification. Les prescriptions générales et abstraites ont en effet conduit à des interprétations divergentes selon les organismes de certification ainsi que selon les communautés et les communautés de référence concernées. Les modifications doivent assurer un niveau de confiance uniforme et suffisamment élevé pour l'exploitation du DEP.

D'autres révisions ponctuelles sont nécessaires, car certains contenus ou certaines prescriptions référençables n'étaient pas encore disponibles au moment de l'entrée en vigueur de la LDEP et des ordonnances d'application afférentes. Ainsi, la marque de certification obligatoire est désormais intégrée et certains standards pour l'échange de données avec la Centrale de compensation (CdC) ont une référence normative puisqu'elles ont entre-temps été approuvées par l'association eCH.

2.2 Métadonnées utilisées pour l'échange de données médicales (art. 3 et annexe 3)

L'annexe 3 ne mentionne plus que les métadonnées nécessaires pour l'échange de données médicales, car les attributs qui doivent être utilisés pour désigner les institutions de santé et les professionnels de la santé dans le service de recherche des institutions de santé et des professionnels de la santé sont désormais définis à l'annexe 9 (cf. ch. 2.6 des commentaires).

2.3 Profils d'intégration (annexe 5)

Les profils d'intégration sont des lignes directrices permettant d'assurer l'interopérabilité technique et sémantique de cas spécifiques d'application, le plus souvent sur la base de normes et de standards reconnus. Ils définissent les acteurs[1] qui interagissent, ainsi que les transactions devant être respectées pour cette interaction et la communication.

Depuis l'entrée en vigueur de la LDEP, le 15 avril 2017, les profils d'intégration internationaux IHE utilisés pour le DEP ont évolué. *IHE International*, l'organisation responsable au niveau international, a adapté les prescriptions ainsi que les standards sous-jacents à l'état de la technique. À des fins d'harmonisation avec les profils d'intégration internationaux, le DFI actualise les versions des profils d'intégration internationaux IHE devant être utilisées pour le DEP (art. 5, al. 1, let. a) ainsi que les adaptations nationales afférentes (art. 5, al. 1, let. b, et annexe 5, ch. 1). En ce qui concerne les profils d'intégration nationaux spécialement conçus pour le DEP (art. 5, al. 1, let. c), des compléments, des précisions et des corrections ont été apportés suite aux expériences faites lors des premiers tests de mise en œuvre (annexe 5, ch. 2).

2.4 Évaluation et recherche (art. 6 et annexe 6)

Conformément à l'art. 22, al. 1, ODEP, les communautés et les communautés de référence sont tenues de mettre régulièrement à la disposition de l'OFSP des données pseudonymisées ou anononymisées en vue de l'évaluation visée à l'art. 18 LDEP. Conformément à l'art. 22, al. 2, ODEP, le DFI fixe les données à fournir et les délais.

En 2016, soit un an avant l'entrée en vigueur de la LDEP, un modèle d'effets couvrant l'essentiel des objectifs de la LDEP ainsi que les principaux effets attendus a été conçu en collaboration avec un groupe d'accompagnement réunissant les acteurs clés. Un concept de monitorage a ensuite été formulé sur la base de ce modèle et les indicateurs y relatifs ont été définis[2]. Après l'entrée en vigueur de la LDEP le 15 avril 2017, un concept de mise en œuvre du monitorage a été élaboré avec pour but d'opérationnaliser avec précision les indicateurs définis. Compte tenu de ce concept de mise en œuvre, le DFI adapte l'art. 6 ODEP-DFI et fixe désormais à l'annexe 6 quelles données doivent être fournies.

2.5 Exigences minimales applicables à la qualification du personnel des organismes de certification (art. 7 et annexe 7)

Conformément à l'art. 28, al. 5, ODEP, le DFI fixe les exigences minimales applicables à la qualification du personnel des organismes de certification. Les normes ISO référencées figurant à l'annexe 7 de l'ODEP-DFI du 22 mars 2017 ne sont plus actuelles et doivent par conséquent être remplacées par les versions mises à jour.

