Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

RS 816.11.n / Annexe 2 de l'ordonnance du DFI du ... sur le dossier électronique du patient

Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (CTO)

Version: 1.0 22.03.2016
Entrée en vigueur : ...

1 Gestion (art. 8 ODEP) 4

1.1 Gestion des institutions de santé (let. a et c) 4
1.2 Gestion des professionnels de la santé (let. a à d) 4
1.3 Gestion des auxiliaires des professionnels de la santé 5
1.4 Identification et authentification (art. 8, let. d) 5
1.5 Gestion de groupes de professionnels de la santé (art. 8, let. a, c, e et f) 6

2 Tenue et transfert des données (art. 9 ODEP) 6

2.1 Destruction de données (al. 1, let. a et b) 6
2.2 Stockage des documents (al. 1, let. c) 6
2.3 Gestion à la demande du patient (al. 2) 7
2.4 Mise en œuvre des niveaux de confidentialité (al. 3, let. a) 7
2.5 Respect des droits d'accès accordés (al. 3, let. a) 7
2.6 Accès en cas d'urgence (al. 3, let. a) 7
2.7 Vérification de la gestion des autorisations (al. 3, let. a) 7
2.8 Métadonnées (let. c) 8
2.9 Profils d'intégration (art. 3, let. d) 8
2.10 Données historisées (al. 3, let. e) 11
2.11 Association du numéro d'identification du patient avec des documents (al. 3) 12

3 Portail d'accès pour les professionnels de la santé (art. 10 ODEP) 13

3.1 Conformité aux dispositions légales 13
3.2 Présentation 13
3.3 Accessibilité 13
3.4 Formats de fichiers : mise à disposition 13
3.5 Formats de fichiers : requête 13

4 Protection et sécurité des données (art. 11 ODEP) 14

4.1 Exigences envers les tiers 14
4.2 Système de gestion de la protection et de la sécurité des données (al. 1) 14
4.3 Responsable de la protection et de la sécurité des données (al. 1, let. a) 14
4.4 Détection des incidents de sécurité (SIEM) (al. 1, let. b) 15
4.5 Gestion des incidents de sécurité (SIEM) (al. 1, let. b) 15
4.6 Protection contre les logiciels malveillants (al. 1, let. b) 16
4.7 Gestion des failles de sécurité (al. 1, let. b) 16
4.8 Gestion des données et des systèmes sensibles (al. 1, let. c et d) 16
4.9 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 applicables aux terminaux (let. e) 17
4.10 Exigences relatives à la protection et à la sécurité des données imposées au personnel (al. 1, let. f) 18
4.11 Exigences relatives à la protection et à la sécurité des données imposées aux tiers (al. 1, let. f) 18
4.12 Surveillance et contrôle des prestations de service (al. 1, let. f) 19
4.13 Obligation de déclarer les incidents de sécurité (al. 2) 19
4.14 Sécurité d'exploitation (al. 3) 19
4.15 Achat, développement et maintenance des systèmes (al. 3) 20
4.16 Cryptage de la communication (al. 3) 21
4.17 Enregistrement crypté des données (al. 3) 21
4.18 Gestion des clés cryptographiques (al. 3) 21
4.19 Sécurité de la communication : gestion des réseaux (al. 3) 21
4.20 Sécurité de la communication : services réseau (al. 3) 22
4.21 Expiration des sessions dans le réseau (« *session timeout* ») (al. 3) 23

4.22 Système intermédiaire (al. 3) 23
4.23 Accessibilité (al. 3) 23
4.24 Dispositifs de stockage sous juridiction suisse (al. 4) 23
5 Service d'assistance pour les professionnels de la santé (art. 12 ODEP) 24
6 Information du patient (art. 14 ODEP) 24
6.1 L'information du patient selon l'art. 14 ODEP comprend au moins les points suivants : 24
7 Consentement (art. 15 ODEP) 25
7.1 Les procédures de constitution du dossier électronique du patient doivent être définies, documentées, mises en œuvre et respectées. 25
8 Gestion (art. 16 ODEP) 26
8.1 Entrée et sortie de patients (al. 1, let. a) 26
8.2 Identification des patients (al. 1, let. b) 26
8.3 Identification et authentification (al. 1, let. c) 26
8.4 Changement de communauté de référence (let. e) 27
8.5 Respect des décisions d'accès visant le traitement de la configuration des autorisations (al. 2) : droits d'accès (art. 2, al. 1, OPED) et options du patient (art. 3 OPED) 27
8.6 Gestion des autorisations (al. 2) : droits d'accès (art. 2, al. 1 à 4, ODEP) 27
8.7 Options du patient (art. 3 ODEP) 27
8.8 Représentation (art. 16, al. 1, let. c et al. 3, ODEP) 28
9 Portail d'accès pour les patients (art. 17 ODEP) 28
9.1 Conformité aux dispositions légales 28
9.2 Présentation 29
9.3 Accessibilité 29
9.4 Formats de fichiers : mise à disposition 29
9.5 Formats de fichiers : requête 29
9.6 Données historisées (let. c) 30
10 Disponibilité des données enregistrées par les patients (art. 18 ODEP) 30
10.1 Stockage des documents de patients 30
10.2 Archivage hors ligne des documents et des métadonnées 30
11 Service d'assistance pour les patients (art. 19 ODEP) 31
12 Suppression du dossier électronique du patient (art. 20 ODEP) 31
12.2 Conditions de la suppression du dossier électronique du patient (al. 1) 31
12.3 Suppression du dossier électronique du patient (al. 2) 31
12.4 Révocation du consentement à la tenue du dossier électronique du patient (al. 2, let. a) 32
12.5 Fermeture en cas d'inutilisation (al. 2, let. b) 32

Exigences à l’égard des communautés

1 Gestion (art. 8 ODEP)

1.1 Gestion des institutions de santé (let. a et c)

1.1.1 Les processus d’entrée et de sortie des institutions de santé doivent être définis, documentés, mis en œuvre et respectés.

1.1.2 Le processus d’entrée des institutions de santé doit garantir :
1.1.2.1 la conclusion d’accords exigeant et contrôlant le respect des tâches et obligations incombant à l’institution de santé, au moins en matière de protection et de sécurité des données ;
1.1.2.2 l’actualisation des données du service de recherche des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP ;
1.1.2.3 le déclenchement du processus « entrée de professionnels de la santé » (voir ch. 1.2.2) pour tous les professionnels de la santé admis rattachés à une institution de santé.

1.1.3 Le processus de sortie des institutions de santé doit garantir :
1.1.3.1 le déclenchement du processus « sortie de professionnels de la santé » (voir ch. 1.2.4) pour tous les professionnels de la santé sortants rattachés à une institution de santé ;
1.1.3.2 si l’institution de santé sortante ne s’affilie à aucune autre communauté :
1.1.3.2.1 la suppression des documents figurant dans les lieux de stockage de l’institution de santé sortante ;
1.1.3.2.2 la suppression des saisies du registre des documents qui renvoient aux documents figurant dans les lieux de stockage de l’institution sortante ;
1.1.3.2.3 l’information en temps utile des patients concernés.

1.1.4 La communauté est tenue, pour les données qu’elle enregistre dans le service de recherche central des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP :
1.1.4.1 de désigner une personne responsable ;
1.1.4.2 de garantir que l’actualité et l’exactitude des données sont vérifiées et confirmées :
1.1.4.2.1 chaque semestre au moins, dans le cas des institutions de santé ;
1.1.4.2.2 chaque trimestre au moins, dans le cas des groupes de professionnels de la santé.

1.2 Gestion des professionnels de la santé (let. a à d)

1.2.1 Les processus d’entrée, de gestion et de sortie des professionnels de la santé doivent être définis, documentés, mis en œuvre et respectés.

1.2.2 Le processus d’entrée des professionnels de la santé doit garantir que :
1.2.2.1 le consentement du professionnel de la santé à respecter les directives spécifiques de la communauté ou de l’institution de santé est documenté ;
1.2.2.2 l’identification du professionnel de la santé

1.2.2.2.1 repose sur le moyen d'identification d'un éditeur certifié selon l'art. 30 ODEP, ou
1.2.2.2.2 correspond aux exigences de l'art. 23 ODEP ;
1.2.2.3 le professionnel de la santé en question répond à la définition énoncée à l'art. 2, let. b, LDEP ;
1.2.2.4 le moyen d'identification du professionnel de la santé émis par un éditeur selon l'art. 30 ODEP est enregistré ;
1.2.2.5 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées. Si le professionnel de la santé figure dans un registre professionnel fédéral ou cantonal (p. ex. Registre des professions médicales universitaires MedReg, Registre des professions de la psychologie PsyReg ou registre des professions de la santé NAREG), les données correspondantes de ce registre sont reprises.

1.2.3 Le processus de gestion des professionnels de la santé doit garantir que :
1.2.3.1 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées ;
1.2.3.2 l'accès au dossier électronique du patient fait l'objet de contrôles ;
1.2.3.3 les droits d'accès sont adaptés.

1.2.4 Le processus de sortie des professionnels de la santé doit garantir que :
1.2.4.1 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées ;
1.2.4.2 l'accès au dossier électronique du patient du patient est désactivé ;
1.2.4.3 les droits d'accès sont supprimés.

1.3 Gestion des auxiliaires des professionnels de la santé

1.3.1 Les communautés doivent prévoir des processus permettant d'enregistrer, de gérer et de supprimer les auxiliaires de professionnels de la santé dans un service interne de gestion des institutions de santé et des professionnels de la santé.

1.3.2 La gestion des auxiliaires est soumise, en dehors des exceptions énumérées ci-dessous, aux mêmes exigences que celles concernant l'entrée, la gestion et la sortie des professionnels de la santé. Font exception :
1.3.2.1 la garantie qu'il s'agit d'un professionnel de la santé au sens de l'art. 2, let. b, LDEP ;
1.3.2.2 l'actualisation du service de recherche des institutions de santé et des professionnels visé à l'art. 40 ODEP.

