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

Contrôles du fonctionnement dans les environnements de production du DEP

Aide à la mise en œuvre pour les communautés (de référence)

Berne, le 22 novembre 2019

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

Informations supplémentaires et diffusion :

www.e-health-suisse.ch

But et positionnement du document

Les contrôles du fonctionnement dans les environnements de production du DEP améliorent la qualité de la production dans la mesure où des failles induites par des modifications du système sont détectées rapidement. La présente aide à la mise en œuvre décrit les instruments dont disposent les communautés (de référence) en la matière et règle la mise en application ainsi que l'utilisation de ces outils.

La présente aide à la mise en œuvre a été élaborée par Thomas Kessler, TEMET AG, sur mandat d'eHealth Suisse et avec la participation du groupe de travail temporaire « Contrôles du fonctionnement / assurance qualité dans les systèmes opérationnels du DEP ». Le rapport est disponible sur le site www.e-health-suisse.ch.

Pour faciliter la lecture du document, et sauf mention particulière, la forme générique est utilisée pour désigner les deux sexes.

Sommaire

Résumé 3
1 Introduction 4
1.1 Situation initiale 4
1.2 Problématique 4
1.3 Objectifs 5
1.4 Délimitation 5
1.5 Structure du document 6
2 Contrôles du fonctionnement à des fins d'assurance qualité 7
2.1 Approche intégrant différents niveaux de test 7
2.2 Expériences tirées des projets pilotes DEP 8
3 Contrôles du fonctionnement dans le DEP 9
3.1 Portée des contrôles du fonctionnement 9
3.2 Cas d'application 9
4 Conditions-cadres 15
5 Solution retenue 16
5.1 Dossiers électroniques du patient (DEP) fictifs 16
5.2 Auxiliaires avec tâches AQ 16
5.3 Distinction entre le contexte d'assurance qualité et le contexte de traitement 17
5.4 Mise en œuvre dans les composants DEP 17
6 Mesures d'exécution 20
6.1 Application de la présente aide à la mise en œuvre 20
6.2 Mesures d'accompagnement ou complémentaires 23

Résumé

Contexte et objectifs

Les communautés (de référence) doivent s'assurer que le fonctionnement et l'interopérabilité de leurs systèmes informatiques restent garantis lors de l'introduction de nouvelles versions ou de nouveaux composants techniques.

Les contrôles du fonctionnement dans les environnements de production du DEP (ou « contrôles post-déploiement ») visent à garantir la qualité de la production dans la mesure où des failles induites par des modifications du système sont détectées rapidement. Il s'agit en particulier de problèmes d'interopérabilité entre les différents protagonistes du système, qui résultent d'erreurs de configuration et qui ne peuvent pas être identifiés dans les environnements de test. Les contrôles du fonctionnement dans les environnements de production du DEP présupposent l'exécution de tests fonctionnels et de tests d'acceptation approfondis dans les différents environnements de test et ne sauraient aucunement s'y substituer.

Solution retenue

Pour procéder aux contrôles du fonctionnement dans les environnements de production du DEP, chaque communauté de référence ouvre deux dossiers électroniques du patient (DEP) fictifs. Les titulaires de ces DEP fictifs sont des personnes fictives instituées par la CdC (Centrale de compensation de la Confédération) dans le service de production UPI et auxquelles est attribué un EPR-SPID réel. Les DEP fictifs contiennent exclusivement des documents fictifs avec des contenus fictifs sans lien avec un traitement médical ou avec des personnes réelles.

Les contrôles du fonctionnement sont effectués par des « auxiliaires avec tâches AQ ». Ces derniers ne se différencient pas des autres auxiliaires, si ce n'est qu'ils utilisent le système de production du DEP dans un contexte d'assurance qualité (AQ) et non dans un contexte de traitement. Les personnes fictives n'obtiennent pas d'identité électronique et ne peuvent pas accéder au portail des patients. C'est pourquoi les contrôles du fonctionnement des services destinés aux patients sont également effectués par les auxiliaires avec tâches AQ en leur qualité de représentant dans le DEP.

Les auxiliaires avec tâches AQ sont subordonnés à un professionnel de la santé qui est responsable de l'exécution en bonne et due forme des contrôles du fonctionnement. Ce « professionnel de la santé avec responsabilité AQ » est autorisé à accéder au DEP fictif par un représentant du patient fictif dans le DEP.

Ensemble de règles pour les contrôles du fonctionnement

Chaque communauté de référence définit un ensemble de règles pour l'exécution des contrôles du fonctionnement et nomme un auxiliaire avec tâches AQ, qui est responsable des deux DEP fictifs de la communauté de référence. Cet auxiliaire tient notamment une liste contenant tous les auxiliaires avec tâches AQ et tous les professionnels de la santé avec responsabilité AQ au sein de la communauté (de référence).

Mesures complémentaires

Les outils permettant un monitoring automatisé et une analyse efficace des erreurs peuvent également contribuer à un niveau élevé de la qualité de l'exploitation, mais ils ne font pas l'objet du présent document.

1 Introduction

1.1 Situation initiale

Niveaux de test

Les communautés (de référence) DEP utilisent une infrastructure complexe dotée de systèmes informatiques de différents exploitants qui sont interconnectés. Elles doivent s'assurer que le fonctionnement et l'interopérabilité de tous les composants restent garantis lors de l'introduction de nouvelles versions ou de nouveaux composants techniques. C'est pourquoi, parallèlement aux environnements de développement des différents exploitants, les communautés disposent d'environnements de test et d'intégration, qui leur permettent de procéder à des tests d'acceptation et d'interopérabilité entre l'ensemble des composants.

Configurations spécifiques à l'environnement

Même si le logiciel est repris tel quel de l'environnement d'intégration vers l'environnement de production, il est impossible d'éviter totalement les différences au niveau de la configuration de ces environnements. Les adresses IP, les URL, les certificats, les règles de pare-feu et d'autres paramètres de configuration doivent être différents et ne peuvent donc pas être validés de manière définitive dans l'environnement d'intégration.

Réduire les risques liés aux erreurs de configuration

À chaque introduction d'une nouvelle version dans l'environnement de production, le risque existe donc que l'ensemble du système ne fonctionne plus (correctement) en raison d'une erreur de configuration. Ces erreurs peuvent survenir non seulement dans les composants modifiés, mais aussi dans ceux devant être adaptés à la suite d'une modification. Les communautés (de référence) peuvent réduire ce risque en exécutant, directement après chaque modification de l'environnement de production du DEP, un contrôle du fonctionnement (ou « contrôle post-déploiement ») et identifier ainsi rapidement d'éventuels problèmes.