2.6 Service de recherche des institutions de santé et des professionnels de la santé (art. 8*a* et annexe 9)

Conformément à l'art. 41, al. 2, ODEP, le DFI est habilité à définir des données que les communautés et les communautés de référence doivent enregistrer dans le service de recherche des institutions de santé et des professionnels de la santé en plus de celles mentionnées à l'art. 41, al. 1, ODEP. Étant donné que les numéros d'identification selon l'art. 3, al. 2, let. c, de l'ordonnance du 30 juin 1993 sur le registre des entreprises et des établissements[3] (numéro REE) sont attribués uniquement à des institutions de santé - les groupes de professionnels de la santé en étant exclus - le Conseil fédéral a décidé

[1] Les acteurs ou acteurs IHE sont des unités fonctionnelles abstraites de systèmes d'information ou des composants de tels systèmes, qui produisent des informations et les échangent ou les gèrent au moyen de transactions.
[2] Pour plus d'informations, voir sous : https://www.bag.admin.ch/bag/fr/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/monitoring.html
[3] RS *431.903*

le 8 mars 2019 qu'il appartient au DFI et non à lui-même de fixer les exigences précises relatives à l'enregistrement de ces données. L'art. 41, al. 1, let. a, ch. 3, ODEP a par conséquent été supprimé. La présente révision de l'ODEP-DFI précise les prescriptions qui s'appliquent à l'enregistrement des données relatives aux institutions de santé.

À l'annexe 9 de l'ODEP-DFI, le DFI définit en outre les métadonnées qui doivent être utilisées pour désigner les institutions de santé et les professionnels de la santé dans le service de recherche.

3 Commentaires des modifications

3.1 Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (annexe 2)

Ch. 1.4 Identification et authentification

Le ch. 1.4.4 est complété pour des raisons de sécurité des données : comme condition à l'obtention de la certification, il est explicitement exigé des communautés qu'elles vérifient que les identificateurs univoques soient associés aux bons patients. Il convient notamment de surveiller les processus de gestion des identificateurs au cours du temps. En effet, les identificateurs peuvent être modifiés, par exemple, en cas de renouvellement ou de blocage des moyens d'identification (cf. art. 26 et 27 ODEP). Il convient alors de veiller à ce que l'attribution du nouvel identificateur se fasse correctement et sans incident.

Ch. 2.5 Enregistrement et transfert cryptés des données

Le ch. 2.5 renvoie désormais explicitement aux exigences relatives à la gestion des clés cryptographiques énoncées au ch. 4.12.

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

Le ch. 2.9.1 mentionne désormais explicitement les normes d'interface à utiliser pour communiquer avec la base de données d'identification (UPI) de la CdC. Lors de l'entrée en vigueur de la LDEP, ces normes n'étaient pas encore approuvées par l'association eCH.

Le ch. 2.9.2 est complété de manière à exiger des communautés, outre le respect des prescriptions inscrites dans le règlement de traitement de la CdC, la mise en œuvre de mesures permettant d'éviter que les données enregistrées dans la base de données UPI de la CdC soient modifiées de façon illicite ou par erreur. La mention explicite de cette exigence est nécessaire, car la CdC ne sait pas à quelles communautés les différents numéros d'identification des patients appartiennent. Elle ne possède donc pas de moyens techniques suffisants pour empêcher que des communautés de référence effectuent des mutations de données de patients sans y être autorisées. Le règlement de traitement définit en particulier que, par dérogation à la norme d'interface eCH-0215, l'interface technique *Broadcast Mutations* proposée par la CdC aux communautés et aux communautés de référence ne transmettra pas d'informations relatives à des données démographiques modifiées par broadcast, mais uniquement des informations concernant les numéros d'identification de patients modifiés ou annulés.

Ch. 2.9.4 à 2.9.30 Profils d'intégration IHE, adaptations nationales aux profils d'intégration IHE et profils d'intégration nationaux

Les modifications apportées aux ch. 2.9.4 à 2.9.30 sont des adaptations aux exigences techniques corrigées et actualisées dans l'annexe 5 de l'ODEP-DFI et dans les suppléments à cette dernière concernant les prescriptions en matière de communication interne aux communautés et de communication intercommunautaire (cf. commentaires y relatifs au ch. 3.3.).

On notera en particulier les nouveaux ch. 2.9.7*a*, 2.9.11*a* et 2.9.25*a*.

Conformément au *ch. 2.9.7a*, les attributs relatifs aux autorisations allégués par certains acteurs IHE (les « *X-Service User* », généralement matérialisés par des portails d'accès ou des systèmes primaires intégrés), comme par exemple, « professionnel de la santé avec GLN 7601234567890 », « adjoint de X », « assistant de Y » doivent être vérifiés par un autre acteur IHE (*X-Service Provider*) par comparaison avec des sources de données fiables (p. ex., registre des assistants et registre des professionnels de la santé responsables de ceux-ci). Cette mesure de sécurité supplémentaire se justifie du fait que les systèmes primaires décentralisés, en particulier, ne doivent pas satisfaire aux mêmes exigences en matière de sécurité et de qualité des données que les éléments de l'infrastructure informatique d'une communauté ou d'une communauté de référence et que l'on ne peut par conséquent pas entièrement se fier à leurs allégations. Les attributs relatifs aux autorisations allégués par les portails d'accès particulièrement bien protégés et gérés de manière centralisée par des communautés ou des communautés de référence peuvent, à certaines conditions et avec l'accord du responsable de la protection et de la sécurité des données, être exemptés de l'obligation d'être vérifiés par l'acteur *X-Service Provider*. Une telle dérogation est justifiée notamment lorsque le portail d'accès en question est lui-même une source de données fiable – voire la seule – utilisable pour vérifier les allégations (cf. commentaires y relatifs au ch. 3.1*b*).