1.4 Identification et authentification (art. 8, let. d)

1.4.1 L'accès des professionnels de la santé au dossier électronique du patient ne peut se faire qu'à l'aide de moyens d'identification valables émis par un éditeur certifié selon l'art. 30.

1.4.2 Les communautés doivent garantir, aussi bien pour les professionnels de la santé que pour les auxiliaires, que leur identificateur univoque figurant dans le moyen d'identification et leur identité enregistrée dans la communauté soient reliées.

1.4.3 Les communautés doivent garantir que tous les systèmes techniques, comme par exemple les systèmes primaires ou les portails d'accès qui y sont reliés, utilisés par des professionnels de la santé ou des auxiliaires pour accéder au dossier électronique du patient :
1.4.3.1 supportent une procédure d'authentification forte conforme à l'état actuel de la technique, qui prévoit au moins deux facteurs d'authentification, comme condition préalable au traitement des données du dossier électronique du patient ;

1.4.3.2 mettent à disposition un terminal fiable pour communiquer de manière sûre avec le fournisseur de services d'identité (éditeur du moyen d'identification) conformément au ch. 3.2 (*P.TrustedCommunityEndpoint*) du profil de protection visé à l'art. 8 ODEP-DFI.

1.4.4 Les communautés sont tenues de reconnaître l'authentification correspondante suivie par d'autres communautés ou communautés de référence certifiées.

1.5 Gestion de groupes de professionnels de la santé (art. 8, let. a, c, e et f)

1.5.1 Les communautés sont responsables de la gestion des groupes de professionnels de la santé. Les directives et les procédures de gestion y afférentes doivent être définies, documentées, mises en œuvre et respectées.

1.5.2 Les directives et procédures doivent garantir que :
1.5.2.1 la composition des groupes est en tout temps identifiable pour les patients ;
1.5.2.2 les patients peuvent être informés lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé ;
1.5.2.3 la taille du groupe reste raisonnable ;
1.5.2.4 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées.

2 Tenue et transfert des données (art. 9 ODEP)

2.1 Destruction de données (al. 1, let. a et b)

2.1.1 Les communautés doivent prévoir des procédures qui garantissent que :
2.1.1.1 les documents saisis auprès d'elles dans le dossier électronique du patient par des professionnels de la santé sont détruits après dix ans;
2.1.1.2 en cas de suppression du dossier électronique du patient en vertu de l'art. 20, al. 1, ODEP, toutes les données sont détruites ; ce faisant, sont détruites au moins les données des systèmes de recherche suivants :
2.1.1.2.1 registre de documents ;
2.1.1.2.2 lieux de stockage des documents ;
2.1.1.2.3 index des patients ;
2.1.1.2.4 gestion des autorisations ;
2.1.1.2.5 portail d'accès.

2.2 Stockage des documents (al. 1, let. c)

2.2.1 Les communautés doivent prévoir des procédures qui garantissent que :
2.2.1.1 les documents du dossier électronique du patient sont enregistrées uniquement dans des lieux de stockage prévus à cet effet ;
2.2.1.2 seuls les formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI peuvent être enregistrées dans les lieux de stockage des documents ;
2.2.1.3 les données au format « Portable Document Format »(PDF) sont sauvegardées uniquement en version PDF/A-1 ou PDF/A-2 ;
2.2.1.4 l'Unicode UTF-8 est utilisé pour le codage des signes, dans les données ou documents consultables.

2.3 Gestion à la demande du patient (al. 2)

2.3.1.1 Les communautés doivent prévoir des procédures afin qu'à la demande du patient des données déterminées le concernant (al. 2) :

2.3.1.1.1 ne soient pas enregistrées dans son dossier électronique du patient ;

2.3.1.1.2 restent accessibles dix années supplémentaires en application de l'art. 9, al. 1, let. a, ODEP ;

2.3.1.1.3 soient détruites dans son dossier électronique du patient.

2.3.2 Ne sont pas assujetties aux prescriptions de l'art. 9, al. 1 et 2, ODEP les données historisées et les données figurant dans les systèmes primaires non interrogeables ainsi que dans les sauvegardes.

2.4 Mise en œuvre des niveaux de confidentialité (al. 3, let. a)

2.4.1 Les communautés doivent garantir que :

2.4.1.1 le patient peut attribuer les niveaux de confidentialité prévus à l'art. 1 ODEP aux données du dossier électronique du patient. A cet effet, elles sont tenues d'appliquer l'un des quatre niveaux de confidentialité aux données selon l'attribution réalisée par le patient via le portail d'accès de la communauté;

2.4.1.2 le niveau de confidentialité prévu à l'art. 1, al. 2, ODEP ou le niveau de confidentialité choisi par le patient en vertu de l'art. 3, let. c, ODEP est attribué aux nouvelles données enregistrées dans le dossier électronique du patient ;

2.4.1.3 les professionnels de la santé peuvent attribuer le niveau de confidentialité « données sensibles » aux données qu'ils enregistrent dans le dossier électronique du patient.

2.5 Respect des droits d'accès accordés (al. 3, let. a)

2.5.1.1 Les communautés doivent garantir qu'il est possible d'accéder aux données enregistrées dans leurs lieux de stockage de documents et dans leur registre de documents uniquement en conformité avec décisions d'accès accordés, qu'elles auront préalablement demandés à la communauté de référence.

2.6 Accès en cas d'urgence (al. 3, let. a)

2.6.1 Concernant l'accès en cas d'urgence médicale (art. 2, al. 5, ODEP), les communautés doivent garantir :

2.6.1.1 qu'une justification de l'accès en cas d'urgence est donnée au préalable ;

2.6.1.2 qu'un accès en cas d'urgence n'est possible qu'après une double confirmation, moyennant une action manuelle, non reproductible automatiquement, du professionnel de la santé ;

2.6.1.3 que le patient est aussitôt informé de l'accès en cas d'urgence (*art. 9, al. 5, EPDG*) ;

2.6.1.4 que l'information concernant l'accès effectué en cas d'urgence ne contient elle-même aucune donnée sensible si elle est transmise par un autre moyen que le dossier électronique du patient (p. ex. SMS, courriel, etc.).

2.7 Vérification de la gestion des autorisations (al. 3, let. a)

2.7.1 La gestion des autorisations doit permettre de vérifier l'exactitude des fonctionnalités et des évaluations des règles en place dans le cadre des scénarios de tests automatisés.

2.8 Métadonnées (let. c)

2.8.1 Les communautés doivent garantir que les métadonnées énumérées à l'annexe 4 ODEP-DFI sont utilisées pour la description des documents mis à disposition dans le dossier électronique du patient.

2.9 Profils d'intégration (art. 3, let. d)

Interface standard avec la base de données d'identification de la Centrale de compensation (CdC)

2.9.1 Les points d'accès des communautés doivent veiller à se servir des interfaces techniques à la base de donnée UPI proposées par la Centrale de compensation (CdC) pour l'attribution et l'utilisation du numéro d'identification du patient conformément au règlement de traitement de la CdC.

2.9.2 Outre l'utilisation techniquement correcte des interfaces, il faut également respecter les prescriptions organisationnelles énoncées dans le règlement de traitement de la CdC.

Profils d'intégration, adaptations nationales des profils d'intégration et profils d'intégration nationaux

2.9.3 Pour la transmission d'informations, les communautés doivent utiliser les profils d'intégration définis à l'art. 5, let. a à c, (profils d'intégration, adaptations nationales des profils d'intégration et profils d'intégration nationaux) de l'annexe 5 ODEP-DFI.

Acteurs et transactions des profils d'intégration – Communication intercommunautaire

2.9.4 Les acteurs IHE *Initiating Gateway* et *Responding Gateway* doivent supporter les transactions suivantes des profils d'intégration IHE XCA et IHE XCPD, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.4.1 Cross Gateway Query [ITI-38]
2.9.4.2 Cross Gateway Retrieve [ITI-39]
2.9.4.3 Cross Gateway Patient Discovery [ITI-55]
2.9.4.4 Patient Location Query [ITI-56]

Acteurs et transactions des profils d'intégration – Communication d'identités attestées

2.9.5 Le regroupement d'autres acteurs avec les acteurs IHE *X-Service Provider* et *X-Service User* du profil d'intégration IHE XUA est régi par les prescriptions des profils d'intégration nationaux et des adaptations nationales des profils selon l'annexe 5 ODEP-DFI et doit être effectué conformément à ces prescriptions.