1.2 Problématique

Les contrôles du fonctionnement ne sont pas prévus par la LDEP

Le droit d'exécution de la loi fédérale sur le dossier électronique du patient (LDEP) ne prévoit aucun contrôle du fonctionnement dans les environnements de production du DEP. Les patients, les professionnels de la santé ou les auxiliaires sont donc les premiers à se rendre compte d'éventuelles erreurs dues à l'introduction de nouvelles versions, ce qui risque de diminuer l'acceptabilité du DEP et de retarder la résolution du problème. Des lacunes ou des défaillances dans le fonctionnement d'un environnement de production du DEP peuvent également mettre en danger

la sécurité des patients, ce qui doit être évité par tous les moyens disponibles.

1.3 Objectifs

Assurance qualité (AQ) par le personnel administratif

Les contrôles du fonctionnement dans les environnements de production du DEP doivent assurer la qualité de la production dans la mesure où des failles induites par des modifications du système sont détectées rapidement.

Les contrôles du fonctionnement doivent pouvoir être effectués par le personnel administratif sans que les patients ou les professionnels de la santé et les auxiliaires intervenant dans les traitements au quotidien ne soient impliqués. Les professionnels de la santé ainsi que les auxiliaires doivent assurer les traitements au quotidien et, en l'absence d'un contexte de traitement spécifique, n'ont pas le droit d'accéder à un DEP. Quant aux patients, ils ne sont en mesure de procéder à des contrôles du fonctionnement que de manière limitée car ils ne disposent pas des connaissances (techniques) approfondies.

Approche uniforme à l'échelle nationale

Une approche uniforme à l'échelle nationale pour l'exécution des contrôles du fonctionnement dans les environnements de production du DEP doit permettre de garantir le bon fonctionnement des systèmes de production du DEP et, si possible, l'exécution de contrôles du fonctionnement pour différentes communautés.

Grâce à cette approche uniforme à l'échelle nationale, il est possible de mettre en œuvre de manière centralisée des éléments importants de la solution, comme par exemple l'attribution d'un numéro d'identification du patient (EPR-SPID) par la Centrale de compensation (CdC) à un nombre limité de personnes fictives.

Contrôles effectués comme prévu

Les contrôles du fonctionnement ont lieu dans tous les cas. Seule se pose la question de savoir s'ils sont effectués, comme prévu, par le personnel administratif ou, de manière spontanée, par les utilisateurs. La standardisation des contrôles du fonctionnement peut empêcher des solutions non abouties et improvisées, difficiles à contrôler et susceptibles d'engendrer des effets indésirables.

1.4 Délimitation

Toutes les phases de test nécessaires

Les contrôles du fonctionnement dans les environnements de production du DEP présupposent l'exécution de tests fonctionnels et d'acceptation approfondis dans les différents environnements de test et ne sauraient aucunement s'y substituer.

Autres éléments liés à l'assurance qualité

Pour assurer une qualité élevée de l'exploitation, les mesures suivantes sont également nécessaires, mais ne font pas l'objet du présent document :

- Surveillance continue de l'exploitation ;
- Analyse des erreurs dans l'exploitation courante ;
- Support aux patients ;
- Support aux professionnels de la santé et aux auxiliaires.

Différentes aspect et outils concernant les contrôles du fonctionnement peuvent également être pertinents pour ces cas d'application, mais leur mise en œuvre concrète ne relève pas du présent document.

1.5 Structure du document

Différents niveaux de test

Le chapitre 2 porte sur les contrôles du fonctionnement à des fins d'assurance qualité dans le cadre de l'approche intégrant différents niveaux de test et résume les expériences tirées des projets pilotes relatifs au DEP MonDossierMédical et myEPD.

Cas d'application (*use cases*)

Le chapitre 3 identifie et décrit les cas d'application des contrôles du fonctionnement : quelles fonctions sont contrôlées par qui et quels problèmes d'interopérabilité classiques peuvent être identifiés ?

Conditions-cadres

Le chapitre 4 porte sur les conditions-cadres pour les protagonistes du système dont il faut tenir compte dans la solution.

Outils à disposition

Le chapitre 5 décrit la solution retenue en vue des futurs contrôles du fonctionnement dans les environnements de production du DEP. Il identifie les outils à la disposition des communautés (de référence) et esquisse leur mise en œuvre dans les composants du DEP.

Mesures

Le chapitre 6 identifie les différents axes pour la mise en œuvre et propose des mesures d'accompagnement complémentaires pour continuer à améliorer la qualité de l'exploitation.

2 Contrôles du fonctionnement à des fins d'assurance qualité

2.1 Approche intégrant différents niveaux de test

Les contrôles du fonctionnement dans les environnements de production du DEP présupposent l'exécution de tests fonctionnels et de tests d'acceptation approfondis dans les différents environnements de test et ne sauraient aucunement s'y substituer.

Les contrôles du fonctionnement ne remplacent pas les tests

L'Illustration 1 montre les niveaux de tests classiques d'une plateforme DEP avec les volumes de données, les composants du système et les configurations (en bleu) ainsi que les mesures importantes concernant l'assurance qualité pour le niveau concerné (en vert) :