Le *ch. 2.9.11a* renvoie aux nouvelles prescriptions relatives à l'authentification des utilisateurs techniques, c.-à-d. les processus automatisés qui, sur mandat de personnes physiques, peuvent mettre des données à disposition dans le DEP. Il s'agit en l'occurrence de l'exécution différée d'actions autorisées par des personnes physiques.
Le *ch. 2.9.25a* comporte désormais des exigences génériques et abstraites relatives à la sécurisation de la configuration des autorisations par le profil d'intégration national CH:PPQ. Les fabricants des systèmes de gestion des autorisations doivent prendre des mesures techniques appropriées pour empêcher tout traitement illicite de la configuration des autorisations. À cet effet, ils doivent garantir que :

a. les systèmes traitants sont autorisés à effectuer de telles opérations ;
b. ces opérations ne sont possibles que sur les configurations d'autorisation pour lesquelles la personne authentifiée (c.-à-d. « connectée » au système) dispose de l'autorisation (c.-à-d. le patient, son représentant ou le professionnel de la santé habilité à cet effet) ;
c. le traitement de la configuration d'autorisation ne se traduit pas par des modifications non spécifiées ou contraires aux règles.

Ch. 2.10 Données historisées
Par mesure de simplification, la disposition du ch. 2.10.5 exige désormais que seuls les critères définis soient historisés. Les résultats de la recherche ne doivent en revanche plus être historisés, car cela implique des coûts d'implémentation excessifs compte tenu des normes, standards et profils d'intégration disponibles.

Le ch. 2.10.9 renvoie au profil d'intégration national *Audit Trail Consumption (CH:ATC)* qui est désormais déterminant pour la présentation des données historisées (cf. ch. 3.3.3 des commentaires).

Le ch. 2.10.10 est complété afin de tenir compte des nouvelles prescriptions relatives à l'évaluation selon l'annexe 6 de l'ODEP-DFI.

Ch. 3.1 Présentation [du portail d'accès pour les professionnels de la santé]
Le *ch 3.1.2* doit être complété, car on a constaté que des objets de données autres que les documents et les métadonnées de documents – qui sont soumis à la gestion des autorisations – peuvent être transmis et représentés sans les droits d'accès correspondants. Par conséquent, la nouvelle disposition stipule que les données et les métadonnées ne peuvent être représentées qu'à condition que la personne qui les consulte dispose des droits correspondants.

Le *ch. 3.1a* prescrit la présence d'une marque de certification sur le portail d'accès au DEP et règle son utilisation. Il est probable qu'à l'avenir, les communautés certifiées étendent leurs activités numériques à des fonctions et des services autres que le DEP. Il importe par conséquent que le portail d'accès des communautés et des communautés de référence montre clairement aux professionnels de la santé quels secteurs sont soumis à la LDEP ; ces secteurs doivent se différencier visuellement de ceux qui ne sont pas soumis à cette législation.

Le *ch. 3.1a.1* vise à établir une distinction claire entre le secteur du DEP et les autres services. Seul l'accès direct au DEP peut porter la marque de certification (cf. illustration).

La marque de certification existe en deux versions de formats différents. Les communautés certifiées décident elles-mêmes de la manière de les utiliser dans leur communication. Les deux versions portent une URL qui identifie la communauté de manière univoque et renvoie à sa page sur le site www.dossierpatient.ch.
Le *ch. 3.1b* est complété afin de tenir compte du degré de fiabilité plus élevé exigé des portails d'accès des communautés et des communautés de référence par rapport aux systèmes primaires.

Ch. 3.4 Exigences techniques
Les nouvelles dispositions énoncées aux *ch. 3.4.1 et 3.4.2* tiennent compte des exigences plus élevées en matière de sécurité auxquelles doivent répondre les portails d'accès internet. Outre les exigences s'appliquant de manière générale à la protection et à la sécurité des données, conformément aux ch. 4 de l'annexe 2 de l'ODEP-DFI, les dispositions du présent chiffre énoncent des prescriptions élargies, plus spécifiques et plus concrètes concernant, d'une part, la gestion des vulnérabilités en matière de sécurité, de surveillance, de détection et d'alerte lors d'incidents liés à la sécurité et, d'autre part, la protection contre diverses formes d'attaques et de compromissions.