2.9.6 Les acteurs IHE *X-Service Provider* et *X-Service User* doivent supporter la transaction suivante du profil d'intégration IHE XUA, dans la version selon l'annexe 5 ODEP-DFI :

2.9.6.1 Provide X-User Assertion [ITI-40]

Acteurs et transactions des profils d'intégration – Service de recherche des institutions de santé et des professionnels de la santé

2.9.7 Les acteurs IHE *Provider Information Consumer* et *Provider Information Source* doivent supporter les transactions suivantes du profil d'intégration IHE HPD, dans la version selon l'annexe 5 ODEP-DFI :

2.9.7.1 Provider Information Query [ITI-58]

2.9.7.2 Provider Information Feed [ITI-59]

Acteurs et transactions des profils d'intégration – Requête de documents

2.9.8 L'acteur IHE *Document Consumer* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.8.1 Registry Stored Query [ITI-18]

2.9.8.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mise à disposition de documents

2.9.9 L'acteur IHE *Document Source* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.9.1 Provide and Register Document Set-b [ITI-41]

2.9.9.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mutation des métadonnées de documents

2.9.10 L'acteur IHE *Document Administrator* doit supporter les transactions suivantes du profil d'intégration IHE XDS Metadata Update, dans la version selon l'annexe 5 ODEP-DFI :

2.9.10.1 Update Document Set [ITI-57]

2.9.10.2 Delete Document Set [ITI-62]

Acteurs et transactions des profils d'intégration – Registre de documents

2.9.11 L'acteur IHE *Document Registry* doit supporter les transactions suivantes des profils d'intégration XDS et IHE XDS Metadata Update, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.11.1 Register Document Set-b [ITI-42]

2.9.11.2 Register Stored Query [ITI-18]

2.9.11.3 Update Document Set [ITI-57]

2.9.11.4 Delete Document Set [ITI-62]

Acteurs et transactions des profils d'intégration – Lieux de stockage des documents

2.9.12 L'acteur IHE *Document Registry* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.12.1 Provide and Register Document Set-b [ITI-41]

2.9.12.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mise à disposition de données pour l'index des patients

2.9.13 L'acteur IHE *Patient Identity Source* doit supporter la transaction suivante des profils d'intégration PIX V3, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.13.1 Patient Identity Feed HL7 v3 [ITI-44]

Acteurs et transactions des profils d'intégration – Mise à disposition et requête de l'index des patients

2.9.14 Les acteurs IHE *Patient Demographics Supplier* et *Patient Demographics Consumer* doivent supporter la transaction suivante du profil d'intégration PDQV3, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.14.1 Patient Demographics Query V3 [ITI-47]

Acteurs et transactions des profils d'intégration – Gestion de l'index des patients

2.9.15 L'acteur IHE *Patient Identifier Cross-reference Manager* doit supporter les transactions suivantes du profil d'intégration IHE PIX V3, dans les versions selon l'annexe 5 ODEP-DFI.

2.9.15.1 Patient Identity Feed HL7 V3 [ITI-44]

2.9.15.2 PIX V3 Query [ITI-45]

2.9.15.3 PIX V3 Update Notification [ITI-46]

Acteurs et transactions des profils d'intégration – Authentification des systèmes et historisation des transactions IHE

2.9.16 Le regroupement d'autres acteurs avec les acteurs IHE *Secure Application* et *Secure Node Grouped with Any IHE Actor* du profil d'intégration IHE ATNA (ou de son adaptation nationale) est régi par les prescriptions des profils d'intégration IHE, des profils d'intégration nationaux et des adaptations des profils d'intégration et doit être effectué conformément à ces prescriptions.

2.9.17 Les acteurs *Secure Node grouped with Any IHE Actor* doivent supporter les transactions suivantes du profil d'intégration IHE ATNA et son adaptation nationale, selon l'annexe 5 ODEP-DFI :

2.9.17.1 Maintain Time [ITI-1]

2.9.17.2 Node Authentication [ITI-19]

2.9.18 Les acteurs *Secure Application* doivent supporter la transaction suivante du profil d'intégration IHE ATNA et son adaptation nationale, selon l'annexe 5 ODEP-DFI :

2.9.18.1 Record Audit Event [ITI-20]

Acteurs et transactions des profils d'intégration nationaux – Requête de la décision d'accès

2.9.19 Le regroupement d'autres acteurs avec l'acteur *Authorization Decision Consumer* du profil d'intégration national CH:ADR est régi par les prescriptions spécifiques de ce profil et doit être effectué conformément à ces prescriptions.

2.9.20 Les acteurs *Authorization Decision Provider*, *Authorization Decision Consumer* et *Policy Repository* doivent supporter les transactions du profil d'intégration national CH:ADR conformément aux spécifications techniques selon l'annexe 5 ODEP-DFI.

Acteurs et transactions des profils d'intégration nationaux – gestion de la configuration des autorisations

2.9.21 Les acteurs *Policy Repository* et *Policy Manager* doivent supporter les transactions du profil d'intégration national CH:PPQ conformément aux spécifications techniques selon l'annexe 5 ODEP-DFI.

Authentification avec des certificats valables

2.9.22 Les communautés doivent disposer d'un certificat électronique valable, acquis auprès d'un fournisseur de services de certification reconnu selon la loi fédérale du 19 décembre 2003 sur la signature électronique[1], pour :

2.9.22.1 l'authentification réciproque de leurs points d'accès ;

2.9.22.2 l'authentification réciproque entre leurs points d'accès et les services de recherche visés à l'art. 38, al. 1, let. a à c, ODEP ;

2.9.22.3 l'authentification réciproque entre leurs points d'accès et la base de données d'identification de la CdC.

2.9.23 Pour les échanges de données avec les services de recherche visés à l'art. 38, al. 1, let. a, ODEP, les communautés doivent utiliser les transactions du profil d'intégration IHE ATNA.

2.9.24 Pour les échanges de données avec la base de données d'identification de la CdC, les communautés doivent utiliser la plateforme d'échange de données SEDEX (*secure data exchange*) de l'Office fédéral de la statistique (OFS).

Cohérence de l'heure en Suisse (al. 6)

2.9.25 L'heure légale en Suisse diffusée par METAS est utilisée pour l'horodatage dans la communication et pour l'historisation. Les horloges de tous les systèmes de traitement de l'information pertinents doivent être synchronisées avec l'heure légale en Suisse.

2.10 Données historisées (al. 3, let. e)

Exigences concernant le système d'historisation

2.10.1 Tout traitement de données du dossier électronique du patient doit être historisé et horodaté.

2.10.2 Les données historisées doivent se limiter à ce qui est nécessaire et ne peuvent contenir aucune donnée médicale.

2.10.3 Les exigences suivantes sont applicables :

2.10.3.1 l'historisation prévue ne doit pas pouvoir être contournée ;

2.10.3.2 toute modification ultérieure des données historisées doit être impossible ;

2.10.3.3 lors de l'historisation, il faut distinguer les accès résultant de l'utilisation du dossier électronique du patient, qui doivent être visibles pour les patients, des accès technico-administratifs dans le cadre de l'exploitation du système ;

2.10.3.4 les administrateurs du système ne doivent pas pouvoir effacer ou désactiver l'historisation de leurs propres activités.

2.10.4 Des saisies dans l'historique consultables par le patient doivent être générées à chaque fois

[1] RS 943.03

2.10.4.1 lors du traitement des données suivantes :

2.10.4.1.1 documents dans les lieux de stockage ;
2.10.4.1.2 saisies dans le registre de documents ;
2.10.4.1.3 configuration de la gestion des autorisations ;
2.10.4.1.4 données de l'index des patients.

2.10.4.2 lors des événements suivants :

2.10.4.2.1 authentification dans le système (connexion/déconnexion) ;
2.10.4.2.2 tentatives d'accès, réussies ou infructueuses, au système ;
2.10.4.2.3 recherche du dossier électronique du patient ;
2.10.4.2.4 recherche de documents dans le dossier électronique du patient ;
2.10.4.2.5 accès d'urgence effectués ;
2.10.4.2.6 tentatives d'accès, réussies ou infructueuses, à des documents ;
2.10.4.2.7 enregistrement d'un nouveau moyen d'identification.

2.10.5 En cas d'accès à une fonction de recherche, l'historique doit contenir au moins :
2.10.5.1 les critères de recherche utilisés (p. ex. identificateurs utilisés, nom, date de naissance, etc.) ;
2.10.5.2 des indications sur le résultat de la recherche (p. ex. nombre de résultats) ;
2.10.5.3 les éventuelles actions consécutives (p. ex. choix d'un enregistrement dans une liste de résultats, impression, exportation de données).

2.10.6 Les données historisées doivent être conservées pendant dix ans.

2.10.7 La requête et la présentation des informations historisées en vue de leur consultation par le patient sont régies par les adaptations nationales du profil d'intégration IHE ATNA (Audit Trail Consumption) et le format d'échange technique pour les informations historisées prévu dans ces adaptations, selon l'annexe 5 ODEP-DFI.

2.11 Association du numéro d'identification du patient avec des documents (al. 3)

2.11.1 Les communautés doivent garantir que le numéro d'identification du patient fourni par la CdC n'est pas enregistré de manière durable dans les lieux de stockage des documents et les registres de documents et qu'il n'est pas relié directement et durablement avec des documents du patient dans les systèmes primaires.

3 Portail d’accès pour les professionnels de la santé (art. 10 ODEP)

3.1 Conformité aux dispositions légales

3.1.1 Le portail d’accès destiné aux professionnels de la santé doit satisfaire aux exigences légales en la matière.

3.2 Présentation

3.2.1 La présentation des interfaces utilisateurs dans le portail d’accès doit être correcte et exhaustive, et montrer clairement :

3.2.1.1 si c’est un professionnel de la santé ou le patient lui-même qui a mis à disposition le document ;

3.2.1.2 quels documents ont été mis à disposition par le professionnel de la santé qui y accède ;

3.2.1.3 quels documents ont été annulés ;

3.2.1.4 quelles versions d’un document sont éventuellement également disponibles.

3.3 Accessibilité

3.3.1 Le portail d’accès doit :

3.3.1.1 être conçu pour être pleinement accessible aux professionnels de la santé âgés ou ayant un handicap ;

3.3.1.2 remplir les conditions de conformité des directives pour l’accessibilité aux contenus Web (WCAG) 2.0 et atteindre le niveau de conformité AA.

3.4 Formats de fichiers : mise à disposition

3.4.1 Le portail d’accès doit :

3.4.1.1 permettre d’enregistrer les formats de fichiers autorisés en vertu de l’annexe 3 ODEP-DFI ;

3.4.1.2 convertir les autres fichiers dans un format autorisé, avant leur enregistrement dans un lieu de stockage.