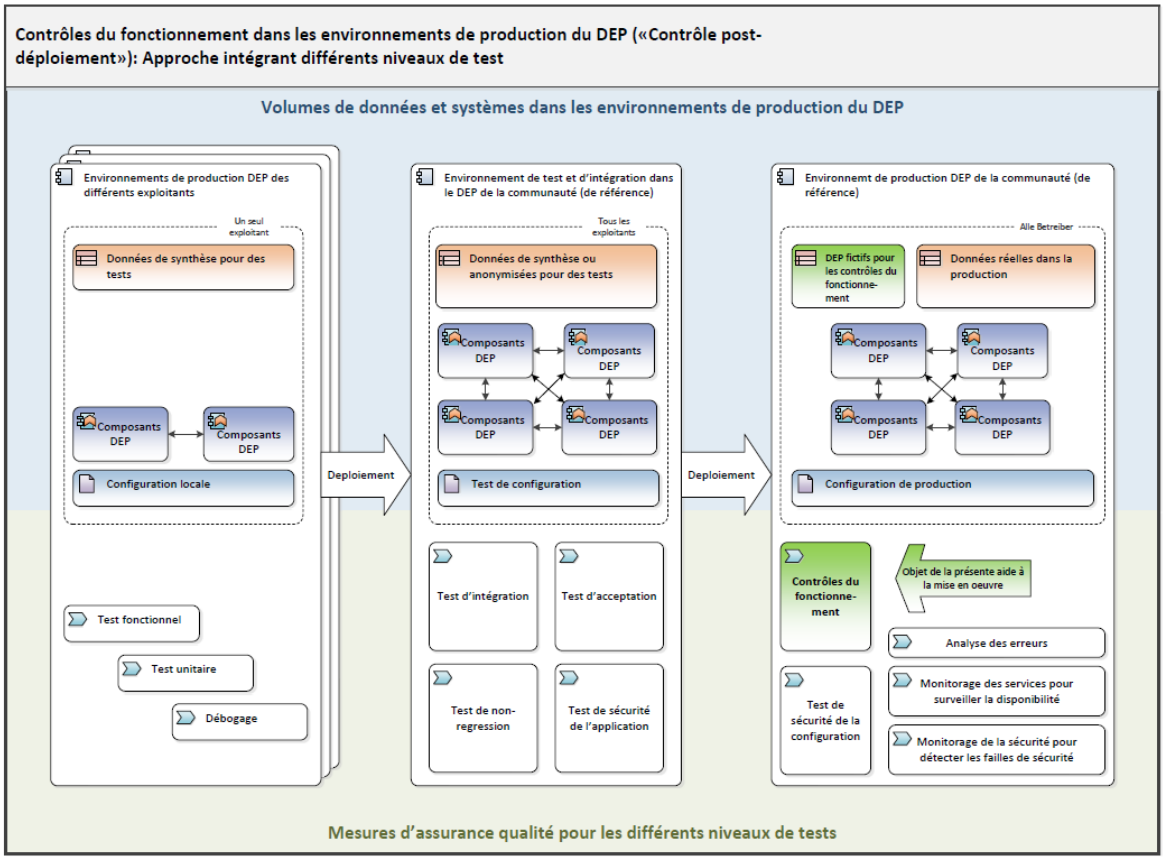


Illustration 1 : contrôles du fonctionnement dans les environnements de production du DEP selon une approche intégrant différents niveaux de test

Les contrôles du fonctionnement dans les environnements de production du DEP ont lieu dans tous les cas. Seule se pose la question de savoir s'ils sont effectués, comme prévu, par le personnel administratif ou, de manière spontanée, par les utilisateurs, qui remarquent des erreurs dans l'exploitation courante et les signalent.

2.2 Expériences tirées des projets pilotes DEP

Les contrôles du fonctionnement dans les environnements de production du DEP sont indispensables dans la pratique

Dans le cadre des deux principaux projets pilotes relatifs au DEP (MonDossierMédical à Genève et myEPD à Bâle), le besoin de pouvoir disposer d'outils pour les contrôles du fonctionnement dans les environnements de production du DEP a été clairement exprimé. Les deux organisations d'entreprise ont constaté que, malgré l'exécution professionnelle de tests approfondis dans les environnements d'intégration, des erreurs de différente nature pouvaient survenir dans la production du DEP. Des défaillances ne sont donc jamais à exclure.

Dans le projet pilote eHealth NW, le département de la santé de Bâle-Ville a ainsi autorisé explicitement les exploitants, donnant suite à leur demande, à utiliser un nombre restreint de myEPD fictifs dans la production du DEP. En outre, un petit nombre bien défini de professionnels de la santé, qui travaillent dans les services informatiques de l'institution de santé affiliée, a obtenu l'autorisation d'accéder aux DEP fictifs, voire aux DEP réels, en la présence de leur titulaire (« friendly users »). Les identités électroniques ordinaires ont été attribuées à toutes les parties prenantes.

À Genève, les autorités cantonales disposent d'un professionnel de la santé fictif, qui intervient également à des fins d'assurance qualité. Cette personne fictive peut générer un MonDossierMédical fictif.

Ces exemples montrent que les responsables d'exploitation ont besoin que des possibilités soient mises à leur disposition et qu'ils les mettent déjà en œuvre afin de pouvoir constater, dans le monde « réel » du DEP, que le système fonctionne bien et à une large échelle. Laisser aux utilisateurs (patients et professionnels de la santé) le soin de signaler les bugs et les dysfonctionnements constitue une stratégie trop risquée, car elle suppose que les données du DEP ne seraient pas disponibles au moment opportun.

3 Contrôles du fonctionnement dans le DEP

3.1 Portée des contrôles du fonctionnement

Tous les composants du système sont concernés

Les contrôles du fonctionnement dans les environnements de production du DEP visent à garantir la qualité de la production, dans la mesure où des failles induites par des modifications sont détectées rapidement. Il s'agit, en particulier, de problèmes d'interopérabilité entre les différents exploitants, qui résultent habituellement d'erreurs de configuration et qui ne peuvent pas être identifiés dans les environnements de test. C'est pourquoi les contrôles du fonctionnement doivent concerner tous les composants dont l'interaction est nécessaire pour que l'ensemble du système DEP puisse fonctionner. Il s'agit notamment des éléments suivants :

- Portail des patients, portail pour les professionnels de la santé et portails pour le personnel administratif ;
- Systèmes intégrés au sein des institutions de santé (systèmes primaires, connecteurs DEP, portails d'accès propres à chaque institution de santé) ;
- Systèmes *backend* dans le DEP ;
- Points d'accès (*gateways*) entre les communautés ;
- Systèmes des *Identity Provider* (IdP) pour les patients et les professionnels de la santé/auxiliaires ;
- Services nationaux (UPI, HPD national, CPI, MDI).

Les erreurs intervenant lors de la reprise des données ou du code de programmation dans le cadre du déploiement ou les problèmes de performance dus à la configuration ne peuvent être identifiés que dans l'environnement de production du DEP.

3.2 Cas d'application

Informations relatives aux cas d'application

Dans les pages suivantes, les cas d'application (*use cases*) sont indiqués dans un tableau, selon un certain ordre.

La description des cas d'application contient les indications suivantes :

- la colonne « cas d'application » contient les fonctions du DEP devant faire l'objet du contrôle (« qu'est-ce qui est contrôlé ») ;
- la colonne « vérificateur » (en jaune) indique qui effectue le contrôle (« qui contrôle ») ;
- la colonne « automatisation » (en rouge) indique s'il est possible d'automatiser le contrôle[1] ;
- la colonne « composants vérifiés » (en bleu) montre quels composants sont concernés pour chaque fonction, faisant ainsi l'objet d'un contrôle du fonctionnement ;
- la colonne « Audit Trail » indique les fonctions dont l'exécution est consignée dans l'Audit Trail (ATNA Log) de la communauté ;

[1] L'automatisation présuppose un vérificateur anonyme ou technique. Pour les fonctions concernant les utilisateurs finaux, il faudrait disposer d'un logiciel d'émulation et d'un moyen d'authentification qui puisse être utilisé sans l'interaction des utilisateurs (p. ex., un *soft token*). Or, ces deux outils ne sont actuellement pas disponibles dans le cadre du DEP.