Après chaque modification des ressources informatiques du portail d'accès (c.-à-d. les logiciels, le matériel, l'infrastructure du réseau, les bases de données, etc.) pouvant avoir des effets sur la sécurité, il y a lieu de prévoir une vérification active des vulnérabilités de sécurité au moyen de tests d'intrusion. De plus, des procédures automatiques de surveillance, de détection et d'alerte des responsables doivent garantir que les incidents de sécurité relatifs à des portails d'accès soient détectés rapidement (cf. *ch. 4.3*).

Un système de gestion des failles de sécurité (cf. *ch. 4.4*) doit quant à lui être activé de manière systématique et régulière de manière à ce que les failles de sécurité reconnues soient traitées conformément au risque encouru et avec la priorité requise pour réduire au minimum la fenêtre temporelle durant laquelle elles peuvent être exploitées.

Le *ch. 3.4.2* exige des mesures de protection contre les types connus d'attaques et de compromissions des catégories suivantes :
- attaques sur la gestion des sessions (p. ex., fixation de session, détournement de session, manipulation de jetons, attaques de réinsertion),
- attaques par injection,
- attaques de redirection,
- attaques de clickjacking,
- attaques de type cross site scripting,
- attaques *Cross Site Request Forgeries,*
- attaques de type SOAP Flooding,
- attaques de type Identity Service Spoofing.

Le *ch. 3.4.3* stipule désormais explicitement que les interactions avec les éditeurs de moyens d'authentification doivent se conformer aux dispositions de l'annexe 8 de l'ODEP-DFI.

Ch. 4 Protection et sécurité des données

Les modifications apportées ch. 4 sont essentiellement des adaptations en vue de préciser ou de concrétiser des dispositions existantes ou d'harmoniser la terminologie avec celle des normes ISO sous-jacentes. Certains chiffres ont ainsi été révisés ou complétés avec de nouvelles dispositions afin de répondre tant aux exigences accrues liées à l'importance et à la criticité de la protection et de la sécurité des données dans le cadre du DEP qu'aux enjeux devenus manifestes du contrôle du respect de ces exigences.

Au plan matériel, le *ch. 4.2.1* prévoit notamment de nouvelles dispositions visant à assurer le développement continu des systèmes de gestion de la protection et de la sécurité des données selon des principes analogues à ceux prévus par les normes pertinentes dans ce domaine (p. ex., ISO DIN EN ISO/IEC 27001:2017-06). Elles sont nécessaires dans la mesure où les communautés et les communautés de référence appliquent une procédure de vérification basée sur les risques et que les résultats et les preuves ainsi obtenus ne reflètent qu'une situation instantanée. Il est par conséquent d'autant plus important que les communautés et les communautés de référence adoptent des systèmes de protection des données et de gestion de la sécurité qui apprennent et s'adaptent aux risques.

Par ailleurs, les effets de la réglementation pour les institutions de santé et les professionnels de la santé (p.ex., *ch. 4.2.2 et 4.7.1, p. ex.)* ainsi que pour les tiers (*ch. 4.9*) sont formulés de manière plus explicite et plus claire.

Le *ch. 4.4.3* exige le « durcissement » habituel des systèmes, c.-à-d. la réduction de la surface d'exposition des moyens informatiques par la désactivation des modules de logiciels, fonctions, services et interfaces qui ne sont pas utilisés. La compromission des systèmes ou des services internet via des fichiers ou des messages XML nuisibles constitue un risque particulier. La *let. c* exige par conséquent de nouvelles mesures en vue de protéger les moyens informatiques contre les attaques et les compromissions typiques, notamment les :

- attaques sur des systèmes d'analyse XML,
- schémas XML malveillants/empoisonnement des schémas,
- attaques XML External Entity,
- services web - attaques de l'homme du milieu,
- attaques d' encapsulation de signature XML,
- attaques par injection XML input/code,
- attaques par injection XML Content,
- attaques de traversement des répertoires.

Le *ch. 4.5.1* précise les prescriptions relatives à la protection contre les logiciels malveillants et énonce de nouvelles exigences en vue de l'exécution et de la vérification régulières des mesures afférentes.

Au *ch. 4.6.2*, l'« inventaire de l'infrastructure informatique » est complété compte tenu notamment des modifications intervenues dans les profils d'intégration et dans les acteurs IHE impliqués.