3.5 Formats de fichiers : requête

3.5.1 Le portail d’accès doit :

3.5.1.1 permettre de faire une requête des formats de fichiers autorisés en vertu de l’annexe 3 ODEP-DFI ;

3.5.1.2 permettre de faire une requête des fichiers à enregistrer dans le système primaire (« download ») ;

3.5.1.3 prévoir le téléchargement non seulement un par un, mais aussi en masse (« bulk download ») des documents sélectionnés ;

3.5.1.4 afficher les données structurées sous une forme directement lisible par l’être humain, correcte et complète ;

3.5.1.5 permettre de télécharger les données structurées aussi bien dans leur format d’origine que sous une forme lisible par l’être humain.

3.5.2 La requête de documents pour affichage ou sauvegarde doit respecter les limites maximales définies en nombre de documents par unité de temps (« rate limits »), qui déclenchent, en cas de dépassement, des mesures adéquates de blocage ou de sécurité renforcée.

4 Protection et sécurité des données (art. 11 ODEP)

4.1 Exigences envers les tiers

4.1.1 Il incombe aux communautés d'assurer le respect des exigences formulées dans le présent chapitre (Protection et sécurité des données), y compris lorsqu'elles confient à des tiers (organisations d'exploitation) la réalisation de leurs prestations.

4.2 Système de gestion de la protection et de la sécurité des données (al. 1)

4.2.1 Les communautés doivent exploiter un système de gestion de la protection et de la sécurité des données tel que défini dans la norme ISO/IEC 27001:2013 qui :

4.2.1.1 définit expressément et maintient à jour toutes les exigences légales auxquelles doivent satisfaire les ensemble de données sensibles ;

4.2.1.2 détermine les mesures spécifiques nécessaires à leur exécution et les personnes chargées d'en assurer la surveillance ;

4.2.1.3 protège tous les enregistrements pertinents contre la perte, la destruction ou la falsification conformément aux exigences légales.

4.2.2 Le système de gestion de la protection et de la sécurité des données doit comprendre au moins :

4.2.2.1 un catalogue des risques, évalué par le responsable de la protection et de la sécurité des données (voir ch. 4.3) ;

4.2.2.2 un plan de traitement des risques ;

4.2.2.3 un inventaire à jour des moyens d'exploitation suivants (voir ch. 4.8) :

4.2.2.3.1 hardware

4.2.2.3.2 logiciels (softwares)

4.2.2.3.3 ensemble de données

4.2.2.3.4 organisation structurelle

4.2.2.3.5 processus

4.2.3 Les changements apportés aux moyens d'exploitation qui ont une incidence sur la sécurité doivent être analysés et documentés.

4.2.4 Un examen de gestion doit intervenir au moins une fois par an ; la direction de la communauté statue à cette occasion sur le catalogue des risques et sur le plan de traitement des risques.

4.3 Responsable de la protection et de la sécurité des données (al. 1, let. a)

4.3.1 Un responsable de la protection et de la sécurité des données est désigné pour s'occuper du système de gestion de la protection et de la sécurité des données. La communauté définit son cahier des charges. Il surveille le respect des prescriptions relatives à la protection et à la sécurité des données et :

4.3.1.1 il a les moyens d’exercer sa fonction en toute indépendance ;
4.3.1.2 il dispose des ressources nécessaires pour accomplir ses tâches.

4.4 Détection des incidents de sécurité (SIEM) (al. 1, let. b)

4.4.1 Les communautés doivent :
4.4.1.1 exploiter un système de détection et de gestion des incidents de sécurité (*security information and event management system* [SIEM]) qui surveille, en fonction des risques, tous les systèmes pertinents de l’infrastructure informatique interne de la communauté, qui détecte les anomalies et enregistre les événements pertinents pour la protection et la sécurité des données ;
4.4.1.2 protéger ces enregistrements contre toute modification ou suppression ;
4.4.1.3 garantir que les événements pertinents pour la protection et la sécurité des données sont traités de manière adéquate sur le plan organisationnel et technique, conformément au ch. 4.5.

4.4.2 Le SIEM doit être conçu en fonction des spécificités de la communauté. Il doit détecter et traiter au moins les schémas suivants :
4.4.2.1 cyberattaques lancées contre le portail d’accès ou le point d’accès de la communauté ;
4.4.2.2 hausse inhabituelle du nombre d’accès en écriture ou en lecture au lieu de stockage des documents, au registre de documents ou à l’index des patients, indiquant une utilisation abusive ou une attaque automatisée ;
4.4.2.3 mutations inhabituelles et critiques au niveau de gestion des autorisations, du système de gestion des identités et des accès (IAM) ou, le cas échéant, du service de gestion des institutions de santé et des professionnels de la santé interne à la communauté de manière analogue au service de recherche des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP (« HPD local »).

4.5 Gestion des incidents de sécurité (SIEM) (al. 1, let. b)

4.5.1 Les communautés doivent :
4.5.1.1 avoir défini des procédures formelles de déclaration immédiate et d’escalade en cas d’événement pertinents pour la protection et la sécurité des données (signalement à l’OFSP et à l’organisme de certification conformément à l’art. 11, al. 2, ODEP), ainsi qu’en exiger et en contrôler le respect ;
4.5.1.2 garantir que ces procédures et les obligations qui en découlent sont familières à tous les collaborateurs concernés de l’institution de santé ainsi qu’aux organisations d’exploitation.

4.5.2 Le SIEM :
4.5.2.1 englobe les processus de gestion des événements pertinents pour la sécurité ;
4.5.2.2 définit, en cas d’événement critique revêtant un niveau de gravité donné, au moins les processus d’urgence suivants visant à stopper immédiatement toute communication :
4.5.2.2.1 modalités et conditions requises pour isoler la communauté, par blocage de son point d’accès, du traitement des données du dossier électronique du patient ;
4.5.2.2.2 modalités et conditions requises pour isoler la communauté d’Internet ;
4.5.2.2.3 modalités et conditions requises pour isoler la communauté d’un système primaire auquel elle est reliée.

4.6 Protection contre les logiciels malveillants (al. 1, let. b)

4.6.1 Les communautés doivent :

4.6.1.1.1 veiller à définir et mettre en œuvre des mesures, des procédures et des systèmes de protection, de détection et de suppression des logiciels malveillants, ainsi que de surveillance des programmes auto-réplicatif (p. ex. virus) ;

4.6.1.1.2 s'assurer que les responsables des systèmes vérifient régulièrement que les programmes de détection et d'élimination des logiciels malveillants sont à jour.

4.7 Gestion des failles de sécurité (al. 1, let. b)

4.7.1 Les communautés doivent disposer d'une gestion des failles de sécurité qui s'informe en temps utile des défauts techniques des systèmes d'information utilisés, qui évalue la vulnérabilité de l'organisation en cas d'exploitation de telles failles et qui adopte des mesures adéquates pour faire face aux risques qui s'ensuivent.

4.7.2 Les mises à jour des logiciels destinées à éliminer les failles de sécurité (appelées « *patch* ») doivent être testées avant leur installation, et évaluées quant à leurs éventuels effets indésirables.

4.7.3 S'il n'existe pas encore de patch disponible pour éliminer une faille de sécurité, d'autres mesures de sécurité doivent être envisagées (p. ex. adaptation des contrôles d'accès ou limitation du trafic réseau).

4.8 Gestion des données et des systèmes sensibles (al. 1, let. c et d)

4.8.1 Les communautés doivent garantir que les institutions de santé affiliées disposent d'un règlement en vertu duquel seules peuvent être rendues accessibles dans le dossier électronique du patient les données contenues dans le dossier médical du patient qui sont pertinentes pour le traitement.

4.8.2 Les communautés doivent veiller à ce que toutes les données sensibles, tous les systèmes et tous les dispositifs sensibles liés du dossier électronique du patient soient clairement identifiés, classifiés et inventoriés.

4.8.3 L'inventaire sert à recenser et à gérer au moins les systèmes suivants :

4.8.3.1 lieux de stockage des documents ;

4.8.3.2 registre de documents ;

4.8.3.3 systèmes d'historisation ;

4.8.3.4 système de gestion des autorisations ;

4.8.3.5 système de gestion des identités et des accès (IAM) ;

4.8.3.6 index des patients ;

4.8.3.7 ensemble de données du système d'exploitation pertinent pour la protection et la sécurité des données (p. ex. historiques, sauvegardes, gestion des accès privilégiés des administrateurs de systèmes) ;

4.8.3.8 systèmes primaires avec les rôles (acteurs IHE) *Document Source* et *Document Consumer*. L'inventaire précise au moins, pour ces éléments :

4.8.3.8.1 le certificat client TLS, permettant d'activer la sécurité de la couche transport (TLS) de l'acteur IHE.

4.8.4 Chaque élément de l'inventaire doit :

4.8.4.1 être attribué à un propriétaire, qui en porte la responsabilité ;

4.8.4.2 mentionner la source originale des données ;
4.8.4.3 préciser la date de la dernière confirmation du responsable de la sécurité et de la protection des données.

4.8.5 Le responsable de la sécurité et de la protection des données doit réexaminer l'inventaire au moins une fois par an.

4.9 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 applicables aux terminaux (let. e)

4.9.1 Les communautés doivent prévoir des règles de protection et de sécurité des données pour les institutions de santé et leurs professionnels de la santé qui :
4.9.1.1 garantissent que les mesures de sécurité à respecter sont signalées aux institutions de santé (voir ch. 1.1.2.1) ;
4.9.1.2 astreignent les institutions de santé à informer leurs professionnels de la santé ayant accès au dossier électronique du patient sur leurs tâches, droits et devoirs liés au traitement des données dans le dossier électronique du patient ainsi que sur les risques et les mesures destinées à garantir la protection et la sécurité des données, et à obliger ces personnes au respect des mesures requises. L'obligation d'information couvre au moins les points suivants :
4.9.1.2.1 utilisation sûre des moyens d'identification et des données d'accès;
4.9.1.2.2 principes de description des documents à rendre accessibles avec des métadonnées ;
4.9.1.2.3 mesures en vue d'une utilisation sûre des terminaux (ordinateur, smartphone, tablette, etc.) ;
4.9.1.2.4 comportements à adopter pour se protéger contre les menaces auxquelles sont exposés les professionnels de la santé, p. ex. ingénierie sociale, « phishing », usage des supports de sauvegarde externes, etc. ;
4.9.1.2.5 services d'assistance et procédure pour la déclaration des incidents de protection et de sécurité des données ;
4.9.1.2.6 responsabilités en cas d'engagement d'auxiliaire.