- Sous « erreurs détectables », on trouve quelques situations d'erreur classiques qui peuvent être identifiées grâce à ce contrôle. À noter que cette liste n'est pas exhaustive.

La colonne « risque » évalue le degré d'utilité du contrôle du fonctionnement sur la base de la fréquence à laquelle les erreurs se produisent et de leur ampleur. L'évaluation des risques mentionnée dans le tableau constitue une aide non contraignante pour les communautés (de référence).

Cas d'application		Vérificateur						Automatisation ?	Composants vérifiés							Audit Trail	Erreurs détectables	Risque		
		Patient	Représentant	Professionnel de la santé	Auxiliaire	Personnel administratif	Utilisateur technique		Portail des patients	Portail des professionnels de la	Portails pour le personnel	Systèmes des institutions de santé	Backend DEP	Systèmes IdP	Services nationaux			Fréquence	Ampleur	Risque chiffré
1	**Champs de valeur (value sets) stockés**							Oui									Documents avec métadonnées non valables ou professionnels de la santé/auxiliaires avec attributs non valables. *Remarque :* les métadonnées valables pour l'échange de données médicales sont fixées à l'annexe 3 de l'ordonnance du DFI et peuvent être consultées dans le Metadata-Index MDI.	2	1	**2**
1a	Rôle de l'auteur													X						
1b	Spécialité de l'auteur													X						
1c	Type organisationnel de l'institution de santé											X	X							
1d	Spécialisation de l'institution de santé											X	X							
1e	Classification du document											X	X							
1f	Type du document											X	X							
1g	Processus documenté											X	X							
1h	Langue du document											X	X							
1i	Sexe du patient											X	X							
1j	Niveau de confidentialité											X	X							
1k	Format technique											X	X							
1l	MIME Type du document											X	X							
1m	Raison de la mise à disposition											X	X							
1n	Rôle de la personne détentrice											X	X							
2	**Vérification des points de terminaison**							Oui									Point de terminaison indisponible / inatteignable (défaillance, erreur dans la configuration du réseau ou du pare-feu, certificats MTLS non valables, …)	3	2	**6**
2a	MPI												X							
2b	HPD de la communauté												X							
2c	Document Repository											(X)[1]	X							
2d	Document Registry												X							
2e	Audit Record Repository												X							
2f	IdP pour les patients													X						
2g	IdP pour professionnels de la santé et auxiliaires													X						
2h	X-Assertion Provider pour les patients												X	(X)[2]						
2i	X-Assertion Provider prof. de la santé et auxiliaires												X	(X)[2]						
2j	Service UPI														X					
2k	HPD national														X					
3	**Monitorage des services**							Oui									Le service ne fonctionne pas (certificats incorrects, défaillance du service, défaillance au niveau de la communauté,…)	3	2	**6**
3a	MPI						X						X							
3b	HPD de la communauté						X						X							
3c	Document Repository						X					(X)[1]	X							

Cas d'application		Vérificateur						Automatisation ?	Composants vérifiés							Audit Trail	Erreurs détectables	Risque		
		Patient	Représentant	Professionnel de la santé	Auxiliaire	Personnel administratif	Utilisateur technique		Portail des patients	Portail des professionnels de la	Portails pour le personnel	Systèmes des institutions de santé	Backend DEP	Systèmes IdP	Services nationaux			Fréquence	Ampleur	Risque chiffré
3d	Document Registry						X						X							
3e	Audit Record Repository						X						X							
3f	IdP pour les patients	X	X					Non						X						
2g	IdP pour professionnels de la santé et auxiliaires			X	X									X						
3h	X-Assertion Provider pour les patients						X	Oui					X	(X) [2]						
3i	X-Assertion Provider prof. de la santé et auxiliaires						X						X	(X) [2]						
3j	Service UPI						X								X					
3k	HPD national						X								X					
4	***On/Off-boarding* de patients**							Non									Problèmes d'intégration de la plateforme DEP avec service UPI, IdP pour les patients	2	1[4]	**2**
4a	Ouverture d'un DEP	X				X			X		X		X	X	X	X				
4b	Changement de communauté de référence	X	(X)[3]			X			X		X		X	X	X	X				
4c	Révocation du DEP	X	(X)[3]			X			X		X		X	X	X	X				
4d	Annulation en cas de décès					X					X		X	X	X	X				
5	**Gestion du MPI**							Non									Les identités locales des patients et leurs attributs ne sont pas gérés ou échangés correctement.	1	3[5]	**3**
5a	Introduction des nouveaux patients dans le MPI					X					X		X		X	X				
5b	Purge des données MPI					X					X		X			X				
6	***On/Off-boarding* de l'institution de santé**					X	X	Non			X		X		X	X	Mauvais provisionnement de l'institution de santé dans les systèmes et le HPD, p. ex., en raison d'OID stockés au mauvais endroit pour la production.	1	2	**2**
7	**Gestion des professionnels de la santé/auxiliaires (y c. groupes)**							Non									Problèmes d'intégration de la plateforme DEP avec le HPD national, l'IdP du professionnel de la santé et les systèmes IAM de l'institution de santé (si disponibles)	2	1[4]	**2**
7a	Gestion manuelle prof. de la santé/auxiliaires			X	X	X					X		X	X	X	X				
7b	Gestion manuelle des groupes (prof. de la santé)					X					X		X	X	X	X				
7c	Gestion des professionnels de la santé/auxiliaires au moyen de l'IAM de l'institution de santé						X	Oui				X	X	X	X	X				
8	**Login professionnels de la santé/auxiliaires**							Non									Problèmes d'intégration du portail pour les professionnels de la santé/afficheur DEP de l'institution de santé avec l'IdP du professionnel de la santé et/ou l'Active Directory de l'institution de santé	2	2	**4**
8a	Login au portail des prof. de la santé depuis Internet			X	X					X			X	X		X				
8b	Login au portail des prof. de la santé avec le SSO de l'institution de santé			X	X					X		X	X	X		X				
8c	Login à l'afficheur DEP de l'institution de santé			X	X					X		X	X	X		X				
9	**Gestion des documents prof. santé/aux.**																Problèmes d'intégration du backend DEP avec l'upload-client de l'institution de santé ou l'Assertion Provider. Intégration intercommunautaire ?	2	2	**4**
9a	Upload/download manuel de documents			X	X			Non		X		X	X	X		X				
9b	Upload automatique de documents (M2M)						X	Oui				X	X	(X)[2]		X				