Le *ch. 4.8.4* introduit des fonctions spécifiques (au sens de « rôles ») qui se sont avérées nécessaires pour l'administration du DEP et des documents enregistrés, et édicte les prescriptions relatives à leur gestion. Il s'agit principalement de rôles techniques indispensables pour certains cas d'application (p. ex. ouverture ou suppression d'un DEP, suppression ou correction de données par des tiers). Pour l'ouverture d'un DEP, par exemple, le système doit prévoir un rôle spécifique capable de générer une configuration d'autorisation initiale, avant même que des autorisations existent (puisqu'elles doivent justement être définies).

La deuxième fonction administrative spécifique visée par le présent chiffre concerne le traitement de documents par des tiers, c.-à-d. des exécutants autres que les patients ou les professionnels de la santé. Il s'agit notamment de la suppression de documents introduits de manière incorrecte dans le DEP ou de la suppression de documents sur mandat du patient ou après une révocation, cas dans lesquels les patients ne peuvent ou ne veulent pas agir par eux-mêmes.

Ch. 4.13 Sécurité d'exploitation
La *let. k* du *ch. 4.13.1* exige une séparation des tâches appropriée entre les personnes responsables d'activités et de processus particulièrement critiques. Certaines activités et certains processus devraient ainsi être soumis au principe du double contrôle afin de diminuer le risque qu'une personne seule puisse agir abusivement ou mettre le système en danger (la gestion des clés cryptographiques, p. ex., ne devrait pas être confiée aux personnes qui disposent d'un droit d'accès aux données protégées au moyen de ces dernières).

Ziff. 4.14. Anschaffung, Entwicklung und Instandhaltung von Systemen
Ziffer 4.14.2 wird um zusätzliche Bestimmungen zur Qualitätssicherung im Rahmen der Software-Entwicklung ergänzt, indem explizitere Vorgaben zur Testplanung, -durchführung und -dokumentation gemacht werden.

Ch. 4.16 Expiration des sessions dans le réseau
Le ch. 4.16.3 introduit des dispositions supplémentaires visant à une gestion sûre des sessions dans le réseau (*session management*). Cette gestion est une des conditions pour la sécurité de l'authentification et de l'autorisation des systèmes et des utilisateurs et elle doit par conséquent être protégée de manière appropriée contre les vecteurs d'attaque spécifiques.

Ch. 9 Portail d'accès pour les patients
Comme les portails d'accès pour les professionnels de la santé, les portails d'accès pour les patients doivent satisfaire à certaines exigences (marque de certification, prescriptions techniques) ; des règles correspondantes ont été introduites ou adaptées (cf. commentaires des ch. 3.1 et 3.4).

3.2 Métadonnées (art. 3 et annexe 3)

Art. 3 Métadonnées utilisées pour l'échange de données médicales
L'art. 3 précise désormais que l'annexe 3 ne contient plus que les métadonnées utilisées pour l'échange de données médicales. Les métadonnées désignant les institutions de santé et les professionnels de la santé qui doivent être utilisées pour le service de recherche des institutions de santé et des professionnels de la santé sont désormais définies à l'annexe 9 (cf. commentaire au ch. 3.6).

Annexe 3 Métadonnées utilisées pour l'échange de données médicales
La nouvelle version de l'annexe 3 ne contient plus que les métadonnées qui doivent être utilisées pour les profils d'intégration visés à l'annexe 5 de l'ODEP-DFI, définissant l'échange de données médicales.

En outre, les plages de valeurs des attributs à utiliser ont été mises à jour conformément à l'état actuel des systèmes de codes internationaux sous-jacents.

3.3 Profils d'intégration (annexe 5)

L'annexe 5 de l'ODEP-DFI établit quels profils d'intégration doivent être utilisés dans le contexte du DEP. Le supplément 1 de cette annexe décrit les adaptations nationales des profils IHE standard. Le supplément 2 définit les profils d'intégration nationaux ; en raison de son volume toujours plus important, il a été scindé en plusieurs parties.

3.3.1 Supplément 1 à l'annexe 5 : adaptations nationales des profils d'intégration selon l'art. 5, al. 1, let. b, ODEP-DFI

Ch. 1.2 Requirements on XDS and XCA
Les adaptations nationales des profils d'intégration XDS et XCA servent à la mise à disposition, la recherche et la consultation de documents dans le contexte du DEP. Le ch. 1.2 énonce de nouvelles prescriptions relatives aux métadonnées de documents qui doivent être utilisées ainsi que des exigences techniques supplémentaires à respecter par les acteurs IHE en vue de l'application des prescriptions en matière de protection et de sécurité des données.

