Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

RS 816.111
Annexe 2 de l’ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient

Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence

Version 1: 22 mars 2017

Entrée en vigueur: 15 avril 2017

A. Exigences à l'égard des communautés

1 Identificateur d'objet et gestion (art. 9 ODEP)

1.1 Identificateur d'objet (art. 9, al. 1)

Les communautés doivent demander un identificateur d'objet (OID) pour elles-mêmes et pour les institutions de santé qui leur sont affiliées au service de recherche de l'OID visé à l'art. 42 ODEP.

1.2 Gestion des institutions de santé (art. 9, al. 2, let. a et d, ODEP)

1.2.1 Les communautés définissent les processus d'entrée, de gestion et de sortie des institutions de santé.

1.2.2 Le processus d'entrée des institutions de santé doit garantir:

a. qu'une demande pour obtenir un OID est faite auprès du service de recherche de l'OID visé à l'art. 42 ODEP;
b. que des accords sont conclus avec les institutions de santé concernant leurs tâches et leurs obligations, notamment en matière de protection et de sécurité des données;
c. que le processus « entrée de professionnels de la santé » (voir ch. 1.3.2) pour tous les professionnels de la santé rattachés à une institution de santé est déclenché;
d. que les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées;
e. que l'« inventaire de l'infrastructure informatique » visé au ch. 4.6 est actualisé.

1.2.3 Le processus de sortie des institutions de santé doit garantir:

a. que le processus « sortie de professionnels de la santé » (voir ch. 1.3.5) pour tous les professionnels de la santé rattachés à l'institution de santé sortante est déclenché;
b. que les données concernant le dossier électronique du patient restent accessibles si l'institution de santé sortante ne s'affilie à aucune autre communauté;
c. que l'« inventaire de l'infrastructure informatique » visé au ch. 4.6 est actualisé.

1.2.4 Les communautés sont tenues, pour les données qu'elles enregistrent dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP:

a. de désigner des personnes responsables;
b. de garantir que l'actualité et l'exactitude des données sont vérifiées régulièrement.

1.3 Gestion des professionnels de la santé (art. 9, al. 2, let. a à f, ODEP)

1.3.1 Les communautés définissent les processus d'entrée, de gestion et de sortie des professionnels de la santé.

1.3.2 Elles s'assurent que les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées.

1.3.3 Le processus d'entrée des professionnels de la santé doit garantir:

a. que le professionnel de la santé s'engage à respecter les directives spécifiques de la communauté relatives à l'utilisation du dossier électronique du patient;

b. que l'identification du professionnel de la santé repose sur un moyen d'identification émis par un éditeur certifié ou répond aux exigences de l'art. 24 ODEP;

c. que le professionnel de la santé en question répond à la définition énoncée à l'art. 2, let. b, LDEP;

d. que les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées;

e. que les données des professionnels de la santé qui pourraient figurer dans le registre professionnel fédéral ou cantonal sont reprises de ces registres.

1.3.4 Le processus de gestion des professionnels de la santé doit garantir:

a. que les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées;

b. que les conditions d'accès au dossier électronique du patient font l'objet de contrôles réguliers.

1.3.5 Le processus de sortie des professionnels de la santé doit garantir que:

a. les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées;

b. l'accès au dossier électronique du patient est désactivé pour le professionnel de la santé sortant.

1.4 Identification et authentification (art. 9, al. 2, let. e, ODEP)

1.4.1 Pour accéder au dossier électronique du patient, les professionnels de la santé doivent s'authentifier avec des moyens d'identification valables émis par un éditeur certifié selon l'art. 31 ODEP.

1.4.2 Les communautés doivent s'assurer que l'identificateur univoque visé à l'art. 25, al. 1, ODEP est relié au bon professionnel de la santé et à son numéro d'identification (GLN).

1.4.3 Les communautés doivent reconnaître l'authentification visée au ch. 1.4.1 suivie par d'autres communautés ou communautés de référence certifiées.

1.5 Gestion de groupes de professionnels de la santé (art. 9, al. 2, let. a, c, d et f, ODEP)

1.5.1 Les communautés sont responsables de la gestion des groupes de professionnels de la santé. Elles définissent le processus de gestion y afférent.

1.5.2 Le processus doit garantir:

a. qu'un OID fondé sur l'OID de l'institution de santé est attribué aux groupes de professionnels de la santé;

b. que les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP sont actualisées;

c. que les patients qui l'exigent sont informés lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé.

1.6 Gestion des auxiliaires des professionnels de la santé

1.6.1 Les communautés définissent des processus pour la gestion des auxiliaires de professionnels de la santé.

1.6.2 Pour accéder au dossier électronique du patient, les auxiliaires doivent s'authentifier avec un moyen d'identification valable, émis par un éditeur certifié selon l'art. 31 ODEP.

1.6.3 Les ch. 1.3 et 1.4.2 s'appliquent par analogie à la gestion des auxiliaires Fait exception l'actualisation du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41 ODEP.

2 Tenue et transfert des données (art. 10 ODEP)

2.1 Mise en œuvre des niveaux de confidentialité (art. 10, al. 1, let. a, ODEP)

Les communautés doivent garantir:

a. que le patient peut attribuer aux données médicales du dossier électronique les niveaux de confidentialité prévus à l'art. 1 ODEP;

b. que 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. 4, let. a, ODEP est attribué aux nouvelles données enregistrées dans le dossier électronique du patient;

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

2.2 Accès en cas d'urgence (art. 10, al. 1, let. a, ODEP)

Concernant l'accès dans des situations d'urgence médicale, les communautés doivent garantir:

a. que le professionnel de la santé qui accède aux données confirme l'accès selon une procédure empêchant efficacement toute utilisation abusive au moyen notamment d'un logiciel malveillant installé sur son terminal;

b. que le patient en est informé dans un délai approprié;

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

2.3 Mise en œuvre des décisions d'accès (art. 10, al. 1, let. a, ODEP)

2.3.1 Les communautés doivent garantir que l'accès aux données enregistrées dans leurs lieux de stockage des documents et dans leur registre des documents ne puisse intervenir qu'après obtention de la décision d'accès de la part de la communauté de référence du patient.

2.3.2 La gestion des autorisations doit permettre de vérifier l'exactitude des décisions d'accès dans le cadre de la procédure de certification, au moyen d'un système ad hoc.

2.4 Stockage des documents (art. 10, al. 1, let. b, et al. 3, ODEP)

Les communautés doivent garantir que:

a. 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;

b. dans les lieux de stockage des documents, les données médicales contenues dans le dossier électronique du patient sont enregistrées séparément des autres données de sorte qu'elles ne puissent pas être utilisées abusivement à d'autres fins;

c. seuls les types de média (« *MIME Media Type* ») autorisés en vertu au chiffre 2.8 de l'annexe 3 ODEP-DFI peuvent être enregistrés dans les lieux de stockage des documents;

d. les données au format « *Portable Document Format* » (PDF) sont sauvegardées uniquement en version PDF/A-1 ou PDF/A-2;

e. les données du type de média « *Portable Document Format* » (PDF) ne peuvent contenir ou télécharger de fichier exécutable, ou s'assurer d'une autre manière qu'elles ne contiennent pas de logiciel malveillant;

f. l'Unicode UTF-8 est utilisé pour le codage des signes, dans les données ou documents consultables.