Cas d'application		Vérificateur						Automatisation ?	Composants vérifiés								Erreurs détectables	Risque		
		Patient	Représentant	Professionnel de la santé	Auxiliaire	Personnel administratif	Utilisateur technique		Portail des patients	Portail des professionnels de la	Portails pour le personnel	Systèmes des institutions de santé	Backend DEP	Systèmes IdP	Services nationaux	Audit Trail		Fréquence	Ampleur	Risque chiffré
10	**Transmission des droits d'accès**			X				Non		X			X			X		1	1	**1**
11	**Fonctions générales du portail pour les professionnels de la santé**			X	X			Non		X			X				Défaillance au niveau du portail pour les professionnels de la santé (erreurs inconnues)	1	2	**2**
12	**Login patients / représentant**	X	X					Non	X				X	X		X	Problèmes d'intégration du portail des patients avec l'IdP des patients et/ou l'X-Assertion Provider pour les patients.	2	2	**4**
13	**Gestion des documents par les patients**							Non									Problèmes d'intégration du backend DEP avec le portail des patients. Problèmes d'intégration intercommunautaires.	2	2	**4**
13a	Affichage de la liste des documents	X	X						X				X			X				
13b	Accès/téléchargement de documents dans sa propre CR	X	X						X				X			X				
13c	Accès/téléchargement de documents intercommunautaires	X	X						X				X			X				
13d	Accès image DICOM dans sa propre CR	X	X						X				X			X				
13e	Accès image DICOM intercommunautaire	X	X						X				X			X				
13f	Upload de documents	X	X						X				X			X				
13g	Adaptation du niveau de confidentialité (dans la CR)	X	X						X				X			X				
13h	Adaptation du niveau de confidentialité (entre les communautés)	X	X						X				X			X				
13i	Exportation de l'archivage hors ligne (XDM)	X	X						X				X			X				
13j	Importation de l'archivage hors ligne (XDM)	X	X						X				X			X				
13k	Exclure la suppression des documents après 20 ans	X	X						X				X			X				
14	**Gestion des droits d'accès par les patients**							Non									Problèmes d'intégration du backend DEP avec le portail des patients.	1	1[4]	**1**
14a	Gestion des droits d'accès des professionnels de la santé (y c. délégation)	X	X						X				X			X				
14b	Gestion des droits d'accès des groupes de professionnels de la santé	X	X						X				X			X				
14c	Configuration de l'accès d'urgence	X	X						X				X			X				
14d	Configuration du niveau de confidentialité normal	X	X						X				X			X				
15	**Institution/révocation d'un représentant**	X	(X)[3]					Non	X		X		X	X		X	Problèmes d'intégration du portail des patients avec l'IdP des patients et le backend DEP.	2	1[4]	**2**
16	**Consulter l'historique d'accès**	X	X					Non	X				X				Problèmes d'intégration du backend DEP avec le portail des patients.	2	1[4]	**2**
17	**Notifications**							Non									Problèmes d'intégration du backend DEP avec le portail des patients.	1	1	**1**
17a	Paramétrage des notifications	X	X						X				X			X				
17b	Notification en cas de changement de groupe	X	X						X				X			X				
17c	Notification en cas d'accès d'urgence	X	X						X				X			X				
18	**Fonctions générales du portail des patients**	X	X					Non	X								Défaillance au niveau du portail des patients (erreurs inconnues).	1	1	**1**

Notes de bas de page relatives au tableau des cas d'application :

[1]: Si l'institution de santé tient elle-même son propre répertoire.

[2]: Si l'X-Assertion Provider est exploité par l'IdP.

[3]: Les communautés de référence peuvent restreindre le droit des représentants volontaires et, par exemple, empêcher la désignation d'autres représentants, la révocation du DEP ou le changement de communauté de référence par le représentant dans le DEP.

[4]: Les cas d'application administratifs (p. ex. gestion des patients et des professionnels de la santé/auxiliaires) sont moins problématiques en termes de disponibilité que les services fonctionnant non-stop (p. ex. login ou upload/download de documents).

[5]: Une défaillance au niveau de la purge des données MPI peut engendrer l'attribution de documents aux mauvais patients.

4 Conditions-cadres

Groupe de travail temporaire Contrôles du fonctionnement

Dans le groupe de travail temporaire « Contrôles du fonctionnement / assurance qualité dans les systèmes opérationnels du DEP », d'importantes catégories d'ayants droit ont été impliquées dans l'élaboration du présent document.

Ces catégories d'ayants droit ont formulé les conditions-cadres ci-dessous pour la solution retenue :

EPR-SPID réels possibles pour (quelques) personnes fictives

Conditions-cadres de la Centrale de compensation (CdC) :

- La CdC peut créer des personnes fictives dans l'environnement de production UPI auxquelles des EPR-SPID réels peuvent être attribués par la CdC (ou les communautés de référence).
- Les communautés (de référence) ne devraient pas utiliser d'EPR-SPID fictifs dans leurs environnements de production car un conflit risque d'intervenir tôt ou tard avec un EPR-SPID réel.
- Les personnes fictives ne peuvent être utilisées que pour vérifier la bonne configuration et la disponibilité de l'ensemble du système de production dans le cadre des contrôles du fonctionnement.
- Les personnes fictives ne doivent pas être utilisées pour l'exécution de tests fonctionnels ; pour ces derniers, seuls les environnements d'intégration DEP peuvent être utilisés.

Les modifications du HPD national ne sont pas autorisées

Conditions-cadres de l'Office fédéral de la santé publique (OFSP) :

- Les contrôles du fonctionnement ne doivent pas nécessiter de modifications techniques ou au niveau de la configuration concernant le HPD national.

Les identités fictives avec une identité confirmée ne sont pas possibles

Conditions-cadres de l'*Identity Provider* pour les patients (IdP) :

- La création d'identités fictives avec une identité confirmée pose un problème de conformité insoluble.

La solution telle que décrite aux chapitres suivants tient compte de ces conditions-cadres.

5 Solution retenue

5.1 Dossiers électroniques du patient (DEP) fictifs

DEP fictifs

Dans le cadre des contrôles du fonctionnement dans les environnements de production du dossier électronique du patient (DEP), les communautés de référence ouvrent des DEP fictifs. Ceux-ci, incluant les droits DEP d'un ou de plusieurs représentants, sont établis par l'exploitant de la plateforme ou par un administrateur système de la communauté de référence sans que l'exécution d'un processus normal d'*onboarding* pour le DEP ne soit nécessaire.

Les titulaires des DEP fictifs sont des personnes fictives auxquelles est attribué un EPR-SPID réel et actif dans le service de production UPI. Il doit être possible d'attribuer aux personnes fictives un EPR-SPID actif par le biais de l'interface eCH-0214.