Ch. 1.3 Requirements on XDS-I.b

Les images et les données radiologiques étant très volumineuses, la manière d'y accéder et de les traiter dans le DEP diffère de celle des autres données médicales. En particulier, les données radiologiques ne sont pas mises à disposition en copie, mais référencées. Par conséquent, l'adaptation nationale du profil d'intégration XDS-I.b règle désormais la manière dont les données d'images radiologiques provenant d'archives doivent être référencées dans le DEP.

Ch. 1.4 Expected actions for receiving actors receiving unexpected parameters

Il s'agit d'une nouvelle disposition qui définit de manière uniforme pour tout l'espace de confiance du DEP comment les acteurs IHE doivent traiter les messages invalides.

Ch. 1.5 Requirements on ATNA

L'adaptation nationale du profil d'intégration ATNA définit des normes générales pour l'authentification d'éléments de réseaux et pour l'historisation des évènements liés au traitement et à la communication. Elle est utilisée en combinaison avec la plupart des autres acteurs IHE. Étant donné que la mise à disposition d'informations historisées en vue de leur reprise par les patients doit désormais, dans les cas complexes ou dépassant les limites d'un seul système, se faire conformément aux prescriptions du nouveau profil d'intégration national CH:ATC (cf. ch. 3.3.3), plusieurs dispositions du présent chiffre sont supprimées.

Ch. 1.6 Requirements on XUA for Authentication and User Assertion

L'adaptation nationale du profil d'intégration XUA sert à confirmer et à transmettre des identités attestées ainsi que des attributs relatifs aux autorisations allégués par des utilisateurs authentifiés dans l'espace de confiance du DEP (p. ex., informations concernant les identificateurs, les rôles ou les liens entre les sujets). Les adaptations nationales du profil d'intégration XUA sont revues de manière exhaustive à des fins de sécurité des données. Elles garantissent que les allégations de systèmes primaires et de portails d'accès concernant l'utilisateur DEP actif sont vérifiées par d'autres systèmes. En outre, des dispositions et des processus standard d'émission et de vérification de ces allégations sont complétés.

Ch. 1.7 Requirements on PIXv3 for Patient Identity Feed

Cette transaction de l'adaptation nationale du profil d'intégration PIXv3 est utilisée par les systèmes primaires et les portails d'accès pour enregistrer ou pour interroger les identificateurs locaux des patients dans le Master Patient Index (MPI) de la communauté ou de la communauté de référence. Pour des raisons de protection des données, le lien avec les parents, possible dans la norme internationale (IHE PIXv3), est supprimé des attributs transférés.

Ch. 1.8 Requirements on PIXv3 Profile for Patient Identifier Cross-reference Query

Cette transaction de l'adaptation nationale du profil d'intégration PIXv3 est utilisée par les systèmes primaires pour interroger les numéros d'identification des patients d'une communauté ou des patients enregistrés dans le Master Patient Index (MPI) de la communauté ou de la communauté de référence au moyen des identificateurs locaux. La modification précise les dispositions relatives à l'interrogation des numéros d'identification des patients.

Ch. 1.9 Requirements on PDQv3 Profile for Patient Demographics Query

L'utilisation du nom du père ou de la mère pour rechercher le DEP d'un patient n'est plus autorisée. Les prescriptions y relatives sont donc supprimées de l'adaptation nationale du profil d'intégration PDQv3.

Ch. 1.10 Requirements on XCPD Profile for Cross- Community Patient Discovery

L'adaptation nationale du profil d'intégration XCPD permet à un système primaire ou à un portail d'intégration d'utiliser le numéro d'identification national du patient pour résoudre le numéro d'identification du patient correspondant dans une autre communauté ou communauté de référence. Celui-ci permet ensuite de consulter les documents enregistrés dans l'autre communauté ou communauté de référence. Les dispositions relatives aux attributs transmis dans les messages conformément à l'adaptation nationale du profil d'intégration XCPD sont révisées et clarifiées. En outre, un autre mode d'interrogation est autorisé.

Ch. 1.11 Requirements on HPD Profile for Replication

L'adaptation nationale du profil d'intégration HPD précise les prescriptions concernant les attributs à implémenter dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP. En outre, les plages de valeurs pour les attributs (p. ex., désignation des institutions de santé et des professionnels de la santé) figurent désormais dans la nouvelle annexe 9 de l'ODEP-DFI.

Ch. 1.12 Requirements on XDS MU and RMU

Les adaptations nationales des profils d'intégration XDS MU et RMU offrent la possibilité d'actualiser les métadonnées de documents. Les nouvelles adaptations nationales prescrivent qui a le droit de modifier des données, et lesquelles.

3.3.2 Supplément 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)

Le profil d'intégration national CH:PPQ permet de définir et de configurer les droits d'accès et les options selon les art. 2 à 4 ODEP. Le profil d'intégration national CH:ADR est utilisé pour transmettre, analyser et exécuter les demandes d'accès.