2.5 Enregistrement et transfert cryptés des données (art. 10, al. 1, let. c, ODEP)

Les communautés doivent garantir que des mesures cryptographiques adéquates et conformes à l'état actuel de la technique:

a. assurent la confidentialité, l'authenticité et l'intégrité des données du dossier électronique du patient lors de chaque transmission;

b. permettent de sauvegarder les données sous forme cryptée et les protègent contre toute modification illicite ou inaperçue.

2.6 Destruction de données (art. 10, al. 1, let. d et e, ODEP)

Les communautés doivent prévoir des procédures qui garantissent:

a. que les données saisies auprès d'elles dans le dossier électronique du patient par des professionnels de la santé sont détruites après 20 ans. Le ch. 2.7., let. b, demeure réservé;

b. en cas de suppression du dossier électronique du patient en vertu de l'art. 21 ODEP, que toutes les données qui y sont contenues sont détruites. Il y a en particulier lieu de détruire les données correspondantes dans les éléments de l'infrastructure informatique mentionnés au ch. 4.6.2., let. a à i, de l'« inventaire de l'infrastructure informatique » et d'éliminer le numéro d'identification du patient de tous les systèmes.

2.7 Options offertes au patient (art. 10, al. 2, ODEP)

Les communautés doivent prévoir des procédures techniques et organisationnelles afin qu'à la demande du patient des données déterminées le concernant:

a. ne soient pas enregistrées dans son dossier électronique;

b. soient exclues de la destruction visée à l'art. 10, al. 1, let. d, ODEP;

c. soient détruites de son dossier électronique.

2.8 Métadonnées (art. 10, al. 3, let. a, ODEP)

Les communautés doivent garantir que les métadonnées sont utilisées selon l'annexe 3 ODEP-DFI.

2.9 Prescriptions relatives à la gestion et au transfert des données du dossier électronique du patient (art. 10, al. 3, let. c, ODEP)

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 utiliser des interfaces techniques à la base de données d'identification proposées par la 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 IHE, adaptations nationales des profils d'intégration IHE et profils d'intégration nationaux

2.9.3 Pour la transmission d'informations, les communautés doivent utiliser les profils d'intégration IHE, leurs adaptations nationales et les profils d'intégration nationaux tels que définis à l'annexe 5 ODEP-DFI.

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 visées à l'annexe 5 ODEP-DFI:

a. Cross Gateway Query [ITI-38];
b. Cross Gateway Retrieve [ITI-39];
c. Cross Gateway Patient Discovery [ITI-55].

2.9.5 Les acteurs IHE *Initiating Imaging Gateway* et *Responding Imaging Gateway* doivent supporter la transaction *Cross Gateway Retrieve Image Document Set* [RAD-75] du profil d'intégration IHE XCA-I dans la version visée à l'annexe 5 ODEP-DFI.

Communication d'identités attestées

2.9.6 Les acteurs IHE *X-Service Provider* et *X-Service User* du profil d'intégration IHE XUA sont regroupés avec d'autres acteurs IHE conformément aux prescriptions des profils d'intégration nationaux et aux adaptations des profils d'intégration visées à l'annexe 5 ODEP-DFI.

2.9.7 Les acteurs IHE *X-Service Provider* et *X-Service User* doivent supporter les transactions suivantes du profil d'intégration IHE XUA, dans la version visée à l'annexe 5 ODEP-DFI:

a. Authenticate User;
b. Get X-User Assertion;
c. Provide X-User Assertion [ITI-40].

Service de recherche des institutions de santé et des professionnels de la santé

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

a. Provider Information Query [ITI-58];
b. Provider Information Feed [ITI-59].
c. Provider Information Delta Download (CH:PIDD).

Requête de données médicales

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

a. Registry Stored Query [ITI-18];
b. Retrieve Document Set [ITI-43].

2.9.10 L'acteur IHE *Image Document Consumer* doit supporter les transactions suivantes du profil d'intégration IHE XDS.b, dans la version visée à l'annexe 5 ODEP-DFI:

a. WADO Retrieve [RAD-55];
b. Retrieve Imaging Document Set [RAD-69].

Mise à disposition de données médicales

2.9.11 L'acteur IHE *Document Source* doit supporter la transaction *Provide and Register Document Set-b* [ITI-41] du profil d'intégration IHE XDS.b, dans la version visée à l'annexe 5 ODEP-DFI:

2.9.12 L'acteur IHE *On-Demand Document Source* doit supporter la transaction *Register On-Demand Document Entry* [ITI-61] du profil d'intégration IHE XDS.b, dans la version selon l'annexe 5 ODEP-DFI:

Mutation des métadonnées de données médicales

2.9.13 L'acteur IHE *Document Administrato*r doit supporter les transactions suivantes du profil d'intégration IHE XDS Metadata Update, dans la version visée à l'annexe 5 ODEP-DFI:

a. Update Document Set [ITI-57];
b. Delete Document Set [ITI-62].

Registre de documents

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

a. Register Document Set-b [ITI-42];
b. Register Stored Query [ITI-18];
c. Update Document Set [ITI-57];
d. Register On-Demand Document Entry [ITI-61];
e. Delete Document Set [ITI-62];

f. Patient Identity Feed HL7 V3 [ITI-44].

Lieux de stockage des documents

2.9.15 L'acteur IHE *Document Repository* doit supporter les transactions suivantes du profil d'intégration IHE XDS.b, dans la version visée à l'annexe 5 ODEP-DFI:

a. Provide and Register Document Set-b [ITI-41];
b. Retrieve Document Set [ITI-43].

2.9.16 L'acteur IHE *Portable Media Creator* doit supporter la transaction *Distribute Document Set on Media* [ITI-32] du profil d'intégration XDM, dans la version visée à l'annexe 5 ODEP-DFI:

Mise à disposition de données pour l'index des patients

2.9.17 L'acteur IHE *Patient Identity Source* doit supporter la transaction *Patient Identity Feed HL7 v3* [ITI-44] du profil d'intégration PIX V3, dans la version visée à l'annexe 5 ODEP-DFI.

Mise à disposition et requête de l'index des patients

2.9.18 Les acteurs IHE *Patient Demographics Supplier* et *Patient Demographics Consumer* doivent supporter la transaction *Patient Demographics Query V3* [ITI-47] du profil d'intégration PDQV3, dans la version visée à l'annexe 5 ODEP-DFI.

Gestion de l'index des patients

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

a. Patient Identity Feed HL7 V3 [ITI-44];
b. PIX V3 Query [ITI-45];
c. PIX V3 Update Notification [ITI-46].