Contrôles du fonctionnement par les représentants dans le DEP

Les personnes fictives n'obtiennent pas d'identité électronique et ne peuvent pas accéder au portail des patients. C'est pourquoi les contrôles du fonctionnement sont effectués par les représentants dans le DEP qui sont désignés pour les DEP fictifs. Pour ce faire, les représentants dans le DEP utilisent une vraie identité électronique et procèdent aux contrôles du fonctionnement en tant que représentant dans le DEP.

Pour les communautés de référence qui restreignent les droits des représentants volontaires dans le DEP et qui, par exemple, empêchent la désignation d'autres représentants, la révocation du DEP ou le changement de communauté de référence par le représentant dans le DEP, il en résulte une restriction des cas d'application lors des contrôles du fonctionnement.

5.2 Auxiliaires avec tâches AQ

Auxiliaires avec tâches AQ

Les contrôles du fonctionnement sont effectués par les auxiliaires mandatés à cet effet. Ces « auxiliaires avec tâches AQ » ne se différencient pas des autres auxiliaires, si ce n'est qu'ils utilisent le système de production du DEP dans un contexte d'assurance qualité et non dans un contexte de traitement. Aucun auxiliaire ou professionnel de la santé fictif n'est institué, ce qui ne nécessite donc aucune modification au niveau du HPD national ou de l'IdP pour les professionnels de la santé.

Pour les contrôles du fonctionnement, les auxiliaires avec tâches AQ utilisent les accès au DEP suivants :

- Le portail réservé aux professionnels de la santé de la communauté (de référence) ou un portail pour les professionnels de la santé propre à l'institution de santé auquel ils s'authentifient par le biais de leur moyen d'identification personnel. Afin de pouvoir accéder aux DEP fictifs, ils sont subordonnés à un professionnel de la santé avec responsabilité AQ (cf. paragraphe suivant) ;
- Les auxiliaires avec tâches AQ peuvent également se connecter au portail des patients en tant que représentant d'un patient fictif, dans la mesure où ils sont enregistrés comme représentant dans le DEP fictif (cf. chapitre 5.1).

Professionnel de la santé avec responsabilité AQ

Les auxiliaires avec tâches AQ sont subordonnés à un professionnel de la santé qui est responsable de l'exécution en bonne et due forme des contrôles du fonctionnement.

Ce « professionnel de la santé avec responsabilité AQ » est autorisé à accéder au DEP fictif par un représentant du patient fictif dans le DEP.

Le professionnel de la santé avec responsabilité AQ peut également accéder aux DEP réels dans un contexte de traitement. C'est pourquoi il doit en informer l'auxiliaire avec tâches AQ qui lui est subordonné et contrôler que l'accès aux DEP réels n'est pas autorisé dans un contexte d'assurance qualité.

5.3 Distinction entre le contexte d'assurance qualité et le contexte de traitement

Stricte distinction entre le contexte d'AQ et le contexte de traitement

Les DEP fictifs ne peuvent contenir que des documents fictifs avec des contenus fictifs sans lien avec un traitement médical ou avec des personnes réelles. On ne peut donc jamais accéder aux DEP fictifs dans un contexte de traitement, mais toujours dans un contexte d'assurance qualité.

L'autorisation d'accès aux DEP fictifs ne peut être accordée qu'aux professionnels de la santé avec responsabilité AQ et seuls les auxiliaires avec tâches AQ ont le droit d'accéder aux DEP fictifs.

Seuls des DEP fictifs peuvent être utilisés pour les contrôles du fonctionnement dans les environnements de production du DEP. Les auxiliaires avec tâches AQ n'ont le droit d'accéder qu'à des DEP fictifs, même s'ils devaient disposer de droits d'accès élargis. Lorsque ce principe ne peut pas être appliqué techniquement (p. ex. accès d'urgence), le professionnel de la santé avec responsabilité AQ doit mettre en œuvre la réglementation définie par la communauté à l'égard des auxiliaires avec tâches AQ.

