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

Rapport explicatif concernant

l'ordonnance sur le dossier électronique du patient (ODEP) et

l'ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI)

Version du 22 mars 2017

Table des matières

1 Partie générale

1.1 Contexte

Le Parlement a adopté la loi fédérale sur le dossier électronique du patient (LDEP ; RS 816.1, FF 2015 4419) le 19 juin 2015. Loi-cadre, la LDEP fixe les conditions permettant de traiter les données relatives au dossier électronique du patient et représente une condition majeure à la réussite de la « Stratégie Cybersanté Suisse ». Elle constitue également une mesure importante dans l'optique du développement du système de santé suisse.

Objet
La LDEP pose le cadre régissant le traitement des données et des documents relatifs au dossier électronique du patient. L'objectif consiste à renforcer la qualité des traitements médicaux, à améliorer les processus thérapeutiques, à augmenter la sécurité des patients, à accroître l'efficience du système de santé et à promouvoir la culture sanitaire des patients. Conçu comme une loi cadre, le projet doit à la fois assurer la sécurité des investissements et offrir une flexibilité suffisante au moment de la mise en œuvre dans les régions.

Grâce au dossier électronique du patient, les professionnels de la santé pourront accéder aux données que d'autres professionnels de la santé participant au processus thérapeutique ont établies. Ils pourront enregistrer ces données, saisies de manière décentralisée par les autres professionnels de la santé, dans les systèmes d'information de leur cabinet ou de leur clinique. Ils devront à cet effet s'affilier à une communauté ou à une communauté de référence certifiée, c'est-à-dire un regroupement de professionnels de la santé et de leurs institutions, et leurs patients devront leur accorder les droits d'accès nécessaires. Le dossier électronique du patient permettra en outre aux patients de consulter leurs données, de les rendre accessibles et de gérer les droits d'accès.

Le texte en question ne règle pas l'utilisation des données des patients en dehors du dossier électronique du patient, comme par exemple, les règles de responsabilité et de documentation ou du secret médical. L'échange de données entre les professionnels de la santé et les assurances sociales ou l'utilisation des données médicales contenues dans le dossier électronique du patient pour développer des registres de maladies ou de qualité et à des fins de statistiques ou de recherche relèvent également de réglementations spécifiques.

Participation au dossier électronique du patient
Le dossier électronique du patient est facultatif pour les patients. Conformément au principe de l'autodétermination des patients en matière d'information, chaque personne décide elle-même si elle consent à la tenue d'un dossier électronique et, le cas échéant, détermine l'étendue des droits d'accès qu'elle entend accorder aux professionnels de la santé en charge de son traitement.
Le caractère facultatif est également valable pour les professionnels de la santé et leurs institutions, à l'exception des fournisseurs de prestations visés aux art. 39 et 49*a*, al. 4, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[1] : Les hôpitaux doivent s'affilier à une communauté ou à une communauté de référence certifiée dans un délai de trois ans après entrée en vigueur de la LDEP (c.-à-d. d'ici au 14 avril 2020) et les maisons de naissance et les établissements médico-sociaux dans un délai de cinq ans, soit d'ici au 14 avril 2022.

Les professionnels de la santé exerçant en milieu ambulatoire décident librement s'ils entendent proposer le dossier électronique du patient à leurs patients. Toutefois, s'ils s'affilient à une communauté ou à une communauté de référence certifiée, ils sont tenus de rendre accessibles les données pertinentes du dossier électronique du patient.

[1] RS **832.10**

Les professionnels de la santé ne peuvent traiter des données dans le cadre du dossier électronique du patient que si le patient y consent. Celui-ci peut accorder des droits d'accès à certains professionnels ou groupes de professionnels de la santé.

Moyens d'identification
Pour que les données puissent être traitées en toute sécurité, une identification et une authentification univoques et sûres des patients et des professionnels de la santé sont nécessaires. Cette exigence est remplie grâce à un moyen d'identification délivré par un éditeur certifié.

Numéro d'identification du patient
Le nouveau numéro d'identification du patient est utilisé comme caractéristique d'identification supplémentaire afin de pouvoir réunir de manière correcte et complète l'ensemble des données et documents médicaux d'un patient saisis dans son dossier électronique. Il complète les caractéristiques d'identification personnelle telles que le nom, le prénom, le sexe ou la date de naissance. Le numéro d'identification du patient est attribué sur demande par la Centrale de compensation de l'AVS (CdC).

Obligation de certification
Pour assurer un traitement des données à la fois sécurisé et conforme aux dispositions légales, tous les participants (communautés, communautés de référence, éditeurs de moyens d'identification) doivent répondre à des critères de certification détaillés. Une procédure de certification garantit le respect de ces critères techniques et organisationnels.

Services de recherche de données
La Confédération exploite les services de recherche centraux nécessaires à la communication entre les communautés et les communautés de référence.

Aides financières
Par ailleurs, la Confédération soutient la constitution et la certification des communautés et des communautés de référence pendant trois ans à compter de l'entrée en vigueur de la LDEP, en allouant des aides financières à hauteur de 30 millions de francs. Ces aides sont liées à une participation des cantons ou de tiers pour un montant égal. Les coûts découlant de l'adaptation des systèmes d'information des cabinets ou des cliniques des professionnels de la santé et de leurs institutions ne sont pas couverts par les aides financières de la Confédération.

1.2 Droit de l'UE

A l'heure actuelle (mars 2016), la Suisse n'est tenue par aucune obligation internationale dans le domaine de la cybersanté. Les directives et les recommandations internationales (par ex. de l'UE) ont toutefois servi de repères lors de l'élaboration de l'ODEP, la recommandation de la Commission européenne sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé ayant été particulièrement importante à cet égard. Par ailleurs, les directives et règlements déterminants en la matière sont les suivants :

- la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2].
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)[3] ;
- la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des

[2] JO L 281 du 23.11.1995, p. 31 ; modifiée par le règlement (CE) no 1882/2003, JO L 284 du 31.10.2003, p. 1.
[3] JO L 201 du 31.7.2002, p. 37 ; modifiée en dernier lieu par la directive 2009/136/CE, JO L 337 du 18.12.2009, p. 11

communications électroniques, et le règlement (CE) 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs[4].

- la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers[5].
- le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[6].

D'autres informations en rapport avec le droit de l'UE figurent dans le message accompagnant la LDEP (FF 2013 4790 ss).

1.3 Aperçu du droit d'exécution relatif au dossier électronique du patient

Le droit d'exécution relatif au dossier électronique du patient comprend l'ordonnance sur le dossier électronique du patient (ODEP), l'ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI) et l'ordonnance sur les aides financières pour le dossier électronique du patient (OFDEP). Les détails sont présentés à la figure 1.