Sécurité des terminaux utilisés par les professionnels de la santé

4.9.2 Les communautés astreignent les institutions de santé leur étant affiliées à garantir une configuration sûre des terminaux utilisés par les professionnels de la santé pour accéder au dossier électronique du patient.

4.9.3 La configuration des terminaux doit comprendre au moins :

4.9.3.1 l'utilisation d'un logiciel régulièrement actualisé contre les programmes malveillants ;
4.9.3.2 l'utilisation de systèmes de protection du réseau (p. ex. pare-feu) ;
4.9.3.3 une gestion restrictive des droits d'administrateur du système pour les utilisateurs normaux du système final ;
4.9.3.4 une actualisation régulière du système d'exploitation et des composants logiciels critiques pour la sécurité (p. ex. environnements de temps d'exécution comme Java, .Net, etc.).

4.10 Exigences relatives à la protection et à la sécurité des données imposées au personnel (al. 1, let. f)

4.10.1 Les communautés doivent disposer d'un recueil de normes qui fixe clairement, pour chaque utilisateur ou groupe d'utilisateurs, les règles de contrôle des accès et d'octroi des autorisations, et qui les mette en œuvre dans les systèmes de traitement d'information et dans les services réseau correspondants.

4.10.2 Les communautés doivent garantir que :

4.10.2.1 les personnes qui utilisent les données ou systèmes du dossier électronique du patient sont suffisamment compétentes pour les tâches prévues, assument leurs responsabilités et se montrent attentives à la protection et à la sécurité des données ;

4.10.2.2 des exigences sont formulées et communiquées pour l'usage des données d'authentification secrètes, comme les mots de passe, p. ex. ;

4.10.2.3 les personnes susceptibles d'avoir accès aux données du dossier électronique du patient sont soumises à un devoir de confidentialité analogue au secret médical ;

4.10.2.4 les processus définis pour la gestion du personnel sont mis en œuvre et respectés.

4.10.3 Les communautés doivent :

4.10.3.1 gérer une liste, visée par le responsable de la sécurité et de la protection des données de la communauté, de toutes les personnes qui ont accès aux données des patients – indépendamment de la gestion des droits prévue dans le dossier électronique du patient (« liste des personnes-clés ») ;

4.10.3.2 effectuer dans chaque cas un contrôle de sécurité relatif aux personnes (CSP) au sens de la loi sur l'armée ;

4.10.3.3 prévoir une procédure définie et officielle, afin de prononcer des mesures disciplinaires ou des sanctions à l'encontre des collaborateurs ayant contrevenu à la protection et à la sécurité des données.

4.11 Exigences relatives à la protection et à la sécurité des données imposées aux tiers (al. 1, let. f)

4.11.1 Les communautés doivent gérer une liste, visée par le responsable de la sécurité et de la protection des données de la communauté, de tous les fournisseurs et prestataires de services (« tiers ») qui, le cas échéant, accèdent aux données du dossier électronique du patient, les traitent, les enregistrent, les transmettent ou fournissent à cet effet des composants d'infrastructure informatique.

4.11.2 Les communautés doivent garantir qu'aucun accès aux données du dossier électronique du patient n'est effectué par des intermédiaires et que les tiers qui pourraient être amenés à accéder aux données du dossier électronique du patient dans le cadre de la fourniture de prestations ou de composants d'infrastructure informatique le font uniquement pour fournir leur prestation à la communauté, à l'exclusion de toute autre fin, et en aucun cas ne traitent ou ne transfèrent des données du dossier électronique du patient.

4.11.3 Toutes les exigences pertinentes de protection et de sécurité des données doivent être fixées en bonne et due forme avec les tiers et convenues dans des contrats de fourniture.

4.11.4 Les contrats de fourniture doivent fixer sans équivoque les obligations et responsabilités quant au respect des exigences pertinentes de protection et de sécurité des données.

4.11.5 Les contrats de fourniture doivent comprendre au moins les dispositions suivantes :

4.11.5.1 obligations du fournisseur de respecter les exigences pertinentes de protection et de

sécurité des données de la communauté, en cas d'utilisation ou de mise à disposition de produits technologiques de l'information et de la communication, de personnel et/ou de services ;

4.11.5.2 exigences et procédures pour la gestion des incidents de protection et de sécurité des données ;

4.11.5.3 indication des interlocuteurs pour toute question ou en cas d'incident dans le domaine de la protection et de la sécurité des données ;

4.11.5.4 droit de réexaminer régulièrement les processus des fournisseurs et les mesures de contrôle liées au contrat ;

4.11.5.5 obligation d'imposer le respect des exigences de protection et de sécurité des données de la communauté tout au long de la chaîne d'approvisionnement, au cas où les fournisseurs mandateraient des sous-traitants ;

4.11.5.6 prescriptions et mesures de contrôle applicables aux contrats de sous-traitance ;

4.11.5.7 devoir d'informer la communauté de toute modification des relations contractuelles avec les sous-traitants impliqués.

4.12 Surveillance et contrôle des prestations de service (al. 1, let. f)

4.12.1 Les communautés doivent régulièrement surveiller et contrôler les prestations de service, les rapports et la documentation fournis par des tiers et par d'éventuels sous-traitants, de façon à garantir que :

4.12.1.1 les conditions fixées par voie contractuelle pour la protection et la sécurité des données sont respectées ;

4.12.1.2 les incidents ou problèmes de protection et de sécurité des données sont traités de manière adéquate ;

4.12.1.3 les modifications apportées aux prestations de service sont soumises à une gestion dirigée du changement.

4.13 Obligation de déclarer les incidents de sécurité (al. 2)

4.13.1 Les communautés doivent avoir défini des procédures formelles de déclaration immédiate à l'organisme de certification et à l'OFSP en cas d'incident qui, selon le système de gestion de la protection et de la sécurité des données, est pertinent pour la sécurité, ainsi qu'en exiger et en contrôler le respect.

4.14 Sécurité d'exploitation (al. 3)

4.14.1 Les communautés doivent garantir que :

4.14.1.1 les accès privilégiés à l'environnement de production, p. ex. par les administrateurs de systèmes d'exploitation, de bases de données et d'applications :

4.14.1.1.1 reposent sur une authentification à deux facteurs ;

4.14.1.1.2 sont surveillés et historisés par un administrateur indépendant ;

4.14.1.1.3 ne permettent pas d'exporter les données de patients.

4.14.1.2 les accès externes par des tiers et des sous-traitants et en particulier les accès externes privilégiés à l'environnement de production, outre ce qui précède :

4.14.1.2.1 sont interdits ou comportent une protection adéquate ;

4.14.1.2.2 sont surveillés et historisés ;

4.14.1.2.3 ne sont autorisés que temporairement, et en cas de besoin.

4.14.1.3 les activités de développement, de test et de mise en service de nouveaux systèmes sont

documentées de façon compréhensible et se déroulent selon un processus contrôlé ;

4.14.1.4 des sauvegardes complètes sont faites et qu'elles sont cryptées ;

4.14.1.5 le matériel de cryptage pour la gestion des sauvegardes est soumis au principe du double contrôle ;

4.14.1.6 les sauvegardes sont horodatées ;

4.14.1.7 les sauvegardes sont enregistrées sur des dispositifs de stockage séparés, où leur intégrité est protégée, et que les dispositifs en question sont déconnectés du réseau après la copie ;

4.14.1.8 les procédures de restauration des systèmes sont convenablement documentées et régulièrement testées ;

4.14.1.9 les journaux techniques ne contiennent aucune donnée non cryptée de patients ;

4.14.1.10 les fichiers d'historisation sont horodatés et sauvegardés de manière à protéger leur intégrité ;

4.14.1.11 les supports de données de patients sont toujours éliminés correctement, et que toutes les données sont préalablement effacées ;

4.14.1.12 les horloges des systèmes sont synchronisées avec l'heure légale en Suisse.

4.14.2 L'environnement de production de l'infrastructure informatique du dossier électronique du patient interne à la communauté doit :

4.14.2.1 être isolé des autres environnements (p. ex. environnement de développement, de recette et de test) ;

4.14.2.2 adopter de nouveaux logiciels exclusivement lors de processus au déroulement contrôlé ;

4.14.2.3 faire l'objet de contrôles réguliers portant sur ses failles de sécurité ;

4.14.2.4 corriger les failles de sécurité détectées, lors d'un processus dûment contrôlé de gestion des patchs ;

4.14.2.5 être isolé des autres systèmes de l'exploitant par une propre segmentation réseau.

4.14.3 Outre le traitement des données du dossier électronique du patient par les professionnels de la santé ainsi que par les patients, il convient d'enregistrer au moins les informations suivantes à propos des événements survenant dans le cadre de l'exploitation du système :

4.14.3.1 date, heure et détails des événements-clés (p. ex. log in et log out) ;

4.14.3.2 tentatives d'accès, réussies ou infructueuses, au système ;

4.14.3.3 tentatives d'accès, réussies ou infructueuses, aux données ou aux documents ;

4.14.3.4 modifications apportées à la configuration du système ;

4.14.3.5 utilisation de droits d'accès privilégiés ;

4.14.3.6 adresses et protocoles réseau ;

4.14.3.7 activation et désactivation des systèmes de protection et d'authentification ;

4.14.3.8 modification des autorisations système et des accès ;

4.14.3.9 création, modification ou suppression de comptes d'utilisateurs (« accounts ») ;

4.14.3.10 copie ou impression d'informations sensibles.