Pour définir les droits d'accès des différents utilisateurs aux données du DEP, le profil d'intégration national CH:ADR utilise les identités attestées, communiquées au moyen du profil d'intégration IHE XUA, ainsi que les allégations pertinentes pour l'autorisation.

Les deux profils d'intégration nationaux CH:ADR et CH:PPQ sont révisés exhaustivement suite à la révision complète des adaptations nationales du profil d'intégration IHE XUA (cf. ch. 3.3.1).

3.3.3 Supplément 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)

Le profil d'intégration national CH:ATC a dû être révisé, car l'agrégation et l'évaluation des messages ATNA Audit n'ont pas permis de tirer les conclusions nécessaires pour déterminer ce qui s'est passé exactement dans le cadre du traitement des données dans le DEP (cf. ch. 3.3.1 des commentaires). Étant donné que l'agrégation des informations historisées pertinentes peut différer en fonction de l'architecture interne des systèmes propres aux communautés, le nouveau profil se limite à des prescriptions relatives aux contenus et à la transmission entre les points d'accès des différentes communautés ou communautés de référence. À cette fin, un type de message spécifique a été défini pour chaque évènement significatif. Les messages appelés par le patient via le portail d'accès sont interrogés et analysés en vue de l'affichage par toutes les communautés et communautés de référence.

3.3.4 Supplément 2.3 à l'annexe 5 : Profils d'intégration nationaux selon l'art. 5, al. 1, let. c, ODEP-DFI – Community Portal Index (CH:CPI)

Le profil d'intégration national CH:CPI doit désormais être utilisé pour interroger le service de recherche des institutions de santé et des professionnels de la santé.

3.4 Évaluation et recherche (art. 6 et annexe 6)

Art. 6 Évaluation et recherche

L'*art. 6, al. 1,* énonce que les données que les communautés et les communautés de référence doivent relever figurent à l'annexe 6 de l'ODEP-DFI.

L'*art. 6, al. 2,* habilite l'OFSP à demander périodiquement les données et à mettre à disposition les formulaires nécessaires à cet effet. Dans le cadre de l'application, l'OFSP procédera par étapes et en concertation avec les communautés et les communautés de référence pour organiser la collecte des données et en particulier leur classification. Il sera ainsi tenu compte de la complexité technique de la collecte et du soin à donner à l'utilisation des métadonnées visées à l'annexe 3 de l'ODEP-DFI.

Au mois d'octobre de chaque année, l'OFSP fournira aux communautés et aux communautés de référence les indications détaillées, valables pour l'année suivante, concernant volume et le format des données à relever ainsi que le jour de référence ; pour la première année d'exploitation, ces informations seront communiquées trois mois avant l'entrée en vigueur opérationnelle du DEP (c.-à-d. à la mi-janvier 2020). Le jour de référence sera probablement le 15 avril de chaque année. Par dérogation à cette règle, les indicateurs-clés « nombre de personnes possédant un DEP » (ch. 3.1 de l'annexe 6 de l'ODEP-DFI), « nombre de documents élaborés au moyen du DEP » (ch. 2.1 de l'annexe 6 de l'ODEP-DFI) et « nombre de consultations de documents mis à disposition » (ch. 2.4 de l'annexe 6 de l'ODEP-DFI) seront relevés tous les trimestres, soit la première fois probablement le 15 juillet 2020.

Annexe 6 Évaluation et recherche

Ch. 1 Critères généraux

Le *ch. 1.1* indique que les métadonnées visées à l'annexe 3 de l'ODEP-DFI doivent être utilisées pour la classification selon les critères du ch. 2. La classification permet une analyse précise des données. Ainsi, le nombre de documents élaborés (*ch. 1.2)* répertoriés selon le « type organisationnel de l'établissement de santé » indique si les documents ont été mis à disposition par un hôpital, un cabinet médical, une pharmacie ou une autre institution de santé affiliée à la communauté ou à la communauté de référence. Les métadonnées « classe de document » et « type de document » permettent en outre de répertorier les documents selon leur nature, c.-à-d. selon qu'il s'agit, par exemple, de notes de consultation, de résultats de tests diagnostiques ou d'un plan de soins. La métadonnée « rôle de l'auteur » indique si le document a été mis à disposition par un professionnel de la santé, un assistant ou par le patient lui-même.

Pour les indicateurs visés au ch. 3, il y a lieu d'utiliser, le cas échéant, les cinq classes d'âge (*ch. 1.2).* La répartition selon ces classes d'âge est usuelle dans la recherche et présente deux avantages : elle est suffisamment sommaire pour tenir dans un tableau, et suffisamment fine pour permettre une analyse adéquate des données.