<table>
<tr>
<td rowspan="2">Au niveau du Conseil fédéral</td>
<td rowspan="2">Ordonnance sur le dossier électronique du patient (ODEP)
– Chapitre 1 : Niveaux de confidentialité et droits d'accès
– Chapitre 2 : Numéro d'identification du patient
– Chapitre 3 : Communautés et communautés de référence
– Chapitre 4 : Moyens d'identification
– Chapitre 5 : Accréditation
– Chapitre 6 : Certification
– Chapitre 7 : Services de recherche de données
– Chapitre 8 : Entrée en vigueur</td>
<td>Ordonnance sur les aides financières pour le dossier électronique du patient (OFDEP)
– Section 1 : Dispositions générales
– Section 2 : Critères et calcul
– Section 3 : Procédure
– Section 4 : Entrée en vigueur</td>
</tr>
<tr>
<td>– Annexe : Coûts imputables</td>
</tr>
<tr>
<td>Au niveau du département</td>
<td>Ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI)
– Annexe 1 : Numéro d'identification du patient
– Annexe 2 : Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence
– Annexe 3 : Métadonnées
– Annexe 4 : Formats d'échange
– Annexe 5 : Profils d'intégration
– Annexe 6 : Évaluation et recherche
– Annexe 7 : Exigences minimales applicables à la qualification du personnel des organismes de certification
– Annexe 8 : Critères techniques et organi-</td>
<td></td>
</tr>
</table>

[4] JO L 337 du 18.12.2009, p. 11
[5] JO L 88 du 04.04.2011, p. 45
[6] JO L 257 du 28.8.2014, p. 73

	sationnels de certification applicables aux éditeurs de moyens d'identification	

Figure 1. Structure du droit d'exécution relatif à la loi fédérale sur le dossier électronique du patient

1.3.1 Ordonnance sur le dossier électronique du patient (ODEP)

L'ODEP réglemente les niveaux de confidentialité et les droits d'accès (chap. 1), l'attribution et la gestion du numéro d'identification du patient par la CdC (chap. 2), les prescriptions relatives à la constitution et à l'exploitation des communautés et des communautés de référence (critères de certification ; chap. 3), les prescriptions relatives aux moyens d'identification et à leurs éditeurs (chap. 4), l'accréditation (chap. 5), la certification (chap. 6) ainsi que les services de recherche de données (chap. 7).

1.3.2 Ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI)

L'ordonnance du département sur le dossier électronique du patient fixe à l'*annexe 1* les exigences applicables au numéro d'identification du patient. En font partie les prescriptions relatives à la composition du numéro d'identification du patient et au calcul de la clé de contrôle, conformément à l'art. 5, al. 2, ODEP.

L'*annexe 2* fixe les critères techniques et organisationnels de certification applicables aux communautés et aux communautés des référence (cf. ODEP, chap. 3 « Communautés et communautés de référence »).

L'*annexe 3* (cf. art. 10, al. 3, let. a) contient la liste des métadonnées à utiliser dans le cadre du dossier électronique du patient pour assurer l'interopérabilité des systèmes et un échange de données en toute sécurité.

L'*annexe 4* (cf. art. 10, al. 3, let. b, ODEP) indique les formats d'échange à utiliser. Il s'agit, par exemple, de prescriptions relatives au carnet de vaccination électronique ou au rapport de sortie électronique. Aucun format d'échange n'a été défini à ce jour. Les formats d'échange seront élaborés dans le cadre d'une procédure impliquant les milieux intéressés concernés et seront intégrés dans le droit d'exécution lors des futures révisions.

L'*annexe 5* (cf. art. 10, al. 3, let. c, ODEP) spécifie les profils d'intégration régissant l'échange intercommunautaire de données ainsi que les adaptations nationales de ces profils. Elle contient également deux profils d'intégration nationaux à utiliser en complément des profils IHE.

L'*annexe 6* (cf. art. 22, al. 2, ODEP) fixera les données à fournir pour l'évaluation ainsi que les délais de fourniture de ces données ; les dispositions correspondantes seront intégrées dans le droit d'exécution lors d'une future révision.

Les exigences minimales en matière de qualification du personnel des organismes de certification sont précisées à l'*annexe 7*.

L'*annexe 8* (cf. art. 31, al. 2, ODEP) fixe les critères techniques et organisationnels de certification applicables aux éditeurs de moyens d'identification.

1.3.3 Ordonnance sur les aides financières pour le dossier électronique du patient (OFDEP)

L'OFDEP règle l'octroi des aides financières conformément aux art. 20 à 23 LDEP. En vertu de l'art. 27, al. 3, LDEP, les demandes d'aide financière pour la constitution et la certification des communautés et des communautés de référence doivent être déposées au plus tard dans les trois ans qui suivent l'entrée en vigueur de la loi. Selon l'art. 26 LDEP, les art. 20 à 23 LDEP, et par conséquent l'OFDEP, sont applicables aux demandes d'aide financière déposées pendant leur durée de validité. Le commentaire relatif à l'OFDEP fait l'objet d'un document séparé.

1.4 Conséquences

Les débats parlementaires n'ont abouti qu'à quelques modifications ponctuelles de la LDEP (en particulier possibilité d'obtenir des aides de la Confédération si des tiers participent au co-financement de la constitution de la communauté ou de la communauté de référence, uniformisation de la procédure d'octroi des aides financières, réduction du délai transitoire applicable aux hôpitaux pour leur affiliation à des communautés ou communautés de référence certifiées et possibilité d'utiliser la carte d'assuré). On peut donc se référer dans une large mesure aux commentaires correspondants figurant dans le message accompagnant la LDEP (cf. FF 2013 4747 ss) en ce qui concerne les conséquences de l'ODEP pour les différents acteurs. Dans la partie qui suit, seuls sont mentionnés brièvement les principaux points du message ainsi que les conséquences liées aux dispositions d'exécution.

1.4.1 Conséquences pour la Confédération

La mise en œuvre de la LDEP entraîne une augmentation des charges financières et des frais de personnel pour la Confédération en raison des tâches suivantes qui lui sont confiées.

L'office fédéral de la santé publique (OFSP) est habilité, en vertu de l'art. 12, al. 2, LDEP, à modifier les critères de certification applicables aux communautés et aux communautés de référence ainsi qu'aux éditeurs de moyens d'identification en fonction des progrès techniques (cf. art. 10, al. 5, art. 30, al. 3, et art. 31, al. 3, ODEP).

Dans le cadre de la certification selon la LDEP, l'OFSP est en outre propriétaire du schéma de certification (*Schema-Owner*), ce qui implique qu'il sert d'interlocuteur pour les questions du Service d'accréditation suisse (SAS). Il veille également à un échange ciblé des informations relatives à la certification entre les entités à certifier (communautés et communautés de référence et éditeurs de moyens d'identification).

Afin d'assurer une certification uniforme à l'échelle nationale dans le cadre des directives régissant l'interopérabilité, l'OFSP, en collaboration avec l'organe de coordination Confédération-cantons « eHealth Suisse », met à la disposition des organismes de certification un système de certification ayant pour fonction de vérifier les normes, standards et profils d'intégration et veille à la bonne exploitation et au développement de ce système de test (art. 28, al. 4, ODEP).