Authentification des systèmes et historisation des transactions IHE

2.9.20 Les acteurs IHE *Secure Application* et *Secure Node* du profil d'intégration IHE ATNA (ou leurs adaptations nationales) sont regroupés avec d'autres acteurs IHE conformément aux prescriptions des profils d'intégration IHE, des profils d'intégration nationaux et des adaptations des profils d'intégration visées à l'annexe 5 ODEP-DFI.

2.9.21 Tous les acteurs IHE ayant le rôle *Secure Node* visé au ch. 2.9.20 doivent supporter les transactions suivantes du profil d'intégration IHE ATNA et de son adaptation nationale visées à l'annexe 5 ODEP-DFI:

a. Maintain Time [ITI-1];
b. Node Authentication [ITI-19];
c. Record Audit Event [ITI-20].

2.9.22 Les acteurs IHE *Secure Application* doivent supporter les transactions suivantes du profil d'intégration IHE ATNA et de son adaptation nationale visées à l'annexe 5 ODEP-DFI:

a. Maintain Time [ITI-1];

b. Record Audit Event [ITI-20].

Requête de la décision d'accès

2.9.23 L'acteur IHE *Authorization Decision Consumer* du profil d'intégration national CH:ADR est regroupé avec d'autres acteurs IHE conformément aux prescriptions du profil d'intégration national CH:ADR visées à l'annexe 5 ODEP-DFI.

2.9.24 Les acteurs IHE *Authorization Decision Provider*, *Authorization Decision Consumer* et *Policy Repository* doivent supporter la transaction *Authorization Decision Request* [CH:ADR] du profil d'intégration national CH:ADR visée à l'annexe 5 ODEP-DFI.

Gestion de la configuration des autorisations

2.9.25 Les acteurs IHE *Policy Repository* et *Policy Manager* doivent supporter la transaction *Privacy Policy Query* [CH:PPQ] du profil d'intégration national CH:PPQ visée à l'annexe 5 ODEP-DFI.

Authentification avec des certificats valables

2.9.26 Les communautés doivent disposer d'un certificat électronique valable, acquis auprès d'un fournisseur de services de certification reconnu selon la loi fédérale du 18 mars 2016 sur la signature électronique (SCSE; RS 943.03), pour:

a. l'authentification réciproque de leurs points d'accès;
b. l'authentification réciproque entre leurs points d'accès et les services de recherche visés à l'art. 39, let. a à c, ODEP;
c. l'authentification réciproque entre leurs points d'accès et la base de données d'identification de la CdC.

Échange de données avec les services de recherche visés à l'art. 39

2.9.27 Pour l'échange de données avec les services de recherche visés à l'art. 39, let. a et c, ODEP, les communautés doivent utiliser les transactions suivantes du profil d'intégration IHE SVS, selon l'annexe 5 ODEP-DFI:

a. Retrieve Value Set [ITI-48];
b. Retrieve Multiple Value Sets [ITI-60].

2.9.28 Pour l'échange de données avec les services de recherche visés à l'art. 39, let. a à c, ODEP, les communautés doivent utiliser les transactions suivantes du profil d'intégration IHE ATNA, selon l'annexe 5 ODEP-DFI:

a. Maintain Time [ITI-1];
b. Authenticate Node [ITI-19];
c. Record Audit Event [ITI-20].

2.9.29 Pour l'échange 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).

Heure déterminante

2.9.30 L'heure légale en Suisse diffusée par METAS est utilisée pour l'horodatage dans la communication et pour l'historisation (cf. ch. 2.9.21 et 2.9.22).

2.10 Données historisées (art. 10, al. 3, let. d, ODEP)

2.10.1 Tout traitement de données du dossier électronique du patient doit être historisé et horodaté au moyen d'une estampille temporelle actuelle.

2.10.2 Le traitement des données suivantes doit être historisé pour les tentatives d'accès réussies ou infructueuses:

a. données médicales dans les lieux de stockage;
b. saisies dans le registre de documents;
c. configuration de la gestion des autorisations;
d. données de l'index des patients.

2.10.3 Doivent également être historisés les événements suivants:

a. authentification dans le système (connexion/déconnexion);
b. transactions intercommunautaires via les points d'accès des communautés;
c. recherche d'un patient;
d. recherche de données médicales contenues dans un dossier électronique du patient;
e. accès d'urgence à un dossier électronique du patient;
f. accès et tentatives d'accès à des données médicales figurant dans un dossier électronique du patient.

2.10.4 Dans tous les cas, les entrées historisées doivent comprendre au moins:

a. l'événement lui-même (« *Event Identification* ») et le contexte dans lequel il s'est produit (exploitation normale, accès d'urgence, usage de droits d'accès spéciaux privilégiés);
b. le moment où l'événement s'est produit (« *Event Timestamp* »);
c. l'auteur de l'événement (« *Active Participant Identification* »);
d. le lieu de l'événement (« *Network Access Point Identification* »);
e. la cause de l'événement (« *Audit Source Identification* »);
f. les données concernées (« *Participant Object Identification* »);
g. le résultat de l'événement (« *Event Outcome Indicator* »).

2.10.5 Lors d'une recherche, les éléments suivants au moins doivent être historisés:

a. les critères de la recherche;
b. le résultat de la recherche, notamment le nombre de résultats;
c. les actions consécutives, notamment le choix d'un enregistrement dans une liste de résultats ou l'exportation des données.

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

2.10.7 L'historisation doit remplir les exigences suivantes:

a. un texte lisible par l'être humain, désignant nommément l'entité référencée au moment de l'historisation doit être historisé en sus des identificateurs;
b. les historisations prescrites ne doivent pas pouvoir être omises;

c. les modifications ultérieures des données historisées doivent être reconnaissables et compréhensibles;
d. lors de l'historisation, il faut distinguer les accès résultant de l'utilisation du dossier électronique du patient des accès technico-administratifs effectués dans le cadre de l'exploitation du système;
e. les administrateurs du système ne doivent pas pouvoir effacer ou désactiver l'historisation de leurs propres activités.

2.10.8 Les données historisées selon le ch. 2.10.1 à 2.10.3 doivent être détruites après 10 ans.

2.10.9 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*) selon l'annexe 5 ODEP-DFI.

2.11 Association du numéro d'identification du patient avec des données médicales (art. 10, al. 3, ODEP)

Les communautés doivent garantir que le numéro d'identification du patient fourni par la CdC n'est pas enregistré dans les lieux de stockage des documents et les registres de documents.

3 Portail d'accès pour les professionnels de la santé (art. 11 ODEP)

3.1 Présentation

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

a. si c'est un professionnel de la santé ou le patient lui-même qui a mis à disposition les données médicales;
b. quelles données médicales ont été mises à disposition par le professionnel de la santé qui y accède;
c. quelles données médicales ont été annulées;
d. quelles versions d'un document sont disponibles.

3.2 Accessibilité

Le portail d'accès doit remplir les conditions de conformité des directives pour l'accessibilité aux contenus Web (WCAG) 2.0 et atteindre au moins le niveau de conformité AA.