Ch. 2 Données à collecter par les communautés

Le nombre de documents mis à dispositions dans le DEP est un indicateur important de l'utilisation effective de ce dernier (*ch. 2.1*). Le relevé du nombre de documents correspondant à un des formats d'échange définis à l'annexe 4 ODEP-DFI (*ch. 2.2*) permet d'évaluer le degré de normalisation sémantique de ces documents. Le relevé doit également montrer la répartition des documents en fonction des trois niveaux de confidentialité visés à l'art. 1 ODEP (*ch. 2.3*). Enfin, le nombre de consultations des documents doit permettre d'identifier à quelle fréquence ceux-ci sont utilisés comme source d'information par les professionnels de la santé ou par les patients (*ch. 2.4*).

Ch. 3 Données supplémentaires à collecter par les communautés de référence

Les données sur le nombre de patients possédant un DEP (*ch. 3.1*) permettent de mesurer sa diffusion. Cet indicateur doit aussi comprendre les personnes qui ont révoqué leur consentement à la tenue d'un DEP conformément à l'art. 21, al. 1, ODEP entre le jour de référence précédent et le jour du relevé (ch. 3.2). La classification selon les cantons (*ch. 3.1, let. a*) donne un aperçu de la répartition géographique des utilisateurs de DEP. La classification combinant l'âge et le sexe permet, par exemple, de déterminer dans quels groupes de patients les personnes possédant un DEP sont les plus ou les moins nombreux (*ch. 3.1, let. b*).

La manière dont les patients usent de la possibilité de gérer les droits d'accès est révélatrice de l'usage qu'ils font de leur droit à l'autodétermination en matière d'information. Différents indicateurs doivent montrer dans quelle mesure les personnes possédant un DEP utilisent les options de configuration prévues à l'art. 4 ODEP (*ch. 3.3, let. a à g* et *ch. 3.6*) ou, au contraire, ne les utilisent pas (*ch. 3.4*). L'indication de l'âge et du sexe permettent d'identifier plus précisément les préférences. Le relevé du nombre de professionnels la santé et de groupes de professionnels de la santé possédant des droits d'accès par DEP doit fournir des informations complémentaires (*ch. 3.5*).

3.5 Exigences minimales applicables à la qualification du personnel des organismes de certification (art. 7 et annexe 7)

Art. 7 Exigences minimales applicables au personnel

Le nouvel *al. 2* donne à l'OFSP la compétence d'adapter les exigences minimales applicables au personnel des organismes de certification aux normes en vigueur, notamment en cas de mise à jour des normes ISO correspondantes.

Annexe 7 Exigences minimales applicables à la qualification du personnel des organismes de certification

Les normes ISO mentionnées aux ch. 1.1.4, 1.1.5 ainsi que 2.14 et 2.1.5 de l'annexe 7 de l'ODEP-DFI du 22 mars 2017 ne sont plus actuelles et doivent par conséquent être remplacées par les versions mises à jour.

3.6 Service de recherche des institutions de santé et des professionnels de la santé (art. 8*a* et annexe 9)

Art. 8*a* Service de recherche des institutions de santé et des professionnels de la santé

Pour les institutions de santé, il convient d'enregistrer outre les données mentionnées à l'art. 41, al. 1, let. a, ODEP également le numéro d'identification visé à l'art. 3, al. 2, let. c, de l'ordonnance du 30 juin 1993 sur le registre des entreprises et des établissements[4] (numéro REE). Le complément apporté au présent article est rendu nécessaire par la suppression de l'art. 41, al. 1, let. a, ch. 3, ODEP.

L'annexe 9 définit quant à elle les métadonnées qui doivent être utilisées dans le service de recherche des institutions de santé et des professionnels de la santé pour désigner les institutions de santé et les professionnels de la santé (*al. 2*). Ces métadonnées servent à classer les institutions de santé et les professionnels de la santé selon leur type et leur spécialisation, de sorte à faciliter la recherche d'une institution ou d'un professionnel déterminés ou à permettre l'analyse des données enregistrées dans le service en fonction de ces catégories.

Annexes 9 Métadonnées utilisées pour le service de recherche des institutions de santé et des professionnels de la santé

Les institutions de santé et les professionnels de la santé doivent être désignés au moyen des métadonnées figurant dans l'annexe 9.

[4] RS *431.903*

3.7 Entrée en vigueur

Les modifications entrent en vigueur le 15 juillet 2019, afin qu'elles soient applicables dès l'automne 2019, lorsque les premières certifications de communautés et de communautés de références seront réalisées.