L'OFSP élabore et exploite les services de recherche de données nécessaires au fonctionnement du dossier électronique du patient (art. 14, al. 1, et art. 19, al. 1, LDEP).

La Confédération alloue des aides financières pendant une durée de trois ans à partir de l'entrée en vigueur de la LDEP pour promouvoir la constitution et la certification de communautés et de communautés de référence (art. 20 à 23 LDEP). L'OFSP examine les demandes d'aide financière, recueille l'avis des cantons concernés et élabore des contrats de prestations avec les communautés et communautés de référence auxquelles des aides sont accordées. Le respect des contrats de prestations fait l'objet d'un contrôle permanent afin de déceler d'éventuelles irrégularités et de prendre les mesures qui s'imposent.

Le *Département fédéral de l'intérieur (DFI)* évalue la loi d'après les principes d'adéquation, d'efficacité et d'économicité (art. 18 LDEP et art. 22 ODEP).

Le traitement de données par des tiers relève du domaine d'application de la loi fédérale sur la protection des données (LPD ; RS 235.1). En leur qualité d'organisations de droit privé, les communautés et communautés de référence sont régies par la LPD et placées sous la surveillance du *Préposé fédéral à la protection des données et à la transparence (PFPDT),* à la condition que la législation spéciale n'en dispose pas autrement. Il en va de même des autres acteurs dans la mesure où il s'agit d'organisations privées.

Le *SAS* reconnaît les organismes d'audit et de certification de systèmes de gestion qui entendent procéder à des certifications selon la LDEP. En les accréditant, il s'assure que l'organisation et les procédures de contrôle mises en place sont en mesure de vérifier les critères de certification des communautés et des communautés de référence et ceux des éditeurs de moyens d'identification. Le contrôle porte aussi bien sur des aspects organisationnels que techniques.

La *CdC* est chargée d'attribuer et de gérer le numéro d'identification du patient selon l'art. 6, al. 1, ODEP. Elle veille à ce que la base de données d'identification existante de la CdC soit développée de manière à répondre aux exigences de la LDEP et de l'ODEP.

L'*organe de coordination Confédération-cantons « eHealth Suisse »* s'assure que les normes, standards et profils d'intégration sont développés dans le cadre de processus participatifs. Le résultat de ces travaux est transmis à l'OFSP, l'Office compétent en matière de révision de la loi et de ses dispositions d'exécution.

« EHealth Suisse » se charge par ailleurs des tâches en relation avec l'information (art. 15 LDEP) et la coordination (art. 16 LDEP).

1.4.2 Conséquences pour les cantons et les communes

La mise en œuvre du présent projet peut engendrer un accroissement des charges et des frais de personnel au niveau des cantons pour les raisons suivantes :

- Examen et, le cas échéant, modification des bases légales en lien avec l'introduction du dossier électronique du patient ;
- éventuelle participation aux coûts de constitution, de certification et d'exploitation des communautés et des communautés de référence ;
- élaboration de prises de position concernant les demandes d'aides financières à la Confédération émanant de communautés ou de communautés de référence prévoyant de s'établir sur le territoire du canton.

Les cantons sont chargés de garantir et d'organiser la couverture sanitaire. Ils sont donc compétents pour aménager, y compris sur le plan financier, les conditions pour que non seulement les établissements hospitaliers (hôpitaux conventionnés ou figurant sur une liste cantonale, cliniques de réadaptation, établissements médico-sociaux et maisons de naissance ; cf. art. 39, al. 1, let. f, et 49*a*, al. 4, première phrase, LAMal), mais aussi les professionnels de la santé exerçant à titre indépendant, notamment les médecins, s'affilient à des communautés ou à des communautés de référence et demandent leur certification.

2 Partie spéciale

2.1 Préambule

Le préambule de l'ODEP renvoie à la LDEP dans son ensemble du fait que celle-ci contient différentes normes fondant des compétences.

2.2 Commentaire des dispositions

Chapitre 1 : Niveaux de confidentialité et droits d'accès

Art. 1 Niveaux de confidentialité

En vertu de l'*al. 1*, le patient peut attribuer aux données médicales de son dossier électronique les trois niveaux de confidentialité suivants (let. a à c) :

a) « normal » : par ex. données et documents pertinents pour le traitement, par ex. rapports, résultats d'examens, traitements dispensés, etc., et informations relatives aux allergies, intolérances et aux maladies particulières, garanties de prise en charge des coûts, directives anticipées, déclaration de volonté de faire don de ses organes, coordonnées des personnes à contacter en cas d'urgence;
b) « restreint » : données médicales jugées sensibles par le patient et que seuls des professionnels de la santé au bénéfice d'un droit d'accès « étendu » peuvent consulter;
c) « secret » : données médicales pouvant exclusivement être consultées par le patient.

La désignation des niveaux de confidentialité ci-dessus n'a qu'une valeur d'exemple et elle ne doit pas être considérée comme étant une définition des données attribuées à un niveau de confidentialité donné. Chaque type de document peut être associé à n'importe quel niveau de confidentialité. Le choix d'un niveau se fait en fonction de l'étendue du droit d'accès, qui varie selon le niveau de confidentialité (cf. commentaire relatif à l'art. 2).

Si le patient ne choisit pas de niveau de confidentialité, le niveau « normal » est attribué par défaut aux nouvelles données enregistrées dans son dossier électronique (al. 2). Cette configuration de base peut être modifiée par le patient (cf. commentaire relatif à l'art. 4, let. a). Les professionnels de la santé peuvent, eux aussi, déroger à la configuration de base et attribuer le niveau de confidentialité « restreint » aux données qu'ils saisissent dans le dossier électronique du patient, mais ils ne peuvent recourir à cette possibilité que si le patient n'a pas fait usage de l'option prévue à l'art. 4, let. a. C'est l'instruction explicite du patient qui prévaut dans ce cas.

Les niveaux de confidentialité s'appliquent uniquement aux documents médicaux et aux données médicales saisis dans le dossier électronique du patient et conservés dans les lieux de stockage ou figurant dans les registres de documents. Les données démographiques du patient ne sont pas concernées. Ces données se trouvent en particulier dans les index de patients des communautés ou des communautés de référence. Elles sont disponibles à tous les participants au dossier électronique du patient. Il est en effet impératif que ceux-ci en disposent pour pouvoir rechercher et retrouver le dossier électronique d'un patient. Les accès en cas d'urgence ne sont possibles que si les données démographiques sont exploitables à des fins de recherche. La recherche ne fait apparaître que les données démographiques, l'accès s'effectuant dans un deuxième temps (sur attribution d'un droit d'accès ou d'une autorisation d'accès en cas d'urgence). Le patient doit être informé de ces possibilités de traitement des données au moment de donner son consentement à l'ouverture d'un dossier électronique afin que son consentement puisse couvrir les traitements de données qu'il entend autoriser. Les processus de recherche et de traitement des données peuvent être retracés à tout moment à l'aide des données historisées (fichiers log).