5.4 Mise en œuvre dans les composants DEP

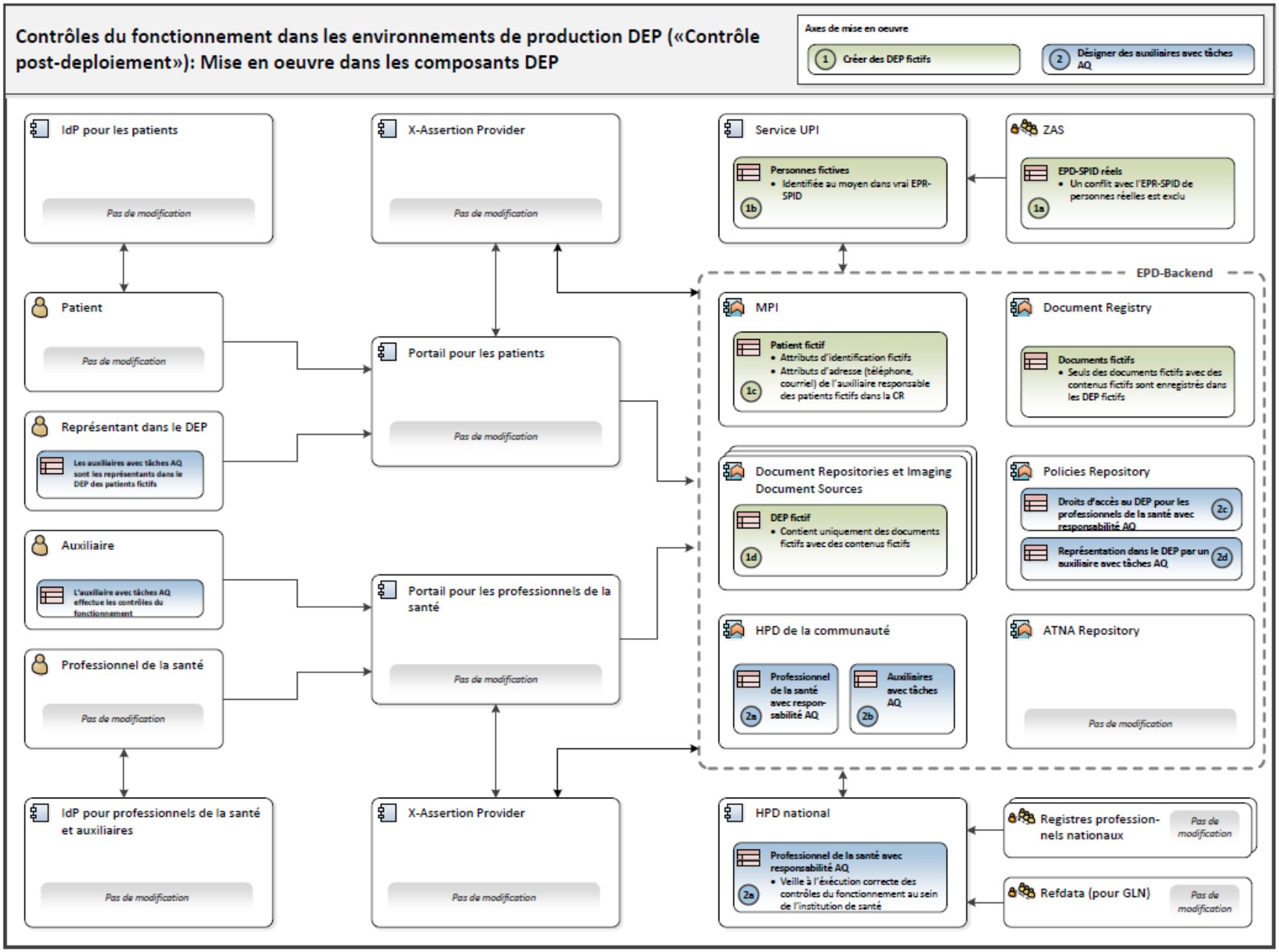
Trois axes de mise en œuvre

Pour que les contrôles du fonctionnement puissent avoir lieu dans les environnements de production du DEP, il importe de prendre les dispositions nécessaires dans les différents systèmes et systèmes environnants du DEP :

1. Création de DEP fictifs : cela nécessite des personnes fictives avec des EPR-SPID réels et les saisies y relatives dans le service de production UPI ainsi que dans l'index des patients (ou MPI) de la communauté (de référence) ;
2. Institution de représentants dans le DEP pour les DEP fictifs. Il peut s'agir d'auxiliaires avec tâches AQ, mais ce n'est pas impératif ;
3. Institution d'auxiliaires avec tâches AQ, ce qui implique que :
   - ⇨ les personnes mandatées sont enregistrées dans le HPD de la communauté (de référence) ;
   - ⇨ les auxiliaires sont subordonnés à un professionnel de la santé avec responsabilité AQ ;
   - ⇨ les droits d'accès aux DEP fictifs sont attribués à ce professionnel de la santé avec responsabilité AQ.

D’un point de vue technique, les auxiliaires avec tâches AQ ne se différencient pas des autres auxiliaires. C’est pourquoi il n’est besoin de procéder à des modifications ou de saisir des données ni dans le HPD national, ni dans le portail pour les professionnels de la santé.

L’illustration à la page suivante montre quelles dispositions mettre en œuvre dans quel composant DEP :


Contrôles du fonctionnement dans les environnements de production DEP («Contrôle post-deploiement»): Mise en oeuvre dans les composants DEP
Axes de mise en oeuvre
1 Créer des DEP fictifs
2 Désigner des auxiliaires avec tâches AQ
IdP pour les patients
Pas de modification
X-Assertion Provider
Pas de modification
Service UPI
Personnes fictives
• Identifiée au moyen dans vrai EPR-SPID
1b
ZAS
EPD-SPID réels
• Un conflit avec l'EPR-SPID de personnes réelles est exclu
1a
EPD-Backend
Patient
Pas de modification
Portail pour les patients
Pas de modification
MPI
Patient fictif
• Attributs d'identification fictifs
• Attributs d'adresse (téléphone, courriel) de l'auxiliaire responsable des patients fictifs dans la CR
1c
Document Registry
Documents fictifs
• Seuls des documents fictifs avec des contenus fictifs sont enregistrés dans les DEP fictifs
Représentant dans le DEP
Les auxiliaires avec tâches AQ sont les représentants dans le DEP des patients fictifs
Document Repositories et Imaging Document Sources
DEP fictif
• Contient uniquement des documents fictifs avec des contenus fictifs
1d
Policies Repository
Droits d'accès au DEP pour les professionnels de la santé avec responsabilité AQ
2c
Représentation dans le DEP par un auxiliaire avec tâches AQ
2d
Auxiliaire
L'auxiliaire avec tâches AQ effectue les contrôles du fonctionnement
Portail pour les professionnels de la santé
Pas de modification
HPD de la communauté
Professionnel de la santé avec responsabilité AQ
2a
Auxiliaires avec tâches AQ
2b
ATNA Repository
Pas de modification
Professionnel de la santé
Pas de modification
IdP pour professionnels de la santé et auxiliaires
Pas de modification
X-Assertion Provider
Pas de modification
HPD national
Professionnel de la santé avec responsabilité AQ
• Veille à l'éxécution correcte des contrôles du fonctionnement au sein de l'institution de santé
2a
Registres professionnels nationaux
Pas de modification
Refdata (pour GLN)
Pas de modification

6 Mesures d'exécution

Le présent chapitre identifie et décrit les mesures permettant d'effectuer les contrôles du fonctionnement dans les environnements de production du DEP. En outre, il esquisse les mesures d'accompagnement recommandées pour continuer à améliorer la qualité de la production.

6.1 Application de la présente aide à la mise en œuvre

M1 Désignation de personnes fictives dans le service UPI

Jusqu'à fin mars 2020, la Centrale de Compensation (CdC) saisit dans le service de production UPI au maximum 24 personnes fictives, qui peuvent être utilisées par les communautés (de référence) DEP pour les contrôles du fonctionnement dans les environnements de production du DEP :

- Chaque communauté de référence dispose de deux personnes fictives de sexe différent auxquelles elle peut attribuer un EPR-SPID.
- Les communautés de référence peuvent utiliser l'une de ces personnes fictives pour les contrôles du fonctionnement lors de transactions internes et de transactions intercommunautaires.
- Il existe également quatre personnes fictives pour les besoins nationaux dont l'EPR-SPID est généré par la CdC :
  - une personne fictive décédée ;
  - une personne fictive de sexe masculin et une de sexe féminin ;
  - dans une extension future du service UPI : une personne de sexe « other » au sens de l'annexe 3 de l'ordonnance du DFI ou de sexe « indéterminé » conformément à la loi sur l'harmonisation des registres (cf. OFS « Catalogue officiel des caractères », version 2014 § 33 Sexe).

Les personnes fictives avec leurs attributs (nom, prénom, sexe, date de naissance) sont saisies par la CdC dans le service de production UPI.

eHealth Suisse attribue à chaque communauté de référence deux personnes fictives dont le DEP fictif (y c. EPR-SPID) relève de la responsabilité de la communauté de référence.