3.3 Requête de données médicales et types de média

Le portail d'accès doit:

a. supporter les types de media visés au chiffre 2.8 de l'annexe 3 ODEP-DFI;
b. supporter l'importation de données médicales et la requête de données médicales à enregistrer dans le système primaire de l'institution de santé;

c. offrir la possibilité d'importer ou de télécharger une ou plusieurs données médicales à la fois;

d. afficher de façon correcte et complète des données structurées et lisibles par l'être humain;

e. supporter le téléchargement de données structurées aussi bien dans leur format d'origine que sous une forme lisible par l'être humain;

f. prévoir, pour la requête de données médicales destinées à être visualisés ou enregistrées, des limites maximales admises définies en nombre de données médicales par unité de temps, avec activation de mesures adéquates de blocage ou de sécurité renforcée en cas de dépassement.

4 Protection et sécurité des données (art. 12 ODEP)

4.1 Exigences envers les tiers

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

4.2 Système de gestion de la protection et de la sécurité des données (art. 12, al. 1, ODEP)

4.2.1 Les communautés doivent exploiter un système de gestion de la protection et de la sécurité des données qui est adapté aux risques et qui

a. définit des mesures appropriées, en particulier des directives, des processus, des procédures, des structures organisationnelles et des fonctions relatives aux logiciels et au matériel en vue de remplir les exigences correspondant aux dispositions mentionnées dans le présent document;

b. établit, pour des fonctions définies, les responsabilités générales et spécifiques relatives à la gestion de la protection et de la sécurité des données et désigne les personnes compétentes en la matière;

c. protège tous les enregistrements pertinents contre la perte, la destruction ou la falsification dans le respect des exigences légales.

4.2.2 Toutes les institutions de santé et leurs professionnels de la santé au sein de la communauté doivent avoir connaissance de l'existence du système de gestion de la protection et de la sécurité des données.

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

a. un catalogue des risques, évalué par le responsable de la protection et de la sécurité des données (voir ch. 4.11);

b. un plan de traitement des risques;

c. un inventaire à jour des moyens d'exploitation de la communauté pertinents pour l'évaluation et le traitement des risques. Celui-ci comprend en particulier:

i. les données du dossier électronique du patient et les processus nécessaires à leur traitement (objets de protection primaires);
ii. les systèmes, les infrastructures, les applications, les installations, les structures organisationnelles, les personnes et les processus dont la protection des objets primaires dépend.

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

4.2.5 Les communautés sont tenues de mettre à jour et de vérifier au moins une fois par an le catalogue des risques et le plan de traitement des risques.

4.3 Détection et gestion des incidents de sécurité (art. 12, al. 1, let. a, ODEP)

4.3.1 Les communautés doivent mettre en place, exploiter et améliorer en permanence des procédures techniques et organisationnelles de détection et de gestion des incidents de sécurité qui:

a. surveillent, en fonction des risques, au moins les éléments enregistrés comme pertinents en termes de risques dans l'« inventaire de l'infrastructure informatique » selon le ch. 4.6;
b. détectent les anomalies dans le système;
c. enregistrent les événements pertinents pour la protection et la sécurité des données de manière à les protéger des modifications illicites ou inaperçues.

4.3.2 Les procédures relatives à la détection, à l'analyse et au compte rendu des incidents de sécurité doivent être définies en fonction de chaque communauté, être adaptées au risque et détecter et traiter au moins les schémas suivants:

a. cyberattaques lancées contre des portails d'accès ou le point d'accès de la communauté;
b. schémas inhabituels 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;
c. 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.

4.3.3 S'agissant des mesures décrites au ch. 4.3.1, les communautés doivent prévoir:

a. des procédures de déclaration immédiate au service compétent de la communauté et à l'OFSP (art. 12, al. 3, ODEP) en cas d'événement pertinents pour la protection et la sécurité des données;
b. des processus pour réagir rapidement à des événements et traiter les éléments qui menacent la protection et la sécurité des données.
c. des processus d'urgence afin d'atténuer les effets néfastes en cas d'événements critiques pour la sécurité d'un certain niveau. En particulier, elles doivent déterminer de quelle manière et à quelles conditions il convient d'isoler, de l'intérieur ou de l'extérieur, les systèmes de la communauté critiques pour la sécurité des accès représentant une menace.

4.4 Gestion des failles de sécurité (art. 12, al. 1, let. a, ODEP)

4.4.1 Les communautés doivent disposer d'une gestion des failles de sécurité qui recueille en temps utile des informations sur les défauts techniques des moyens informatiques utilisés, qui évalue la vulnérabilité de la communauté en cas d'exploitation de telles failles et qui adopte des mesures adéquates pour faire face aux risques encourus.

4.4.2 S'il n'existe pas encore de de correctif du logiciel (*patch*) pour éliminer les failles de sécurité (patch), d'autres mesures de sécurité doivent être envisagées et, si possible, mises en œuvre.

4.5 Protection contre les logiciels malveillants (art. 12, al. 1, let. a, ODEP)

Les communautés doivent:

a. prendre les mesures visant à protéger notamment les éléments sensibles de l'infrastructure informatique mentionnés aux ch. 4.6.2, let. a à i et k, contre les logiciels malveillants, en particulier celles qui permettent de détecter et de supprimer de tels logiciels;

b. vérifier régulièrement que les logiciels utilisés pour détecter et supprimer les logiciels malveillants sont à jour.

4.6 Gestion des moyens informatiques et des recueils de données sensibles (« inventaire de l'infrastructure informatique ») (art. 12, al. 1, let. b, ODEP)

4.6.1 Les communautés doivent veiller à ce que toutes les données sensibles, tous les systèmes et tous les dispositifs sensibles liés au dossier électronique du patient sont identifiés de manière univoque, classifiés, enregistrés dans un « inventaire de l'infrastructure informatique » et maintenus à jour.

4.6.2 L'« inventaire de l'infrastructure informatique » doit recenser et gérer au moins les éléments suivants de l'infrastructure informatique de la communauté pour le dossier électronique du patient:

a. points d'accès (acteurs IHE *Initiating Gateway*, *Responding Gateway*);

b. lieux de stockage des documents (acteur IHE *Document Repository*);

c. registre de documents (acteur IHE *Document Register*);

d. systèmes et stockages de données pour les données historisées que les patients peuvent consulter (acteurs IHE *Audit Repository, Audit Record Repository*);

e. systèmes de gestion des autorisations (acteurs IHE *Policy Repository, Authorization* Decision Provider);

f. s'ils existent, systèmes du service de recherche des institutions de santé et des professionnels de la santé internes à la communauté (acteurs IHE *Provider Information Directory*, *Provider Information Source*, *Provider Information Consumer*);

g. système de gestion des identités et des accès (IAM);

h. index des patients (acteurs IHE *Patient Demographics Supplier, Patient Identifier Cross-reference Manager, Patient Identity Source*);

i. portails d'accès pour les professionnels de la santé ou les patients;

j. systèmes primaires raccordés dans la mesure où ils effectuent au moins l'un des acteurs IHE suivants ou des fonctionnalités analogues: *Document Source, Document Consumer, Policy Manager, Provider Information Source, Provider Information Consumer, Patient Demographics Consumer, Patient Identifier Cross-reference*

Consumer, Patient Identity Source, X-Service User, Document Audit Consumer;

k. systèmes, applications et ensembles de données du système d'exploitation, tels que ceux pour les données historisées, les sauvegardes et la gestion des accès pour les administrateurs du système.