Art. 2 Droits d'accès

L'*art. 2* fixe les modalités de l'attribution des droits d'accès par le patient. La mise en œuvre incombe aux communautés de référence. Le respect de la réglementation en cas d'urgence médicale doit être garanti aussi bien par les communautés de référence que par les communautés.

Selon l'*al. 1*, le patient peut attribuer des droits d'accès différents aux professionnels de la santé ou aux groupes de professionnels de la santé. Il a la possibilité soit d'attribuer le droit d'accès aux données du niveau de confidentialité « normal », ce qui ne permet d'accéder qu'aux données normalement accessibles, soit d'accorder ce droit pour les données des deux niveaux de confidentialité « normal » et « restreint », ce qui correspond à un droit d'accès étendu. Seul le patient a accès au niveau de confidentialité « secret ».

En situation d'urgence médicale, les professionnels de la santé peuvent consulter le dossier électronique du patient sans qu'aucun droit d'accès ne leur ait été accordé au préalable (*al. 2*). Ils ont alors accès au niveau de confidentialité « normal ». Cette possibilité leur est offerte uniquement en cas d'urgence médicale. L'urgence d'une situation est exclusivement établie sur la base de critères médicaux. Afin d'empêcher un recours abusif à l'accès en cas d'urgence, par ex. attaques automatiques visant un terminal, le professionnel de la santé doit confirmer l'accès pour urgence médicale au moyen d'une action manuelle, non reproductible automatiquement (cf. annexe 2 ODEP-DFI, ch. 2.2, let. a). On pourrait imaginer des éléments de sécurité supplémentaires, comme l'obtention d'un mot de passe à usage unique ou la double entrée d'un critère de sécurité quelconque. L'accès en cas d'urgence est interdit aux professionnels de la santé figurant sur la liste d'exclusion d'un patient, de même qu'aux personnes que le patient a exclus de l'accès en cas d'urgence (cf. commentaire relatif à l'art. 4, let. e). Étant donné le caractère exceptionnel de la situation, la loi prévoit que le patient doit être informé d'un accès en cas d'urgence (art. 9, al. 5, 2e phrase, LDEP). L'obligation d'informer en temps utile incombe à la communauté ou à la communauté de référence au sein de laquelle s'effectue l'accès en urgence (cf. annexe 2 ODEP-DFI, ch. 2.2, let. b). Cette obligation peut être déléguée à l'institution de santé où l'accès en urgence a eu lieu ; l'information peut aussi être effectuée par un procédé technique automatisé. La communauté peut s'acquitter de son obligation d'information par un moyen à sa convenance, que ce soit par courrier postal, courrier électrossnique ou SMS. L'organisme qui communique une information par un canal non sécurisé doit garantir qu'elle ne contient pas d'informations médicales (cf. annexe 2 ODEP-DFI, ch. 2.2, let. c).

Pour des considérations pratiques, des droits d'accès peuvent aussi être accordés de manière sommaire à des groupes de professionnels de la santé (par ex. groupe interdisciplinaire d'experts [*tumor board*] ou service hospitalier). Cela implique que le patient puisse choisir le groupe de professionnels de la santé concerné par l'intermédiaire du service de recherche des institutions de santé et des professionnels de la santé (art. 41 ODEP) et s'informer de sa composition. Selon l'*al. 3*, les droits d'accès des groupes de professionnels de la santé sont fonction de l'appartenance au groupe : Le professionnel de la santé qui intègre un groupe reçoit le droit d'accès associé à ce groupe. Cette disposition garantit que le professionnel concerné a accès aux informations nécessaires dans le cadre d'un traitement. Lorsque qu'un professionnel de la santé quitte un groupe, le droit d'accès associé au groupe lui est automatiquement retiré.s

Art. 3 Durée des droits d'accès

L'*art. 3* fixe la durée de validité des droits d'accès accordés.

En vertu de l'*al. 1*, les droits d'accès accordés à des professionnels de la santé sont valables tant que le patient ne les a pas retirés. La loi ne prévoit pas de limitation temporelle. La possibilité existe cependant de limiter la validité des droits d'accès (cf. commentaire relatif à l'art. 4, let. d).

L'*al. 2* dispose que les droits d'accès des groupes de professionnels de la santé sont accordés pour une durée fixée par le patient. Cette disposition obéit au principe de proportionnalité. D'une part, elle

se justifie par le fait qu'en règle générale, les traitements stationnaires dans les institutions hospitalières ne durent pas trop longtemps. D'autre part, comme les professionnels de la santé bénéficiant de droits d'accès de groupe sont toujours plus nombreux que ceux participant effectivement au traitement, l'inconvénient inhérent à la nature des droits d'accès de groupe doit être compensé par la compétence donnée au patient de décider de la durée de tels droits d'accès en tout connaissance de cause. À titre d'aide à la décision, la communauté de référence peut par exemple offrir au patient différentes possibilités de limiter les durées de validité.

Art. 4 Options données au patient

L'*art. 4* présente les différentes options données patient pour définir les niveaux de confidentialité et l'attribution de droits d'accès. La mise en œuvre incombe aux communautés de référence. Le respect de la réglementation en cas d'urgence médicale doit être garanti aussi bien par les communautés de référence que par les communautés.

D'après la *let. a*, le patient a la possibilité de déterminer le niveau de confidentialité attribué par défaut aux nouvelles données saisies dans son dossier électronique. Il peut changer la configuration de base de manière à attribuer le niveau de confidentialité « restreint » aux nouvelles données. Cette option lui donne la possibilité d'attribuer d'emblée un niveau de confidentialité assorti d'un droit d'accès plus limité à des données de toute évidence sensibles pour lui. C'est le cas, par exemple, face à un diagnostic stigmatisant pour le patient. Bien entendu, il peut en tout temps revenir au niveau de confidentialité « normal » de la configuration de base.

En vertu de la *let. b*, le patient peut interdire à certains professionnels de la santé l'accès à son dossier électronique (cf. art. 9, al. 3, LDEP). Les professionnels de la santé concernés sont alors placés sur une « liste d'exclusion ». Le patient peut également placer sur une liste d'exclusion un professionnel de la santé membre d'un groupe de professionnels de la santé. La liste d'exclusion prime les autres dispositions. Même s'ils sont membres d'un groupe ayant reçu un droit s'accès, les professionnels concernés ne peuvent donc pas accéder au dossier électronique de ce patient. L'accès en cas d'urgence leur est également interdit.

En vertu de la *let. c*, le patient peut exiger d'être informé lorsqu'un professionnel de la santé intègre un groupe auquel il a attribué un droit d'accès (cf. commentaire relatif à l'art. 9, al. 2, let. f). Les patients ont ainsi la possibilité de vérifier la composition du groupe et, le cas échéant, de retirer à un professionnel de la santé le droit d'accès qu'il a automatiquement obtenu du fait de son intégration dans le groupe.