Le cas d'application « Révocation du DEP » doit lui aussi faire l'objet de contrôles. Afin que le nombre d'EPR-SPID utilisés pour les contrôles du fonctionnement reste limité (comparé au total de tous les EPR-SPID possibles), une communauté de référence n'a pas le droit d'annuler plus de 400 EPR-SPID par an dans le cadre des contrôles du fonctionnement dans la production.

Remarques :

- Conformément aux règles de base de la CdC, les EPR-SPID sont générés de façon aléatoire et une fois annulés, ils ne peuvent plus jamais être utilisés. Il n'est dès lors pas possible de réutiliser le même EPR-SPID après la révocation d'un DEP.
- Les personnes fictives peuvent également être consultées par d'autres clients du service UPI.

M2 Création de DEP fictifs dans les communautés (de référence)

Les communautés de référence ouvrent un dossier électronique du patient (DEP) pour chacune des personnes fictives qui leur a été attribuée.

Les DEP fictifs, avec les droits DEP d'au moins un représentant, sont établis par l'exploitant de la plateforme ou par un administrateur système de la communauté de référence sans qu'il ne soit nécessaire d'exécuter un processus normal d'*onboarding* pour le DEP. À cet égard, les éléments suivants sont mis en place :

- Inscription dans le MPI avec un EPR-SPID actif, que la CdC met à la disposition du titulaire fictif du DEP au sein d'une communauté de référence définie (via la transaction Patient Identity Feed HL7 V3 [ITI-44], pas de droit DEP nécessaire) ;
- Règles de configuration DEP (21, 22, 23), où est inscrit l'EPR-SPID correspondant (via la transaction Privacy Policy Feed [PPQ-1], droits DEP d'« administrateur de police » (« policy administrator ») nécessaires) ;
- Règle d'accès au DEP (« Access Policy ») (33) qui permet à un ou plusieurs représentants d'accéder au DEP avec l'EPR-SPID adéquat (via la transaction Privacy Policy Feed [PPQ-1], droits DEP d'« administrateur de police » (« policy administrator ») nécessaires) ;
- Le cas échéant, autres éléments spécifiques à la plateforme DEP qui sont nécessaires au fonctionnement du portail des patients p. ex., conformément au modèle de données (par le biais de méthodes propres à l'application, pas de droit DEP nécessaire).

Les documents et les métadonnées ainsi que les droits d'accès peuvent être créés dans le DEP fictif par le représentant dans le DEP.

Remarque : seules les communautés de référence peuvent ouvrir des DEP fictifs étant donné que les communautés ne disposent pas de l'infrastructure adéquate.

M3 Auxiliaire responsable des DEP fictifs

La communauté de référence désigne précisément un auxiliaire avec tâches AQ (y c. représentant), qui est responsable des deux DEP fictifs de la communauté de référence.

Cet auxiliaire avec tâches AQ :

- est responsable des données des deux patients fictifs ;
- est le représentant dans le DEP des deux patients fictifs ;
- gère d'autres représentations dans le DEP pour les patients fictifs, ceci étant limité aux auxiliaires avec tâches AQ ;
- délivre les droits d'accès aux DEP fictifs à tous les professionnels de la santé avec responsabilité AQ au sein de sa propre communauté de référence ;
- peut délivrer les droits d'accès aux DEP fictifs à des professionnels de la santé avec responsabilité AQ qui font partie d'autres communautés ;

- vérifie, durant les contrôles du fonctionnement, que seuls des documents fictifs avec des contenus fictifs se trouvent dans les DEP fictifs.

M4 Attributs des patients fictifs

Les données de référence des personnes fictives (nom, prénom, sexe, date de naissance) sont saisies par la CdC dans le service UPI. Toutes les autres données des patients fictifs sont saisies par l'auxiliaire responsable des DEP fictifs selon les principes suivants :

- Adresse postale des patients fictifs :
  Adresse postale de la communauté de référence
- Adresse e-mail des patients fictifs :
  Adresse e-mail de l'auxiliaire responsable
- Numéros de téléphone des patients fictifs :
  Numéros de téléphone de l'auxiliaire responsable

Les autres attributs sont définis en fonction des besoins de la communauté de référence.

M5 Règles pour l'exécution des contrôles du fonctionnement

Dans le cadre de l'exécution des contrôles du fonctionnement (contrôles post-déploiement), chaque communauté (de référence) définit un ensemble de règles portant au moins sur les points suivants :

- Tâches, compétences et responsabilités (TCR) des auxiliaires avec tâches AQ et des professionnels de la santé avec responsabilité AQ ;
- Instructions délivrées aux auxiliaires avec tâches AQ quant à l'interdiction d'accéder aux DEP réels dans le contexte d'assurance qualité ;
- Marche à suivre pour l'exécution des contrôles du fonctionnement. Il s'agit, par exemple, de clarifier les points suivants :
  - ⇨ Dans quels cas les DEP fictifs sont-ils révoqués (selon M1, une communauté de référence a le droit d'annuler au maximum 400 EPR-SPID de personnes fictives chaque année) ?
  - ⇨ Les droits d'accès et les représentations sont-ils retirés après chaque contrôle du fonctionnement ou sont-ils permanents ?
  - ⇨ Quelles règles sont valables pour l'exécution des contrôles manuels du fonctionnement avec l'utilisation de DEP fictifs au sein de sa propre communauté (de référence) ou d'autres communautés de référence ?
  - ⇨ Quelles règles s'appliquent à l'upload automatique de documents fictifs (clairement identifiés comme tels) dans les DEP fictifs ?
- Le cas échéant, règles pour l'utilisation des DEP fictifs dans les systèmes primaires d'institutions de santé raccordées (gestion des patients, KIS, etc.)

M6 Liste de tous les auxiliaires et professionnels de la santé avec fonctions AQ

L'auxiliaire responsable des DEP fictifs tient une liste comportant :

- tous les auxiliaires avec tâches AQ au sein de la communauté (de référence) ;
- tous les professionnels de la santé avec responsabilité AQ au sein de la communauté (de référence).

Les problématiques et les tâches de coordination concernant plusieurs communautés (de référence) relèvent de la compétence d'eHealth Suisse.

6.2 Mesures d'accompagnement ou complémentaires

En sus des mesures décrites au point 6.1 pour l'application de la présente aide à la mise en œuvre, il convient d'envisager d'autres mesures en vue d'améliorer durablement la qualité de la production :

MA1 Monitorage automatisé

Contrôle automatisé et continu pour s'assurer que les points de terminaison du DEP soient atteignables et que les services du DEP soient disponibles (cas d'application 2a à 2k, 3a à 3e et 3h à 3k).

MA2 Outils pour l'analyse des erreurs

Mise à disposition d'outils pour l'analyse des erreurs survenant dans les environnements de production du DEP, le cas échéant au moyen des DEP fictifs.