4.6.3 Pour les systèmes primaires visés au ch. 4.6.2, let. i, l'« inventaire de l'infrastructure informatique » doit en outre au moins comprendre le certificat client TLS, permettant d'activer la sécurité de la couche transport (TLS) de l'acteur IHE concerné ou de l'élément de l'infrastructure informatique en question.

4.6.4 Chaque élément de l'inventaire doit être attribué à un propriétaire, qui en porte la responsabilité.

4.6.5 Le responsable de la sécurité et de la protection des données doit réexaminer l'« inventaire de l'infrastructure informatique » au moins une fois par an.

4.7 Prescriptions relatives à la protection et à la sécurité des données imposées aux institutions de santé affiliées ainsi qu'à leurs professionnels de la santé et à leurs terminaux (art. 12, al. 1, let. c, ODEP)

4.7.1 Les communautés doivent:

a. signaler aux institutions de santé les mesures de sécurité à respecter (voir ch. 1.3.3, let. a);

b. astreindre les institutions de santé à informer leurs professionnels de la santé ayant accès au dossier électronique du patient de leurs droits et de leurs devoirs liés au traitement des données dans le dossier électronique du patient et les obliger à respecter les mesures prescrites;

c. astreindre les institutions de santé à garantir une configuration sûre des terminaux utilisés par les professionnels de la santé pour accéder au dossier électronique du patient.

4.7.2 Les prescriptions pour la configuration des terminaux doivent comprendre au moins:

a. l'utilisation d'un logiciel régulièrement actualisé contre les programmes malveillants;

b. l'utilisation de systèmes de protection du réseau;

c. une actualisation régulière du système d'exploitation et des composants logiciels critiques pour la sécurité;

d. une gestion restrictive des droits d'administrateur du système.

4.7.3 Les communautés doivent garantir que les terminaux, dont les configurations n'ont pas un niveau sûr, ne traitent aucune donnée du dossier électronique du patient.

4.8 Exigences relatives à la protection et à la sécurité des données imposées au personnel technique ou administratif (art. 12, al. 1, let. c, ODEP)

4.8.1 Des directives doivent être édictées pour réglementer l'accès et le traitement des données du dossier électronique du patient par le personnel technique et administratif des communautés, et les mesures techniques et organisationnelles nécessaires doivent être prises pour assurer leur respect.

4.8.2 Les communautés doivent garantir:

a. que les personnes qui utilisent les données ou systèmes du dossier électronique du patient sont suffisamment compétentes pour les tâches prévues, assument leurs responsabilités et respectent consciencieusement la protection et la sécurité des données;

b. que l'utilisation des données d'authentification secrètes est contrôlé au moyen d'un processus de gestion formel et que les exigences en matière d'utilisation sûre (p. ex., confidentialité, longueur des mots de passe, validité) sont formulées et communiquées;

c. que les personnes susceptibles d'avoir accès aux données du dossier électronique du patient sont soumises au secret médical conformément à l'art. 321 CP ou tenus par contrat à l'obligation de garder le secret;

d. que les processus destinés à la gestion du personnel pour satisfaire aux exigences en matière de protection et de sécurité des données sont définis, mis en œuvre et respectés;

e. qu'une procédure officielle est prévue afin de prononcer des mesures disciplinaires ou des sanctions à l'encontre des collaborateurs ayant contrevenu aux règles de la protection et à la sécurité des données.

4.8.3 Les communautés doivent:

a. dresser une liste, visée par le responsable de la sécurité et de la protection des données de la communauté, de tous les administrateurs du système qui peuvent accéder aux données du dossier électronique du patient;

b. garantir que ces personnes sont sélectionnées avec soin, jouissent d'une réputation irréprochable et s'engagent à respecter des exigences en matière de sécurité clairement définies ;

c. contrôler régulièrement le respect des exigences en matière de sécurité.

4.9 Exigences relatives à la protection et à la sécurité des données imposées aux tiers (art .12, al. 1, let. c, ODEP)

4.9.1 Les communautés doivent dresser 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 pourraient accéder aux données du dossier électronique du patient, les traiter, les enregistrer, les transmettre ou fournir des composants d'infrastructure informatique à cet effet.

4.9.2 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.

4.9.3 Les contrats de fourniture doivent fixer sans équivoque les obligations et responsabilités pour satisfaire aux exigences pertinentes de protection et de sécurité des données.

4.9.4 Ils doivent comprendre au moins les dispositions suivantes:

a. obligations du fournisseur de respecter en tout temps les exigences pertinentes de protection et de sécurité des données de la communauté, en cas d'utilisation ou de mise à disposition de moyens informatiques, de personnel et/ou de services;

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

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

d. droit de réexaminer régulièrement les processus des fournisseurs et les mesures de contrôle liés au contrat;

e. obligation de continuer 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;

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

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

4.10 Surveillance et contrôle des prestations de service (art. 12, al. 1, let. c, ODEP)

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:

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

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

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

4.11 Responsable de la protection et de la sécurité des données (art. 12, al. 2, ODEP)

4.11.1 Les communautés doivent désigner un responsable de la protection et de la sécurité des données chargé d'administrer leur système de gestion de la protection et de la sécurité des données et doivent définir son cahier des charges.

4.11.2 Le responsable de la protection et de la sécurité des données doit:

a. veiller au respect des prescriptions relatives à la protection et à la sécurité des données;

b. avoir les moyens d'exercer sa fonction en toute indépendance;

c. disposer des compétences et des ressources techniques nécessaires pour accomplir ses tâches.

4.12 Gestion des clés cryptographiques (art. 12, al. 4, ODEP)

Les communautés doivent garantir que:

a. des procédures sûres et conformes à l'état actuel de la technique sont mises en œuvre pour la création, la distribution, l'activation, l'actualisation, la révocation ou la désactivation et la suppression des clés cryptographiques;

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

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

d. les dispositifs de création, de sauvegarde et d'archivage des clés sont protégés de manière appropriée.