Selon la *let. d*, le patient a la possibilité de limiter comme il l'entend la durée des droits d'accès qu'il a accordés à un professionnel de la santé. Cela permet de s'assurer que les professionnels de la santé qui n'interviendront probablement qu'une fois dans un traitement, ou seulement pour une brève période, n'auront pas accès à son dossier électronique pendant une durée indéterminée. Les droits d'accès de durée limitée s'éteignent à l'échéance prévue sans autre intervention du patient. Cette manière de procéder réduit le risque d'« oublier » que des droits d'accès ont été accordés.

Selon la *let. e*, le patient a la possibilité d'étendre au niveau de confidentialité « restreint » ou, au contraire, d'exclure totalement le droit d'accès à son dossier électronique en cas d'urgence médicale.

Selon la *let. f*, le patient a la faculté de désigner un représentant qui pourra accéder à son dossier électronique du patient et attribuer des niveaux de confidentialité ainsi que des droits d'accès en son nom. Le nombre de représentants n'est pas limité. Les représentants n'ont besoin ni d'un numéro d'identification du patient propre ni d'un dossier électronique du patient. Toutefois, ils doivent impérativement disposer d'un moyen d'identification propre pour pouvoir accéder au dossier électronique de la personne qu'ils représentent. On peut penser ici à la représentation d'un enfant ou de personnes âgées par des proches ou des personnes de confiance.

En vertu de la *let. g*, le patient peut habiliter des professionnels de la santé de sa communauté de référence à transmettre leur droit d'accès à d'autres professionnels de la santé ou groupes de professionnels de la santé intervenant dans le traitement. Ces deux options sont disponibles indépendamment l'une de l'autre. Le professionnel de la santé habilité peut au plus transmettre des droits d'accès équivalents aux siens.

Chapitre 2 : Numéro d'identification du patient

Art. 5 Format

L'*al. 1* définit le format et la composition du numéro d'identification du patient visé à l'*art. 4 LDEP*. Le numéro d'identification du patient comporte 18 chiffres, dont une clé de contrôle, et sa structure est basée sur celle du «*Global Service Relation Number*» (GSRN) de GS1 (cf. figure). Le numéro de base comprend un code pays et un numéro de participant qui sert de référence à l'OFSP. Le numéro d'identification est un numéro à 10 chiffres, conformément à la structure de numérotation de GS1. Le premier chiffre de ce numéro sert à désigner l'application « dossier électronique du patient ». Le cercle de numéros peut ainsi être étendu à d'autres applications.

Position	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}
Désignation	Code de pays		Numéro du participant					DEP	Numéro d'identification									Clé de contrôle
Valeur	**7**	**6**	**1**	**3**	**3**	**7**	**6**	**1**	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	$\mathbf{I_7}$	$\mathbf{I_8}$	$\mathbf{I_9}$	**C**

Les numéros d'identification de patients sont gérés par la CdC, qui attribue un numéro unique à chaque patient à l'ouverture de son dossier électronique. C'est un numéro « muet » qui, en vertu de l'al. 1, ne doit donner aucune possibilité de tirer des conclusions sur le patient ou de déduire son numéro d'assuré au sens de l'*art. 50c LAVS* (NAVS13).

Les prescriptions relatives à la composition du numéro d'identification du patient et au calcul de la clé de contrôle sont fixées dans l'annexe 1 de l'ODEP-DFI.

Art. 6 Demande d'attribution

L'ouverture du dossier électronique incombe à la communauté de référence du patient (art. 15 ss.). C'est pour cette raison que *l'al. 1* prévoit que la communauté de référence est compétente pour demander le numéro d'identification auprès de la CdC, conformément à l'*art. 17, al. 1, let. d (cf. art. 4, al. 1, LDEP).* Le patient doit au préalable être identifié conformément à l'annexe 2 ODEP-DFI, ch. 8.2.1, let. a.

Les *al. 2 et 3* portent sur l'assurance de la qualité lors de l'octroi du numéro d'identification du patient. En principe, les données visées à l'*al. 2* devraient suffire pour identifier un patient de manière univoque dans la base de données d'identification de la CdC et lui attribuer un numéro d'identification. En cas de doute, la CdC peut demander des compléments d'information pour lever toute ambiguïté *(al. 3).*

Si le patient ne figure pas dans la base de données d'identification de la CdC et qu'il ne possède pas de numéro d'assuré au sens de l'art. 50*c* LAVS, la communauté de référence peut demander à la CdC un numéro d'assuré qui sert exclusivement à l'attribution au patient d'un numéro d'identification.

Art. 7 Consultation et saisie

La consultation du numéro d'identification du patient, processus qui inclut son attribution (art. 6) et son annulation (art. 8), peut s'effectuer par voie électronique.

Art. 8 Annulation

Lorsqu'un patient révoque son consentement, son dossier électronique du patient est supprimé conformément à l'art. 21. La CdC doit être informée de toute suppression d'un dossier électronique du patient ; le numéro d'identification du patient doit alors être annulé dans la base de données d'identification de la CdC puisqu'il constitue une composante du dossier électronique du patient (al. 1).Le numéro n'est dès lors plus disponible pour consultation au sens de l'art. 7*.*

En vertu de l'*al. 2*, la CdC communique les numéros d'identification de patient annulés aux communautés et aux communautés de référence dans un avis diffusé sur la plate-forme d'échange de données SEDEX (« *secure data exchange* ») de l'Office fédéral de la statistique (annexe 2 ODEP-DFI, ch. 2.9.29).

Selon l'*al. 3*, les numéros d'identification annulés ne sont pas réattribués, et ce, afin d'éviter les risques d'erreur de référencement. Le patient qui ouvre un nouveau dossier électronique après avoir révoqué un premier dossier se voit attribuer un nouveau numéro d'identification.

Chapitre 3 : Communautés et communautés de référence

Section 1 : Communautés

Les dispositions de cette section (art. 9 à 13) se réfèrent toujours, sauf mention contraire expresse, à des communautés et à des communautés de référence. Les dispositions de la section 2 (art. 14 à 21) et les commentaires qui s'y rapportent s'appliquent uniquement aux communautés de référence.

Art. 9 Identificateur d'objet et gestion

En vertu de l'*al. 1*, les communautés doivent demander un identificateur d'objet (*Object Identifier*, OID) au service de recherche de l'OID visé à l'art. 39, let. d, pour elles-mêmes et pour les institutions de santé qui leur sont affiliées (cf. commentaire relatif à l'art. 42).