4.15 Achat, développement et maintenance des systèmes (al. 3)

4.15.1 Les communautés doivent veiller à la protection et à la sécurité des données tout au long du cycle de vie des systèmes du dossier électronique du patient. A cet effet, il est nécessaire de définir, d'introduire et de respecter des processus formels de documentation, de spécification, de test, de contrôle-qualité et de mise en œuvre contrôlée pour :

4.15.1.1 l'introduction ou le développement de nouveaux systèmes ;

4.15.1.2 les modifications ou développements majeurs réalisés sur les systèmes existants ;

4.15.1.3 le changement des plateformes d'exploitation.

4.15.2 Il convient de démontrer au moins que dans chaque cycle de développement :

4.15.2.1 les exigences de sécurité sont définies dès le stade de la planification, au moyen d'une

analyse structurée des exigences, avant tout mandat de développement ou toute extension des systèmes d'information en place ;

4.15.2.2 les modifications apportées aux systèmes sont soumises à une procédure formelle documentée de contrôle des modifications ;

4.15.2.3 l'accès au code source des logiciels est limité, contrôlé et historisé ;

4.15.2.4 des lignes directrices en vue d'un développement en toute sécurité sont disponibles, y compris pour les activités de développement de systèmes qui ont été externalisées, et qu'elles sont utilisées et mises en œuvre durant le cycle de développement ;

4.15.2.5 les environnements de test ne comportent aucune donnée de patients ;

4.15.2.6 l'organisation d'exploitation supervise et contrôle le développement de logiciels en cas d'externalisation.

4.16 Cryptage de la communication (al. 3)

4.16.1 Les communautés veillent à ce que la confidentialité, l'authenticité et l'intégrité soient assurées lors de la transmission de données du dossier électronique du patient, au sein de la communauté ainsi qu'entre communautés, par des mesures cryptographiques adéquates et conformes à l'état actuel de la technique.

4.17 Enregistrement crypté des données (al. 3)

4.17.1 Les données sensibles du dossier électronique du patient doivent être sauvegardées sous une forme cryptée, à l'aide de mesures cryptographiques adéquates et conformes à l'état actuel de la technique, et de manière à ce que leur intégrité soit protégée.

4.18 Gestion des clés cryptographiques (al. 3)

4.18.1 Les communautés doivent garantir que :

4.18.1.1 les procédures de production, de distribution, d'activation, d'actualisation, de révocation ou de désactivation et de suppression des clés cryptographiques sont définies, mises en œuvre et contrôlées ;

4.18.1.2 les clés cryptographiques utilisées sont protégées contre toute modification ou perte ;

4.18.1.3 les clés secrètes et privées sont protégées contre toute utilisation ou divulgation non autorisée ;

4.18.1.4 les dispositifs de production, de sauvegarde et d'archivage des clés sont physiquement protégés.

4.19 Sécurité de la communication : gestion des réseaux (al. 3)

4.19.1 Les communautés doivent garantir que :

4.19.1.1 des directives sur la sécurité du réseau sont définies, respectées et contrôlées ;

4.19.1.2 les réseaux sont gérés de façon à ce que les données du dossier électronique du patient figurant dans les applications et les systèmes soient protégées contre les accès non autorisés ;

4.19.1.3 des règles sur les compétences en matière de gestion des réseaux à l'intérieur de la communauté sont définies, respectées et contrôlées.

4.20 Sécurité de la communication : services réseau (al. 3)

4.20.1 Les communautés doivent garantir, par une conception adéquate du réseau et de ses composants ainsi que par la structure adéquate et la configuration des services de réseau, que les données du dossier électronique du patient figurant dans les applications et les systèmes sont protégées :

4.20.1.1 en définissant des structures de réseau sûres et appropriées, en les représentant sur des plans de réseau et en les mettant en œuvre, tout en maintenant séparés des groupes dédiés de services d'information, d'utilisateurs et de systèmes d'information. En particulier, les pare-feu, les routeurs, les commutateurs réseaux, etc. et les solutions technologiques de services réseau doivent être configurés de façon à ce que :

4.20.1.1.1 seuls les systèmes faisant partie d'une communauté certifiée puissent accéder aux interfaces techniques de leur infrastructure informatique interne (« services IHE ») ;

4.20.1.1.2 les systèmes accédant à un service IHE par Internet s'authentifient auprès des services IHE au moyen du protocole TLS, en utilisant un certificat électronique valable. D'où la nécessité :

4.20.1.1.2.1 pour les portails ainsi que les *Responding Gateways*, d'utiliser au moins des certificats TLS publics à validation étendue (*extended validation, EV*) ;

4.20.1.1.2.2 pour d'autres services IHE, d'utiliser au moins des certificats TLS publics à validation étendue *EV* ou des certificats TLS uniquement valables au sein de la communauté.

4.20.1.1.3 tous les services IHE accessibles à partir d'Internet authentifient le système appelant via *TLS-Client-Authentication* ;

4.20.1.1.4 les *Responding Gateways* n'autorisent l'établissement d'une liaison que si le système appelant fait partie d'une communauté certifiée ;

4.20.1.1.5 tous les services IHE internes n'étant pas accessibles à partir d'Internet n'autorisent l'établissement d'une liaison que si le système appelant fait partie de la même communauté certifiée, s'il a été enregistré dans son inventaire et si le responsable de la protection et de la sécurité des données de la communauté l'a accepté ;

4.20.1.2 en documentant les procédures utilisées à cet effet (p. ex. certificats pour les serveurs clients, filtres d'adresses IP ou MAC).

4.20.2 Les communautés doivent :

4.20.2.1 séparer, au niveau du réseau, tous les systèmes de la communauté où sont enregistrées durablement des données du dossier électronique du patient (à savoir le registre de documents, leur lieu de stockage, la gestion des autorisations et l'index des patients) de tous les autres systèmes affichant un niveau de sécurité moins élevé ;

4.20.2.2 documenter les procédures utilisées à cet effet (p. ex. segmentation du réseau à l'aide de pare-feu).

4.20.3 Les communautés doivent notamment documenter le dispositif de sécurité implémenté pour assurer la protection de leur portail d'accès. La documentation comprend au moins :

4.20.3.1 la topologie du réseau et le justificatif concernant la « zone démilitarisée » (DMZ) ;

4.20.3.2 les versions et le niveau des logiciels utilisés pour le pare-feu applicatif Web (WAF) et le serveur Web ainsi que des composants logiciels employés par des tiers pertinents pour la sécurité ;

4.20.3.3 les mesures prévues pour la détection et le traitement des attaques et des failles de sécurité.

4.21 Expiration des sessions dans le réseau (« *session timeout* ») (al. 3)

4.21.1 Les sessions réseau inactives prennent fin après une période d'inactivité définie (20 minutes pour les patients, deux heures pour les professionnels de la santé).

4.21.2 L'authentification aux portails d'accès et sur les terminaux doit être répétée avant tout nouvel accès, faute d'interaction de l'utilisateur avec le dossier électronique du patient pendant 20 minutes dans le cas des patients, ou pendant deux heures pour les professionnels de la santé.

4.22 Système intermédiaire (al. 3)

4.22.1 Les éléments de l'infrastructure informatique interne à la communauté servant à transmettre les documents du dossier électronique du patient (notamment les points d'accès) ne peuvent pas les sauvegarder durablement.

4.23 Accessibilité (al. 3)

4.23.1 Les communautés doivent garantir que :

4.23.1.1 les services techniques destinés à l'utilisation du dossier électronique du patient sont à l'abri des interruptions, afin que de graves perturbations n'aient que des effets limités et prévus par contrat sur les systèmes de traitement de l'information et que la reprise en temps voulu de tous les services puisse être garantie ;

4.23.1.2 les services techniques exposés de l'infrastructure informatique affichent une disponibilité convenue contractuellement d'au moins 98 % sur la durée, et restent disponibles en cas de forte sollicitation ;

4.23.1.3 toutes les interfaces du dossier électronique du patient accessibles par Internet sont protégées contre les attaques DoS (par déni de service, *denial of service*) ;

4.23.1.4 des processus éprouvés leur permettent de réduire à un niveau acceptable, grâce à une combinaison de mesures de prévention et de remise en état, le temps de restauration après une perte d'information due, p. ex., à une catastrophe naturelle, à un accident, à une défaillance d'applications, de systèmes ou d'appareil, ou à des dommages intentionnels.

4.24 Dispositifs de stockage sous juridiction suisse (al. 4)

4.24.1 La communauté doit garantir que l'exploitation interne à la communauté d'un dispositif de stockage du dossier électronique du patient (lieux de stockage des documents, registre de documents et index des patients notamment) incombe à des personnes morales qui :

4.24.1.1 sont soumises au droit suisse ;

4.24.1.2 agissent exclusivement sous le régime du droit suisse pour accomplir leurs prestations ;

4.24.1.3 sont détenues en majorité en propriété suisse ;

4.24.1.4 fournissent toutes leurs prestations sur le territoire suisse.

5 Service d’assistance pour les professionnels de la santé (art. 12 ODEP)

5.1.1 Les communautés doivent proposer aux professionnels de la santé un service d’assistance (« *service desk* ») afin de les aider dans l’utilisation du dossier électronique du patient.

5.1.2 Les communautés doivent garantir au moins que :

5.1.2.1 les collaborateurs du « service desk » connaissent leurs tâches, leurs droits et devoirs, ainsi que les risques et les mesures propres à assurer la protection et la sécurité des données ;

5.1.2.2 les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis à un devoir de confidentialité analogue au secret médical ;

5.1.2.3 le consentement des collaborateurs à respecter les directives spécifiques de la communauté est documenté ;

5.1.2.4 l’accès à distance aux terminaux des professionnels de la santé pour des activités d’assistance n’est possible que si les intéressés en ont connaissance et ont donné leur consentement, et que l’accès est documenté automatiquement.