4.13 Sécurité d'exploitation (art. 12, al. 4, ODEP)

4.13.1 Les communautés doivent garantir que:

a. les accès, assortis de droits spéciaux, à l'environnement de production, p. ex. par les administrateurs de systèmes d'exploitation, de banques de données et d'applications

nécessitent une authentification forte à deux facteurs, sont surveillés et historisés et ne permettent pas les exportations illégales, en particulier de données de patients;

b. les accès externes effectués par des tiers et des sous-traitants se trouvant en dehors du réseau local (accès à distance) et en particulier les accès externes privilégiés, assortis de droits spéciaux, à l'environnement de production, outre ce qui précède, sont interdits ou comportent une protection adéquate, sont surveillés et historisés et ne sont autorisés que temporairement, et en cas de besoin;

c. 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;

d. des sauvegardes complètes sont faites et que les données qu'elles contiennent sont cryptées;

e. les sauvegardes sont enregistrées de manière à les protéger de toute modification illicite ou inaperçue;

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

g. seules des personnes autorisées ont accès aux journaux techniques;

h. les fichiers d'historisation sont horodatés et sauvegardés de manière à les protéger de toute modification illicite ou inaperçue;

i. les supports de données de patients sont toujours éliminés ou détruits correctement de sorte que toutes les données s'y trouvant soient illisibles et qu'il ne soit pas possible de les rétablir;

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

4.13.2 Les communautés doivent garantir que l'environnement de production de l'infrastructure informatique du dossier électronique du patient interne à la communauté:

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

b. est doté de nouveaux logiciels exclusivement dans le cadre de processus contrôlés;

c. fait l'objet de contrôles réguliers et actifs, notamment dans le cadre de tests d'intrusion, portant sur ses failles de sécurité;

d. est débarrassé des failles de sécurité détectées à l'aide d'un processus dûment contrôlé de gestion des patchs.

4.13.3 Outre les événements liés au traitement des données du dossier électronique du patient par les professionnels de la santé ainsi que par les patients conformément au ch. 2.10, il convient d'enregistrer au moins les événements suivants survenant dans le cadre de l'exploitation du système:

a. login et logout;

b. tentatives d'accès, réussies ou infructueuses, au système;

c. tentatives d'accès, réussies ou infructueuses, aux données;

d. modifications apportées à la configuration du système;

e. utilisation de droits d'accès spéciaux privilégiés;

f. adresses et protocoles réseau;

g. activation et désactivation des systèmes de protection et d'authentification;

h. modification des autorisations système et des accès;

i. création, modification ou suppression de comptes d'utilisateurs;

j. copie de données considérées comme sensibles.

4.14 Achat, développement et maintenance des systèmes (art. 12, al. 4, ODEP)

4.14.1 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. À cet effet, il est nécessaire de définir des processus de documentation, de spécification, de test, de contrôle-qualité et de mise en œuvre contrôlée pour:

a. l'introduction ou le développement de nouveaux systèmes;
b. les modifications ou développements majeurs réalisés sur les systèmes existants;
c. le changement des plateformes d'exploitation.

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

a. 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;
b. les modifications apportées aux systèmes sont soumises à une procédure formelle documentée de contrôle des modifications;
c. l'accès au propre code source des logiciels est limité, contrôlé et historisé;
d. 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;
e. les environnements de test ne comportent aucune donnée productive ni aucune donnée particulièrement sensible;
f. l'organisation d'exploitation supervise et contrôle le développement de logiciels en cas d'externalisation.

4.15 Sécurité de la communication: gestion des réseaux et des services réseau (art. 12, al. 4, ODEP)

4.15.1 Les communautés doivent prévoir des directives sur la sécurité du réseau et définir les compétences en matière de gestion des réseaux à l'intérieur de la communauté.

4.15.2 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.

4.15.3 Pour cela, elles doivent définir des structures de réseau sûres, 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:

a. seuls les systèmes faisant partie d'une communauté certifiée puissent accéder aux interfaces techniques de leur infrastructure informatique interne (*services*);
b. les systèmes accédant à un service par Internet s'authentifient auprès de celui-ci au moyen du protocole TLS, en utilisant un certificat électronique valable.

4.15.4 Les structures de réseau doivent remplir les exigences suivantes:

a. pour les portails et les points d'accès, utiliser au moins des certificats TLS publics à validation étendue (*extended validation, EV*); pour d'autres services, utiliser au moins des certificats TLS publics à validation étendue *EV* ou des certificats TLS uniquement

valables au sein de la communauté;

b. tous les services accessibles à partir d'Internet doivent authentifier le système appelant via TLS-Client-Authentication;

c. les points d'accès répondeurs (« *Responding Gateways* ») ne doivent autoriser l'établissement d'une liaison que si le système appelant fait partie d'une communauté certifiée qui figure dans le service central de recherche des communautés et communautés de référence aux termes de l'art. 40 ODEP;

d. tous les services internes à la communauté avec lesquels il n'est pas possible de relier par 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 l'a accepté;

e. les procédures utilisées à cet effet doivent être documentées.

4.15.5 Les communautés doivent:

a. séparer, au niveau du réseau, tous les supports de données de la communauté contenant des données du dossier électronique du patient (parmi lesquelles les éléments de l'« inventaire de l'infrastructure informatique » selon le ch. 4.8) de tous les autres systèmes affichant un niveau de sécurité moins élevé;

b. documenter les procédures utilisées à cet effet.

4.15.6 Les communautés doivent notamment documenter les prescriptions de sécurité appliquées pour assurer la protection de leur portail d'accès. La documentation comprend au moins:

a. la topologie du réseau et la nature de la séparation du réseau local (LAN) d'Internet;

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

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

4.16 Expiration des sessions dans le réseau (session timeout) (art. 12, al. 4, ODEP)

4.16.1 Les sessions réseau inactives prennent automatiquement fin après une période d'inactivité définie par le responsable de la protection et de la sécurité des données.

4.16.2 L'authentification aux portails d'accès et sur les terminaux doit être répétée avant tout nouvel accès lorsqu'aucune interaction de l'utilisateur avec le dossier électronique du patient n'a eu lieu avant l'expiration du temps prescrit.

4.17 Système intermédiaire (art. 12, al. 4, ODEP)

Les éléments de l'infrastructure informatique interne à la communauté servant à transmettre les données médicales du dossier électronique du patient, notamment les points d'accès, ne doivent pas sauvegarder ces données durablement, mais doivent les conserver uniquement pendant la durée de la transaction.

4.18 Accessibilité (art. 12, al. 4, ODEP)

Les communautés doivent garantir:

a. que les données du dossier électronique du patient sont disponibles;

b. que les services techniques et les systèmes de traitement et de protection des données du dossier électronique du patient sont disponibles et à l'abri des interruptions;

c. qu'après un dérangement, l'exploitation du système puisse reprendre;

d. que les données du dossier électronique du patient sont protégées en tout temps;

e. que 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 sollicitation extraordinaire;

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

g. que 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'informations 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.

4.19 Dispositifs de stockage sous juridiction suisse (art. 12, al. 5, ODEP)

4.19.1 La communauté doit garantir:

a. 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 sont soumises au droit suisse;

b. que ces mémoires de données se trouvent en Suisse.

5 Service d'assistance pour les professionnels de la santé (art. 13 ODEP)

5.1.1 Les communautés doivent désigner un service d'assistance pour aider les professionnels de la santé dans l'utilisation du dossier électronique du patient.