En application de l'*al. 2*, les communautés doivent prévoir (c.-à-d. définir, documenter et communiquer) des mesures appropriées (directives, processus, méthodes, structures organisationnelles et responsabilités) et les appliquer, ou les prescrire et les faire respecter, pour assurer la bonne gestion des institutions de santé (par ex. hôpitaux, pharmacies, cabinets médicaux, organisations d'aide et de soins à domicile, EMS), des professionnels de la santé et des groupes de professionnels de la santé conformément aux exigences décrites ici.

Les ch. 1.2 à 1.6 des critères techniques et organisationnels de certification (annexe 2 ODEP-DFI) précisent les exigences applicables à la gestion des institutions de santé, des professionnels de la santé et de leurs auxiliaires ainsi que des groupes de professionnels de la santé.

<u>Gestion des institutions de santé</u>
En vertu de la *let. a*, les communautés doivent régler l'entrée ou la sortie des institutions de santé, des professionnels de la santé et des groupes de professionnels de la santé.

Le processus d'entrée inclut la conclusion d'une convention dans laquelle l'institution de santé s'engage à respecter les prescriptions de la communauté en matière d'organisation interne et, plus particulièrement, à remplir les tâches et les obligations qui lui sont imparties dans le domaine de la protection et de la sécurité des données (annexe 2 ODEP-DFI, ch. 1.2.2 et 4.9). Dans le cadre de

cette convention, une communauté peut en outre déléguer aux institutions de santé qui lui sont affiliées la responsabilité de certains critères de certification. C'est le cas en particulier de la gestion des professionnels de la santé et des groupes de professionnels de la santé qui travaillent dans ces institutions (al. 2, let. a à d). L'entrée, la mutation et la sortie des données d'un professionnel de la santé ne peuvent être traitées que si l'institution de santé pour laquelle il travaille est déjà affiliée à la communauté.

Par ailleurs, lorsqu'une institution de santé quitte une communauté sans s'affilier à une autre communauté ou communauté de référence, la communauté en question doit veiller à ce que les données médicales saisies par l'institution de santé sur ses propres supports de données pour le dossier électronique du patient restent accessibles (annexe 2 ODEP-DFI, ch. 1.2.3 let. b).

Selon la *let. d*, les communautés doivent s'assurer que les données relatives aux institutions de santé qui leur sont affiliées figurant dans le service de recherche central des institutions de santé et des professionnels de la santé visé à l'*art. 41* sont à jour ou sont régulièrement actualisés par les institutions de santé. La mise à jour des données enregistrées dans le service de recherche central doit être effectuée sans délai, car c'est sur ces données que repose l'attribution des droits d'accès aux professionnels de la santé et aux groupes de professionnels de la santé. Les communautés peuvent déléguer cette tâche aux institutions de santé, mais elles restent responsables de l'exactitude et de l'actualité des données enregistrées et doivent veiller à ce que les modifications soient apportées dans un délai convenable (dans la plupart des cas, la mise à jour devra vraisemblablement être quotidienne) (annexe 2 ODEP-DFI, ch. 1.2.4).

Les prescriptions relatives à la tenue d'un inventaire des moyens informatiques et des recueils de données selon l'*art. 12*, *al. 1*, *let. b*, ainsi que les précisions apportées à l'annexe 2 ODEP-DFI, ch. 4.6, stipulent en outre que les communautés doivent tenir cet inventaire à jour dans le cadre de leur gestion des institutions de santé (entrées, mutations, départs).

Gestion des professionnels de la santé

En application de la *let. a*, les communautés doivent définir, documenter, mettre en œuvre et respecter des processus appropriés pour gérer les professionnels de la santé qui sont pressentis pour accéder au dossier électronique du patient dans les institutions de santé qui leur sont affiliées. En plus des exigences visées aux *let. b*, *d*, *e et f*, ces processus doivent garantir le respect d'autres prescriptions (annexe 2 ODEP-DFI, ch. 1.3, 1.4, 1.6 et 4.7). Elles doivent en particulier régir l'information des professionnels de la santé sur leurs tâches, leurs droits et leurs obligations en lien avec le traitement des données du dossier électronique du patient (annexe 2 ODEP-DFI, ch. 4.7.1) ainsi que sur les risques et les mesures à prendre dans le domaine de la protection et de la sécurité des données. Les communautés doivent en outre mettre en place des procédures visant à recueillir le consentement des professionnels de la santé à l'égard des directives spécifiques de la communauté et des directives spécifiques en découlant adoptées par les institutions de santé (annexe 2 ODEP-DFI, ch. 1.2.2, let. b).

Il faut également définir la procédure concrète à suivre lorsqu'un professionnel de la santé quitte une communauté (par ex. suite à un changement d'emploi, à une cessation d'activité professionnelle ou à un décès). En cas de sortie, mais aussi de changement du champ d'activité à l'intérieur de la communauté, il convient de vérifier en particulier si les conditions d'accès au dossier électronique du patient sont toujours remplies (cf. la définition du professionnel de la santé au sens de l'art. 2, let. b, LDEP). Dans le cas contraire, les possibilités d'accès (« *login* ») au dossier électronique du patient doivent être bloquées immédiatement (annexe 2 ODEP-DFI, ch. 1.3.5, let. b). L'entrée, la mutation et la sortie des données d'un professionnel de la santé ne peuvent être traitées que si l'institution de santé pour laquelle il travaille est déjà affiliée à la communauté. Celle-ci peut déléguer la tâche de gestion des professionnels de la santé aux institutions de santé qui leur sont affiliées.

L'identification des professionnels de la santé visée à la *let. b* doit respecter les critères énoncés à l'art. 24, sauf si elle peut être effectuée avec un moyen d'identification émis par un éditeur certifié selon l'art. 31. La communauté doit en outre s'assurer que la personne qui participe au traitement des patients est bien un professionnel de la santé au sens de l'art. 2, let. b, LDEP (annexe 2 ODEP-DFI, ch. 1.3.3, let. c), c'est-à-dire un professionnel reconnu au sens du droit fédéral ou cantonal. À cet effet, elle peut utiliser soit un moyen d'identification émis par un éditeur qui a vérifié la qualification du professionnel lors de la procédure d'émission conformément à l'art. 25, al. 3, soit se fonder sur l'inscription dans un registre professionnel cantonal ou fédéral (par ex. Registre des professions médicales universitaires [MedReg], du Registre des professions de la psychologie [PsyReg] ou du Registre national des professions de la santé [NAREG]). Pour les professionnels de la santé qui sont reconnus au sens du droit fédéral ou cantonal, mais ne sont inscrits dans aucun des registres professionnels fédéraux ou cantonaux existants, des procédures de vérification des diplômes peuvent au besoin être fixées avec les associations professionnelles cantonales ou nationales.

En vertu de la *let. c*, les communautés doivent attribuer aux groupes de professionnels de la santé un OID qui se fonde sur l'OID de l'institution de santé au sens de l'*al. 1* (cf. commentaire relatif à l'art. 42). L'octroi et l'attribution de l'OID à un groupe s'effectuent sous la propre responsabilité de la communauté. La communauté crée d'autres OID à cette fin dans le cadre de la structure de l'institution de santé et les attribue à des groupes de cette institution pour leur inscription au service de recherche central des institutions de santé et professionnels de la santé conformément à la *let. d*.