Exigences supplémentaires applicables aux communautés de référence

6 Information du patient (art. 14 ODEP)

6.1 L’information du patient selon l’art. 14 ODEP comprend au moins les points suivants :

6.1.1 Informations sur le but du dossier électronique du patient.

6.1.2 Informations sur les principes essentiels du traitement des données, dont au moins :

6.1.2.1 la perpétuation des documents dans les systèmes primaires et les lieux de stockage ;

6.1.2.2 le droit de révoquer son consentement présumé à la mise à disposition de documents en cas de traitement ainsi que d’obtenir la destruction de certains documents ;

6.1.2.3 les possibilités et fonctions du portail d’accès destiné aux patients ;

6.1.2.4 les possibilité de consulter les données historisées ;

6.1.2.5 les possibilité de désigner un représentant ;

6.1.2.6 les possibilité d’habiliter des professionnels de la santé à transmettre des droits d’accès, conformément à l’art. 3, let. h, ODEP.

6.1.3 Informations sur les conséquences du consentement et sur la possibilité de le révoquer, dont au moins :

6.1.3.1 le consentement libre ;

6.1.3.2 la possibilité de disposer d’un seul dossier de patient à la fois ;

6.1.3.3 les modalités de l’attribution et de l’utilisation du numéro d’identification du patient ;

6.1.3.4 la possibilité de changer de communauté de référence, avec les conséquences qui s’ensuivent pour la perpétuation des données, ainsi que pour les éventuels représentants et professionnels de la santé habilités ;

6.1.3.5 la possibilité de révoquer son consentement, sans aucune exigence de forme ou de justification de motif ;

6.1.3.6 la possibilité, après une révocation, d'ouvrir à nouveau un dossier électronique du patient auquel sera assigné un nouveau numéro d'identification du patient ;

6.1.4 Informations sur les possibilités d'octroi des droits d'accès selon les art. 1 à 3 ODEP, dont au moins :

6.1.4.1 la configuration des droits d'accès des professionnels de la santé et du niveau de confidentialité des documents suite à l'ouverture du dossier électronique du patient ;

6.1.4.2 les possibilités d'accorder des droits d'accès à des professionnels de la santé et à des groupes de professionnels de la santé, de les modifier et de les retier ;

6.1.4.3 les possibilité d'accès prévue pour les auxiliaires enregistrés par les professionnels de la santé, avec le niveau d'accès accordé au professionnel de la santé responsable ;

6.1.4.4 les possibilité d'accès prévue pour les professionnels de la santé dans des situations d'urgence médicale, et possibilité de limiter, étendre ou exclure un tel accès ;

6.1.4.5 les possibilité d'exclure de tout accès certains professionnels de la santé (liste d'exclusion) ;

6.1.4.6 les possibilité des collaborateurs du « service desk » d'accéder à distance aux terminaux du patient, moyennant son consentement y relatif.

6.1.5 Informations sur les mesures recommandées en matière de protection et de sécurité des données, dont au moins :

6.1.5.1 éventuels risques résiduels et mesures prévues en matière de protection et de sécurité des données ;

6.1.5.2 authentification sécurisée et usage des moyens d'identification et des données d'accès ;

6.1.5.3 principes de description des documents à mettre à disposition avec les métadonnées ;

6.1.5.4 mesures visant à une utilisation sûre des terminaux (ordinateur, smartphone, tablette, etc.) ;

6.1.5.5 recommandations de comportement à adopter pour protéger les patients contre les risques auxquels ils sont exposés, p. ex. l'ingénierie sociale, le « phishing », etc.

7 Consentement (art. 15 ODEP)

7.1 Les procédures de constitution du dossier électronique du patient doivent être définies, documentées, mises en œuvre et respectées.

7.1.1 La procédure d'ouverture d'un dossier électronique du patient doit garantir que le consentement du patient est recueilli avec sa signature.

8 Gestion (art. 16 ODEP)

8.1 Entrée et sortie de patients (al. 1, let. a)

8.1.1 Les processus de gestion des patients doivent être définis, documentés, mis en œuvre et respectés. Ils doivent garantir en particulier que :

8.1.1.1 les processus visant à garantir le respect des prescriptions énoncées aux let. b à e sont définis, documentés, mis en œuvre et respectés.

8.2 Identification des patients (al. 1, let. b)

8.2.1 Les processus d'identification des patients doivent être définis, documentés, mis en œuvre et respectés.

8.2.2 Ils doivent garantir que :

8.2.2.1 l'identification du patient (let. b)

8.2.2.1.1 se base sur le moyen d'identification d'un éditeur certifié selon l'art. 30 ODEP, ou

8.2.2.1.2 satisfait aux exigences de l'art. 23, al. 1, ODEP ;

8.2.2.2 un dossier électronique du patient est ouvert uniquement lorsqu'il est préalablement établi que la personne concernée n'en possède pas déjà un ;

8.2.2.3 le patient figure dans l'index des patients de la communauté de référence ;

8.2.2.4 le moyen d'identification du patient est lié de manière univoque à son dossier électronique du patient (let. c) ;

8.2.2.5 un numéro d'identification du patient est demandé conformément aux art. 5 et 6 ODEP et qu'il est correctement attribué au dossier électronique du patient à constituer (let. d) ;

8.2.2.6 les données démographiques de la banque de données d'identification de la Centrale de compensation (CdC) sont reprises dans l'index des patients de la communauté de référence (let. d).

8.3 Identification et authentification (al. 1, let. c)

8.3.1 L'accès des patients au dossier électronique du patient ne peut se faire qu'à l'aide de moyens d'identification valables, émis par un éditeur certifié selon l'art. 30 ODEP.

8.3.2 Les communautés doivent garantir qu'un lien fiable est établi entre l'identificateur univoque figurant dans le moyen d'identification des patients et de leurs éventuels représentants et l'identité de chacune de ces personnes enregistrée dans la communauté.

8.3.3 Les communautés doivent garantir que les portails d'accès :

8.3.3.1 supportent une procédure d'authentification forte conforme à l'état actuel de la technique, qui prévoit au moins deux facteurs d'authentification, comme condition préalable au traitement des données du dossier électronique du patient ;

8.3.3.2 mettent à disposition un terminal fiable pour communiquer de manière sûre avec le fournisseur de services d'identité (éditeur du moyen d'identification) conformément au ch. 3.2 (*P.TrustedCommunityEndpoint*) du profil de protection visé à l'art. 8 ODEP-DFI.

8.4 Changement de communauté de référence (let. e)

8.4.1 Les processus de changement de communauté de référence par le patient doivent être définis, documentés, mises en œuvre et respectés.

8.4.2 Le processus de changement de communauté de référence doit garantir que :
8.4.2.1 la configuration individuelle de gestion des autorisations peut être transférée à la nouvelle communauté de référence et reprise par elle. A cet effet, il faut respecter les prescriptions relatives au format technique du profil d'intégration national CH:PPQ, selon l'annexe 5 ODEP;
8.4.2.2 l'habilitation dont dispose un professionnel de la santé en vertu de l'art. 3, let. h ODEP est supprimée ;
8.4.2.3 les possibilités d'accès d'éventuels représentants d'un patient sont supprimées.

8.5 Respect des décisions d'accès visant le traitement de la configuration des autorisations (al. 2) : droits d'accès (art. 2, al. 1, OPED) et options du patient (art. 3 OPED)

8.5.1 Les communautés doivent garantir que le traitement de la configuration de la gestion des autorisations est effectué uniquement en conformité avec les décisions d'accès accordés.

8.6 Gestion des autorisations (al. 2) : droits d'accès (art. 2, al. 1 à 4, ODEP)

8.6.1 Les patients doivent avoir la possibilité d'accorder et d'adapter les droits d'accès aux professionnels de la santé aux groupes de professionnels de la santé. Les prescriptions de l'art. 2, al. 1 à 4, OPED doivent être respectées dans ce contexte.

8.6.2 Les prescriptions à respecter concernent notamment :
8.6.2.1 la possibilité d'accorder des droits d'accès à certains professionnels de la santé ou groupes de professionnels de la santé conformément à l'art. 1, al. 1, ODEP ;
8.6.2.2 la validité des droits d'accès accordés jusqu'à leur retrait par le patient ;
8.6.2.3 la mise en œuvre correcte des modifications des droits d'accès au sens de l'art. 2, al. 4, ODEP, liées aux entrées et sorties de professionnels de la santé dans un groupe, y c. la prise en compte des éventuels droits d'accès leur étant accordés à titre individuel.

8.7 Options du patient (art. 3 ODEP)

8.7.1 Les communautés de référence doivent garantir que :
8.7.1.1 les patients peuvent faire usage des options que leur donne l'art. 3 ODEP ;
8.7.1.2 les exigences énoncées à l'art. 3 sont mises en œuvre correctement.

8.7.2 Les exigences à respecter concernent la mise en œuvre correcte des options suivantes :
8.7.2.1 la possibilité d'accorder des droits d'accès limités dans le temps en vertu de l'art. 3, let. a, ODEP ;
8.7.2.2 la limitation, l'extension et l'exclusion des accès en cas d'urgence médicale ;
8.7.2.3 le choix du niveau de confidentialité attribué aux nouvelles données saisies dans le dossier électronique du patient ;
8.7.2.4 l'exclusion de certains professionnels de la santé de l'accès au dossier électronique du patient ;
8.7.2.5 la désactivation de l'information prévue à l'art. 8, let. f, ODEP ;
8.7.2.6 le choix que les professionnels de la santé qui intègrent un groupe n'obtiennent pas automatiquement les droits d'accès accordés à ce groupe ;

8.7.2.7 la désignation d’un représentant ;
8.7.2.8 l’habilitation de certains professionnels de la santé à transmettre leurs droits d’accès, conformément à l’art. 3, let. h, ODEP ;
8.7.2.9 l’évaluation correcte des règles en vigueur concernant les autorisations.