5.1.2 Les communautés doivent garantir au moins:

a. que les collaborateurs du service d'assistance connaissent leurs droits et leurs devoirs, ainsi que les mesures propres à assurer la protection et la sécurité des données;

b. que les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis au secret médical conformément à l'art. 321 CP ou tenus par contrat à l'obligation de garder le secret;

c. que les collaborateurs du service d'assistance n'ont accès aux terminaux des professionnels de la santé que si ceux-ci ont donné leur consentement, et que l'accès est documenté.

B. Exigences supplémentaires applicables aux communautés de référence

6 Information du patient (art. 15 ODEP)

6.1 Information du patient (art. 15 ODEP)

6.1.1 Le patient doit être informé:

a. du but du dossier électronique du patient;
b. des principes essentiels du traitement des données;
c. du stockage des données médicales dans les systèmes primaires;
d. de la conservation et de la destruction éventuelle de données médicales dans les lieux de stockage.

6.1.2 Le patient doit en particulier être informé du fait qu'il:

a. peut révoquer son consentement présumé à la mise à disposition de données médicales en cas de traitement (art. 3, al. 2, ODEP);
b. peut détruire des données médicales qu'il a enregistrées dans des lieux de stockage du dossier électronique du patient;
c. dispose des fonctions du portail d'accès destiné aux patients;
d. peut consulter les historisations;
e. peut désigner un représentant;
f. peut demander à être informé de l'entrée de professionnels de la santé dans des groupes auxquels il a accordé des droits d'accès;
g. peut habiliter des professionnels de la santé de sa communauté de référence à transmettre des droits d'accès à d'autres professionnels de la santé ou groupes de professionnels de la santé.

6.1.3 Le patient doit être informé des conséquences du consentement et de la révocation, dont au moins:

a. le fait que le consentement est libre;
b. la possibilité de disposer d'un seul dossier de patient à la fois;
c. les modalités de l'attribution et de l'utilisation du numéro d'identification du patient;
d. 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;
e. la possibilité de révoquer son consentement, sans aucune exigence de forme ou de justification de motif;
f. le fait qu'en cas de révocation, le dossier électronique du patient sera supprimé et les données qu'il contient seront détruites;
g. 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 Le patient doit être informé des niveaux de confidentialité pour les données médicales, dont au moins:

a. la possibilité d'attribuer en tout temps un des trois niveaux de confidentialité aux données médicales du dossier électronique du patient;

b. l'attribution automatique du niveau de confidentialité « normal » aux données médicales nouvellement saisies;

c. la possibilité pour les professionnels de la santé d'attribuer le niveau de confidentialité « restreint » aux données médicales nouvellement saisies;

d. la possibilité pour le patient de fixer lui-même un autre niveau de confidentialité pour les données médicales nouvellement saisies, avec pour conséquence que cette disposition prime sur les let. b et c.

6.1.5 Le patient doit être informé des modalités d'octroi de droits d'accès, dont au moins de la possibilité:

a. d'exclure de tout accès certains professionnels de la santé (liste d'exclusion);

b. d'exclure de tout accès des professionnels de la santé en classant des données médicales dans le niveau de confidentialité « secret »;

c. d'accorder à des professionnels de la santé et à des groupes de professionnels de la santé, soit le droit d'accès au niveau de confidentialité « normal », soit celui aux niveaux de confidentialité « normal » et « restreint »;

d. de modifier ces droits d'accès, de les limiter ou de les retirer;

e. pour les auxiliaires enregistrés des professionnels de la santé, d'accéder également aux données avec le droit d'accès accordé au professionnel de la santé responsable;

f. pour les professionnels de la santé, d'accéder aux « normal » dans des situations d'urgence médicale;

g. d'étendre l'accès aux « restreint » dans des situations d'urgence médicale ou d'exclure entièrement un tel accès;

h. d'être informé lorsqu'un accès dans une situation d'urgence médicale a eu lieu.

6.1.6 Le patient doit être informé des mesures recommandées en matière de protection et de sécurité des données, dont au moins:

a. les risques résiduels et les éventuelles mesures préventives;

b. l'authentification sécurisée et l'usage des moyens d'identification et des secrètes;

c. les mesures visant à une utilisation sûre des terminaux;

d. les recommandations de comportement à adopter pour se défendre contre les tentatives de fraude.

7 Consentement (art. 16 ODEP)

7.1 Constitution du dossier électronique du patient

7.1.1 La signature manuscrite du patient est nécessaire à la constitution d'un dossier électronique du patient.

8 Gestion (art. 17 ODEP)

8.1 Ouverture, gestion et suppression du dossier électronique du patient (art. 17, al. 1, let. a, ODEP)

Les communautés de référence définissent les processus d'ouverture, de gestion, et de suppression du dossier électronique du patient.

8.2 Identification des patients (art. 17, al. 1, let. b et d, ODEP)

8.2.1 Les processus d'identification des patients doivent être définis. Ils doivent garantir que:

a. le patient est identifié à l'aide d'un moyen d'identification d'un éditeur certifié ou conforme aux exigences de l'art. 24, al. 1, ODEP;

b. le patient ne possède pas encore de dossier électronique du patient;

c. le patient est enregistré dans l'index des patients de la communauté de référence;

d. un numéro d'identification du patient est demandé conformément aux art. 6 et 7 ODEP et qu'il est correctement attribué au dossier électronique du patient à constituer;

e. les données démographiques du patient figurant dans la banque de données d'identification de la CdC sont reprises dans l'index des patients de la communauté de référence.

8.2.2 Les communautés de référence doivent s'assurer que l'identificateur univoque visé à l'art. 25, al. 1, ODEP est relié avec le bon patient et son numéro d'identification.

8.3 Identification et authentification lors de l'accès (art. 17, al. 1, let. c, ODEP)

Pour accéder à leur dossier électronique, les patients doivent s'authentifier avec des moyens d'identification valables émis par un éditeur certifié selon l'art. 31 ODEP.

8.4 Représentation (art. 17, al. 1, let. c, ODEP)

8.4.1 Le représentant visé au ch. 8.6.3, let. f, doit accéder au dossier électronique du patient qu'il représente avec son propre moyen d'identification émis par un éditeur certifié selon l'art. 31 ODEP.

8.4.2 La communauté de référence doit garantir que:

a. l'identification du représentant repose sur un moyen d'identification émis par un éditeur certifié selon l'art. 31 ODEP ou satisfait aux exigences de l'art. 24, al. 1, ODEP;

b. le représentant est informé des principes essentiels du traitement des données, ainsi que des possibilités, des droits et des obligations liés à l'utilisation du dossier électronique du patient;

c. l'identificateur univoque du moyen d'identification est correctement attribué au représentant du patient conformément à l'art. 25, al. 1, ODEP;

d. l'accès du représentant au dossier électronique du patient n'est accordé que pour la durée de la représentation.