Aux termes de la *let. d*, les données des professionnels de la santé doivent être enregistrées, mises à jour et effacées s'il y a lieu dans le service de recherche central des institutions de santé et des professionnels de la santé visé à l'art. 41. Si le professionnel de la santé est inscrit dans un registre professionnel fédéral ou cantonal (par ex. MedReg, NAREG, etc.), les informations du registre doivent être reprises dans le service de recherche (annexe 2 ODEP-DFI, ch. 1.2.2, let. d). Les renseignements à reprendre (supplément 1 à l'annexe 5 de l'ODEP-DFI, ch. 1.9.5.1.2) comprennent le nom, le prénom et le GLN du professionnel de la santé. Il est important, en particulier, de s'assurer que seuls sont inscrits dans le service de recherche des professionnels de la santé qui répondent à la définition de l'art. 2, let. b, LDEP, qui travaillent pour l'institution de santé affiliée concernée et qui ont besoin d'avoir accès à des dossiers électroniques. La communauté doit veiller à ce que l'actualité et l'exactitude des données enregistrées chez elle soient régulièrement vérifiées par ses soins ou par l'institution de santé responsable des données (annexe 2 ODEP-DFI, ch. 1.2.4). Ces tâches peuvent, elles aussi, être déléguées aux institutions de santé affiliées à la communauté, mais celle-ci reste responsable de l'exactitude et de l'actualité des données enregistrées.

En vertu de la *let. e*, les professionnels de la santé ne peuvent accéder au dossier électronique du patient qu'avec un moyen d'identification valable, émis par un éditeur certifié conformément à l'art. 31 (annexe 2 ODEP-DFI, ch. 1.4.3). Peu importe que l'accès ait lieu via le portail d'accès pour les professionnels de la santé (art. 11) ou via d'autres systèmes (par ex. un accès intégré dans le système primaire). Cela signifie que toutes les voies d'accès au dossier électronique du patient utilisées par les professionnels de la santé ou leurs auxiliaires doivent supporter une procédure d'authentification forte, conforme aux progrès techniques et comportant au moins deux facteurs d'authentification. Une telle procédure d'authentification n'est obligatoire que pour le traitement des données du dossier électronique du patient. Une authentification d'autres communautés certifiées conforme à une telle procédure peut être reconnue comme fiable pour le traitement intercommunautaire de données du dossier électronique du patient.

Les communautés doivent établir un lien fiable entre l'identificateur univoque visé à l'art. 25, al. 1, et l'identité de chacun des professionnels de la santé et des auxiliaires enregistrés dans la communauté (annexe 2 ODEP-DFI, ch. 1.4.2 ; « phase d'enregistrement »).

Les professionnels de la santé peuvent confier le traitement des données du dossier électronique du patient à des auxiliaires. Afin de protéger leurs droits de la personnalité, les auxiliaires ne sont pas

enregistrés dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 41. De ce fait, les patients ne peuvent pas gérer leurs droits d'accès de manière indépendante avec la fonction de gestion des autorisations. Le rattachement d'un auxiliaire à un professionnel de la santé doit néanmoins être géré à l'intérieur de la communauté afin que l'auxiliaire bénéficie des droits d'accès du professionnel de la santé responsable et que ses traitements de données puissent être historisés. L'identification des auxiliaires et leur accès aux dossiers électroniques sont soumis aux dispositions de l'*art. 9, al. 2, let. b et e* (annexe 2 ODEP-DFI, ch. 1.3).

Gestion de groupes de professionnels de la santé

Selon la *let. d*, les communautés doivent assurer la gestion des groupes de professionnels de la santé dans le service de recherche central des institutions de santé et des professionnels de la santé visé à l'art. 41. Elles peuvent déléguer cette tâche aux institutions de santé qui leur sont affiliées, mais demeurent responsables de l'exactitude et de l'actualité des données enregistrées.

Le patient peut aussi attribuer des droits d'accès à des groupes de professionnels de la santé (art. 2, al. 1).Le professionnel de la santé qui intègre un groupe ultérieurement reçoit les droits d'accès accordés à son groupe (art. 2, al. 3), mais seulement si le patient ne l'a pas exclu de tout accès à son dossier électronique (art. 4, let. b).

La *let. f* précise à ce propos que les patients doivent, à leur demande, être informés de l'intégration de professionnels de la santé dans un groupe. L'information peut s'effectuer automatiquement par voie électronique.

Les communautés devraient définir la composition et la taille des groupes de telle manière que les patients puissent gérer convenablement leurs droits d'accès. En particulier, il ne faudrait pas qu'un nombre disproportionné de professionels de la santé sans rapport concret avec le traitement d'un patient partage le droit d'accès accordé à un groupe de professionnels de la santé. De manière générale, les communautés et les institutions de santé qui leur sont affiliées doivent convenir de la manière dont elles entendent organiser en interne les possibilités d'accès au dossier électronique du patient et, partant, définir quels sont les professionnels de la santé qui ont besoin d'un tel accès et comment les gérer par groupes le cas échéant. Le plan concret de mise en œuvre doit respecter le principe de proportionnalité et être adapté à l'accomplissement des tâches. Comme les parcours thérapeutiques, par exemple dans les hôpitaux, s'étendent souvent sur plusieurs unités organisationnelles (par ex. admission en urgence → laboratoire → radiologie→ unité de lits en médecine interne), il peut être judicieux de composer les groupes de manière à assurer une combinaison appropriée de professionnels de la santé de toutes les unités impliquées. Une autre option concevable serait de définir des groupes ayant pour fonction première de ne reprendre que les données médicales dans le système primaire. On pourrait définir par exemple, pour les grands services ou unités cliniques d'un hôpital, des groupes de composition majoritairement stable qui puissent assurer la disponibilité continue des personnes qui le composent. Les membres d'un tel groupe pourraient alors transférer les données médicales pertinentes pour le traitement dans le système primaire de l'hôpital lors de l'admission du patient et les rendre ainsi accessibles aux professionnels de la santé participant à son traitement dans l'institution de santé. Il n'est donc ni nécessaire, ni vraiment utile tant sur le plan pratique que du point de vue du patient, de tenir à jour les plans de service de chacun des services internes d'un hôpital ou d'un EMS dans le service de recherche des données pour institutions de santé et professionnels de la santé. Dans les organisations d'aide et de soins à domicile, les groupes peuvent être de taille variable selon le modèle de soins choisi (personnel effectuant des roulements ou personne de référence).