8.8 Représentation (art. 16, al. 1, let. c et al. 3, ODEP)

8.8.1 Les communautés de référence doivent offrir au patient la possibilité de désigner un représentant.

8.8.2 Le représentant doit accéder par son propre moyen d’identification, émis par un éditeur certifié selon l’art. 30, au dossier électronique du patient du patient qu’il représente.

8.8.3 La communauté de référence doit garantir que :
8.8.3.1 l’identification du représentant
8.8.3.1.1 repose sur le moyen d’identification d’un éditeur certifié selon l’art. 30, ou
8.8.3.1.2 correspond aux exigences de l’art. 23, al. 1, ODEP ;
8.8.3.2 les conditions juridiques liées à l’exercice du droit de représentation sont remplies ;
8.8.3.3 le représentant est informé, selon l’art. 14, ODEP, des principes essentiels du traitement des données, ainsi que des possibilités, des droits et obligations liés à l’utilisation du dossier électronique du patient ;
8.8.3.4 le moyen d’identification servant au représentant du patient, émis par un éditeur certifié selon l’art. 30, est relié de manière univoque et correcte au dossier électronique du patient du patient qu’il représente ;
8.8.3.5 l’accès du représentant au dossier électronique du patient se limite à la durée de sa fonction en tant que représentant.

9 Portail d’accès pour les patients (art. 17 ODEP)

9.1 Conformité aux dispositions légales

9.1.1 Le portail d’accès pour les patients doit satisfaire aux exigences juridiques en la matière.

9.1.2 Le portail d’accès doit permettre aux patients et aux professionnels de la santé habilités au sens de l’art. 3, let. h, ODEP de procéder à la gestion des autorisations, conformément aux prescriptions énoncées aux art. 1 à 3 ODEP.

9.1.3 Le portail d’accès doit notamment remplir les conditions-cadres suivantes quant à l’utilisation des données du patient :
9.1.3.1 les données mises à disposition par le patient dans des domaines ne relevant pas du dossier électronique du patient ne peuvent y être enregistrées que si le patient y a consenti ;
9.1.3.2 les données mises à disposition par le patient lui-même doivent toujours pouvoir être enregistrées directement dans le dossier électronique du patient, soit sans recours à une lieu de stockage intermédiaire ;
9.1.3.3 les données du dossier électronique du patient ne peuvent être transférées automatiquement et sans l’accord explicite du patient dans des domaines fonctionnels situés « en dehors » du dossier électronique du patient.

9.2 Présentation

9.2.1 La présentation sur l'interface utilisateur du portail d'accès doit être correcte et exhaustive, et montrer clairement :

9.2.1.1 si c'est un professionnel de la santé ou le patient lui-même qui a mis à disposition le document ;

9.2.1.2 les documents fournis par le patient lui-même ;

9.2.1.3 les documents annulés ;

9.2.1.4 les versions d'un document éventuellement également disponibles ;

9.2.1.5 les droits d'accès dont dispose chaque professionnel de la santé ;

9.2.1.6 le niveau de confidentialité de chaque document ;

9.2.1.7 utiliser pour la présentation des métadonnées prescrites selon l'annexe 3 ODEP-DFI sur l'interface utilisateurs du portail d'accès les termes et expressions préconisés pour la langue choisie (« defined terms »).

9.3 Accessibilité

9.3.1 Le portail d'accès doit :

9.3.1.1 être conçu pour être pleinement accessible aux patients agés ou ayant un handicap ;

9.3.1.2 remplir les conditions de conformité des directives pour l'accessibilité aux contenus Web (WCAG) 2.0 et atteindre le niveau de conformité AA.

9.4 Formats de fichiers : mise à disposition

9.4.1 Le portail d'accès doit :

9.4.1.1 permettre de mettre à disposition des formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI ;

9.4.1.2 convertir les fichiers différents dans un format autorisé, avant leur enregistrement dans un lieu de stockage.

9.5 Formats de fichiers : requête

9.5.1 Le portail d'accès doit :

9.5.1.1 permettre une requête des formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI ;

9.5.1.2 permettre une requête des fichiers à enregistrer dans le système primaire (« download ») ;

9.5.1.3 prévoir le téléchargement non seulement un par un, mais aussi en masse (« bulk download ») des documents sélectionnés ;

9.5.1.4 présenter les données structurées sous une forme directement lisible par l'être humain, correcte et complète ;

9.5.1.5 permettre de télécharger les données structurées aussi bien dans leur format d'origine que sous une forme directement lisible par l'être humain.

9.5.2 La requête de documents pour affichage ou enregistrement doit respecter les limites maximales définies par unité de temps (« rate limits »), qui déclenchent, en cas de dépassement, des mesures adéquates de blocage ou de sécurité renforcée.

9.6 Données historisées (let. c)

9.6.1 Les patients doivent avoir la possibilité de consulter, sous une forme lisible pour eux, les données historisées de toutes les communautés ou communautés de référence concernant leur dossier électronique du patient.

10 Disponibilité des données enregistrées par les patients (art. 18 ODEP)

10.1 Stockage des documents de patients

10.1.1 Les communautés de référence doivent mettre à disposition des lieux de stockage internes spéciaux pour les documents enregistrés par les patients eux-mêmes.

10.1.2 Les documents ne doivent être soumis à aucun délai d'effacement.

10.1.3 L'espace de stockage prévu à cet effet comporte au moins deux gigaoctets (Go).

10.1.4 Les communautés de référence doivent gérer les capacités de l'espace de stockage destiné aux documents enregistrés par les patients.

10.2 Archivage hors ligne des documents et des métadonnées

10.2.1 Les données concernant les patients et les métadonnées afférentes doivent pouvoir être mises à la disposition des patients dans un format électronique usuel interopérable.

10.2.2 Il faut prévoir des procédures permettant de déterminer si les données ont été modifiées après leur mise à disposition.

10.2.3 Les communautés de référence doivent garantir que les données qui sont mises à disposition une nouvelle fois dans le dossier électronique du patient n'ont pas été modifiées entre-temps.

11 Service d’assistance pour les patients (art. 19 ODEP)

11.1.1 Les communautés de référence doivent désigner un service d’assistance (« *service desk* ») destiné aux patients afin de les aider dans l’utilisation du dossier électronique du patient.

11.1.2 Les communautés de référence doivent garantir au moins que :

11.1.2.1 les collaborateurs du « service desk » connaissent leurs tâches, leurs droits et obligations ainsi que les risques et les mesures propres à assurer la protection et la sécurité des données ;

11.1.2.2 les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis à des obligations analogues au secret médical ;

11.1.2.3 le consentement des collaborateurs du « service desk » à respecter les directives spécifiques de la communauté est documenté ;

11.1.2.4 l’accès à distance aux terminaux des patients pour des activités d’assistance n’est possible que si les intéressés en ont connaissance et ont donné leur consentement, et que l’accès est documenté automatiquement.

12 Suppression du dossier électronique du patient (art. 20 ODEP)

12.1.1 Les communautés de référence doivent définir, documenter, mettre en œuvre et respecter des procédures régissant la suppression du dossier électronique du patient en cas de révocation, d’inutilisation ou de décès du patient.

12.2 Conditions de la suppression du dossier électronique du patient (al. 1)

12.2.1 La procédure de suppression du dossier électronique du patient doit être déclenchée lorsque :

12.2.1.1 le patient révoque son consentement à la tenue du dossier électronique du patient ;

12.2.1.2 personne n’a accédé au dossier électronique du patient durant dix ans ; ou

12.2.1.3 le patient est décédé.

12.3 Suppression du dossier électronique du patient (al. 2)

12.3.1 La procédure de suppression du dossier électronique du patient doit garantir que :

12.3.1.1 le dossier électronique du patient à supprimer est correctement identifié ;

12.3.1.2 tous les droits d’accès au dossier correspondant sont aussitôt retirés ;

12.3.1.3 toutes les données du dossier correspondant sont détruites en application de l’art. 9, al. 1, let. b, ODEP ;

12.3.1.4 toutes les communautés et communautés de référence sont informées dans un délai approprié de la suppression du dossier électronique du patient ;

12.3.1.5 la CdC est informée de la suppression du dossier électronique du patient dans un délai approprié.

12.4 Révocation du consentement à la tenue du dossier électronique du patient (al. 2, let. a)

12.4.1 En cas de révocation du consentement du patient à la tenue de son dossier électronique du patient, la procédure de suppression du dossier électronique du patient doit garantir, outre les points énoncés sous le ch. 12.3, que :

12.4.1.1 la révocation est documentée de façon juridiquement valable ;

12.4.1.2 la déclaration de révocation est conservée pendant dix ans.

12.4.2 Il doit être garanti que :

12.4.2.1 l'identification de la personne exerçant son droit de révocation

12.4.2.1.1 repose sur le moyen d'identification émis par un éditeur certifié selon l'art. 30, ou

12.4.2.1.2 correspond aux exigences de l'art. 23, al. 1, ODEP ;

12.4.2.2 la personne exerçant son droit de révocation a été informée des conséquences qui en découlent ;

12.5 Fermeture en cas d'inutilisation (al. 2, let. b)

12.5.1 En cas d'inutilisation, la procédure de suppression du dossier électronique du patient au sens de l'art. 20, al. 1, let. b, doit garantir, outre les points énoncés sous le ch. 12.3, que :

12.5.1.1 le patient est informé de la suppression de son dossier trois mois à l'avance.