8.5 Changement de communauté de référence (art. 17, al. 1, let. e, ODEP)

8.5.1 Le processus de changement de communauté de référence par le patient doit être défini.

8.5.2 Le processus de changement de communauté de référence doit garantir:

a. que la configuration individuelle de gestion des autorisations peut être transférée à la nouvelle communauté de référence. À cet effet, il faut respecter les prescriptions relatives au format technique d'échange du profil d'intégration national CH:PPQ, selon l'annexe 5 ODEP;

b. l'habilitation dont disposent les professionnels de la santé en vertu de l'art. 4, let. g, ODEP est supprimée;

c. la possibilité d'accès d'éventuels représentants d'un patient est supprimée.

8.6 Gestion des autorisations (art. 17, al. 2, ODEP)

8.6.1 Les patients doivent avoir la possibilité d'accorder, de modifier ou de retirer les droits d'accès des professionnels de la santé ou des groupes de professionnels de la santé. Les prescriptions des art. 2 et 3 ODEP doivent être respectées.

8.6.2 Les communautés de référence doivent garantir que la configuration de la gestion des autorisations peut être modifiée uniquement en conformité avec la volonté du patient.

8.6.3 Les communautés de référence doivent garantir que les patients peuvent faire usage des options que leur donne l'art. 4 ODEP. À cet effet, elles doivent permettre au patient:

a. de définir le niveau de confidentialité attribué aux nouvelles données médicales saisies;

b. d'exclure certains professionnels de la santé de l'accès à son dossier électronique;

c. d'être informé de l'intégration de professionnels de la santé dans des groupes autorisés;

d. de limiter dans le temps, à sa seule discrétion, les droits d'accès accordés aux professionnels de la santé;

e. d'étendre ou d'exclure les accès d'urgence;

f. de désigner un représentant;

g. d'habiliter des professionnels de la santé à transmettre leurs droits d'accès à d'autres professionnels de la santé ou groupes de professionnels de la santé.

9 Portail d'accès pour les patients (art. 18 ODEP)

9.1 Mise en œuvre de la gestion des autorisations (art. 18, let. a, ODEP)

Le portail d'accès doit:

a. donner la possibilité au patient d'administrer les autorisations dans le respect des prescriptions énoncées aux art. 1 à 4 ODEP;

b. indiquer les droits d'accès dont dispose chaque professionnel de la santé;

c. indiquer la composition des groupes de professionnels de la santé.

9.2 Présentation (art. 18, let. a, ODEP)

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

a. si les données médicales ont été fournies par un professionnel de la santé ou par le patient lui-même ;
b. quelles données médicales ont été annulées;
c. quelles versions des données médicales sont disponibles;
d. quelles données médicales ont été attribuées à quel niveau de confidentialité.

9.3 Présentation des données historisées (art. 18, let. b, ODEP)

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.

9.4 Saisie et consultation de données (art. 18, let. c, ODEP)

9.4.1 Le portail d'accès doit donner la possibilité aux patients:

a. d'exclure les données médicales saisies par les professionnels de la santé de la destruction visée à l'art. 10, al. 1, let. d;
b. d'éliminer du dossier électronique du patient certaines données le concernant.

9.4.2 En ce qui concerne les types de média, le portail d'accès doit satisfaire aux mêmes exigences que le portail d'accès interne pour les professionnels de la santé selon le ch. 3.3.

9.4.3 Le portail d'accès doit au moins remplir les conditions suivantes concernant les données saisies par le patient lui-même:

a. 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;
b. 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 un lieu de stockage intermédiaire.

9.5 Accessibilité (art. 18, let. d, ODEP)

Le portail d'accès doit satisfaire aux mêmes exigences que le portail d'accès pour les professionnels de la santé selon le ch.3.2.

10 Données enregistrées par les patients (art. 19 ODEP)

10.1 Stockage des données médicales de patients

10.1.1 Les communautés de référence doivent mettre à disposition des lieux de stockage internes à la communauté pour les données médicales enregistrées par les patients eux-mêmes.

10.1.2 Les données médicales ne doivent être soumises à aucun délai d'effacement.

10.1.3 Un espace de stockage suffisant doit être prévu à cet effet.

10.2 Archivage hors ligne des données médicales et des métadonnées

10.2.1 Les patients doivent avoir la possibilité de télécharger les données de leur dossier électronique dans un format électronique usuel interopérable ou de se les procurer d'une autre manière (voir ch. 2.9.16).

10.2.2 À cette fin, il faut prévoir des procédures permettant de déterminer si les données archivées ont été modifiées depuis leur mise à disposition.

10.2.3 Les communautés de référence doivent garantir que les données archivées qui sont mises à disposition une nouvelle fois dans le dossier électronique du patient n'ont pas été modifiées depuis leur première mise à disposition.

11 Service d'assistance pour les patients (art. 20 ODEP)

11.1.1 Les communautés de référence doivent désigner un service d'assistance 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:

a. les collaborateurs connaissent leurs droits et leurs obligations ainsi que les risques et les mesures propres à assurer la protection et la sécurité des données;

b. les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis au secret médical conformément à l'art. 321 CP ou tenus par contrat à l'obligation de garder le secret;

c. les collaborateurs du service d'assistance n'ont accès aux terminaux des patients que si ceux-ci ont donné leur consentement, et que l'accès est documenté.

12 Suppression du dossier électronique du patient (art. 21 ODEP)

12.1 Processus pour la suppression du dossier électronique

Les communautés de référence doivent prévoir des processus pour la suppression du dossier électronique du patient.

12.2 Révocation du consentement à la tenue du dossier électronique du patient (art. 21, al. 1, ODEP)

12.2.1 Les communautés de référence doivent veiller à la suppression sans délai du dossier électronique du patient en cas de révocation par celui-ci de son consentement à la tenue de son dossier électronique.

12.2.2 Le processus de suppression du dossier électronique du patient en cas de révocation du consentement doit garantir que:

a. l'identification de la personne exerçant son droit de révocation repose sur le moyen d'identification émis par un éditeur certifié et que la personne exerçant son droit de révocation est informée des conséquences qui en découlent;
b. la révocation est documentée de façon juridiquement valable;
c. la déclaration de révocation est conservée pendant dix ans.

12.3 Suppression après le décès du patient (art. 21, al. 2, ODEP)

Les communautés de référence doivent garantir que la suppression du dossier électronique du patient a lieu au plus tôt deux ans après le décès du patient.

12.3 Suppression du dossier électronique du patient (art. 21, al. 3, ODEP)

Le processus de suppression du dossier électronique du patient doit garantir:

a. que le dossier électronique du patient à supprimer est correctement identifié;
b. que tous les droits d'accès au dossier correspondant sont aussitôt retirés;
c. que toutes les données du dossier correspondant sont détruites selon le ch. 2.1, let. b et que le numéro d'identification du patient est supprimé de tous les systèmes;
d. que toutes les communautés et communautés de référence sont informées dans un délai approprié de la suppression du dossier électronique du patient;
e. que la CdC est informée de la suppression du dossier électronique du patient dans un délai approprié.