Art. 10 Tenue et transfert des données

Mise en œuvre de la gestion des autorisations

En vertu de l'*al. 1*, *let. a*, les communautés doivent mettre en œuvre la gestion des autorisations de manière à ce que les prescriptions énoncées à l'art. 9 LDEP et les dispositions relatives à l'attribution

des niveaux de confidentialité et à l'accès pour urgence médicale visées aux *art. 1 et 2, al. 2, ODEP* soient appliquées correctement et respectées (annexe 2 ODEP-DFI, ch. 2.1 à 2.3). Les communautés sont en particulier tenues d'appliquer aux données qu'elles détiennent du dossier électronique celui des niveaux de confidentialité (art. 1) que le patient leur a attribué via le portail d'accès de la communauté de référence (annexe 2 ODEP-DFI, ch. 2.3.1).

Les communautés ont également l'obligation de veiller à ce que l'accès aux données enregistrées dans dans leurs lieux de stockage des documents et dans leur registre de documents ne puisse avoir lieu qu'après obtention de la décision d'accès de la part de la communauté de référence du patient (annexe 2 ODEP-DFI, ch. 2.3). À titre de sécurité supplémentaire, par exemple pour repousser les tentatives d'interception (attaques de type *man-in-the-client*), l'annexe 2 ODEP-DFI, ch. 2.2, prévoit que les accès pour urgence médicale doivent être confirmés d'une manière qui empêche efficacement les abus, causés notamment par des logiciels malveillants installés sur le terminal. Cela peut se faire par exemple moyennant l'ajout d'une interaction manuelle, non reproductible automatiquement (par ex. la saisie d'un mot de passe à usage unique ou d'un identifiant personnel (NIP) généré par un dispositif à jetons local ou *token*).

Comme la mise en œuvre de la gestion des autorisations et le respect des droits d'accès accordés sont critiques pour la garantie de la protection des données, il faut que les fonctionnalités et l'évaluation des règles en place pour la gestion des autorisations puissent être contrôlées dans le cadre de la procédure de certification (annexe 2 ODEP-DFI, ch. 2.3.2).

Lieux de stockage des données

Pour des raisons de protection et de sécurité des données, la *let. b* prévoit que les données médicales du dossier électronique du patient doivent impérativement être enregistrées séparément des autres données de la communauté ou de ses institutions de santé afin d'empêcher leur usage illicite à d'autres fins. Est notamment illicite le transfert de données médicales de ou vers des lieux de stockage de documents par des personnes autres que des professionnels de la santé. En revanche, la transmission directe de données médicales à d'autres professionnels de la santé ou institutions de santé à l'aide d'éléments de l'infrastructure informatique du dossier électronique du patient est admise si le destinataire est également membre d'une communauté certifiée.

Le but de cette réglementation est de maintenir une séparation au moins logique entre les données médicales du dossier électronique du patient et les autres données (annexe 2 ODEP-DFI, ch. 2.4, let. b) et de sauvegarder ainsi les données médicales saisies dans les systèmes primaires des institutions de santé en les copiant sur des supports *ad hoc*. Cette séparation s'impose, entre autres du fait que les données du dossier électronique du patient, d'une part, sont soumises à d'autres règles de conservation et d'effacement que les données des systèmes primaires et, d'autre part, sont complètement – ou, à la demande du patient (al. 2, let. c), sélectivement – détruites après suppression du dossier électronique du patient (al. 1, let. e).

De plus, un lieu de stockage sans véritable séparation des données constituerait un risque disproportionné pour la protection et la sécurité des données, vu qu'il serait impossible d'isoler suffisamment bien de tels systèmes par rapport à de grands groupes d'utilisateurs et espaces réseau, ce qui créerait un risque de diffusion incontrôlée de données entre le dossier électronique du patient et les autres données.

Un enregistrement à part doit assurer par exemple que les personnes disposant de droits d'accès privilégiés au système d'exploitation ou à la base de données du système primaire ne peuvent pas accéder du même coup aux données médicales du dossier électronique du patient et à d'autres ensembles de données. Que la séparation soit physique (matériel dédié, centres de calcul distincts), logique (par ex. bases de données séparées, ordinateurs virtuels, isolement cryptographique, etc.) ou résulte d'une combinaison de plusieurs mesures, les lieux de stockage doivent pouvoir être isolés de manière étanche aux différents niveaux techniques. Une perméabilité accidentelle (défaut d'isolation)

résultant d'une défaillance technique ou créée par un logiciel malveillant ou une action humaine illicite doit être empêchée au maximum par des moyens techniques appropriés, complétés le cas échéant par des mesures organisationnelles.

Il est possible d'obtenir un enregistrement à part suffisant par cryptage au niveau des applications si les clés des ensembles de données sont gérées de manière à protéger ceux-ci des accès non autorisés. Cela permet aussi des utilisations hybrides d'ensembles de données sur le même matériel, le même système d'exploitation et avec les mêmes bases de données. Outre les procédures (saisies, téléchargements) prévues pour les professionnels de la santé, il ne peut exister qu'un rôle supplémentaire doté de privilèges système permettant un transfert autorisé de données entre le dossier électronique du patient et d'autres ensembles de données. Afin de réduire encore ce risque résiduel de transfert illicite de données, les accès à ces données ou les clés d'application correspondantes doivent être adéquatement sécurisés et protégées par ex. par des mesures organisationnelles supplémentaires (« *segregation of duties* », principe du double contrôle).

Cryptage

La *let. c* prévoit que les communautés doivent utiliser pour le stockage et le transfert de données des méthodes de cryptage appropriées (procédés cryptographiques conformes aux progrès techniques) afin de prévenir toute perte de confidentialité, d'authenticité et d'intégrité de ces données (annexe 2 ODEP-DFI, ch. 4.12 ; cf. commentaire relatif à l'art. 12, al. 4).

Destruction des données

La *let. d* fixe à vingt ans le délai au bout duquel les données enregistrées dans le dossier électronique du patient par les professionnels de la santé doivent être détruites. Le but de cette réglementation est d'assurer la disponibilité des données médicales pendant un temps suffisant. Les données enregistrées par les patients ne sont soumises à aucun délai d'effacement. En application de l'*al. 2*, *let. b*, des données peuvent être exclues de cette destruction à la demande du patient. Les patients peuvent ainsi veiller à ce que des données pertinentes pour le traitement sur une très longue durée (maladies chroniques ou congénitales, par ex.) restent disponibles dans leur dossier électronique au-delà de ce délai.

Dans des cas exceptionnels justifiés techniquement, notamment ceux de systèmes d'archivage de fichiers comportant un très gros volume de données tels qu'ils sont souvent générés par des méthodes d'imagerie en radiologie, par exemple, les données ou documents médicaux n'ont pas à être mis en ligne en copie mais peuvent être ouverts directement dans les archives intégrées aux systèmes primaires. Dans ces cas, les règles de suppression des données visées à l'*al. 1, let. d et e,* ainsi qu'à l'*al. 2, let. c,* s'appliquent uniquement à l'inscription correspondante dans le registre de documents.

En vertu de la *let. e*, une suppression du dossier électronique du patient aux termes de l'*art. 21, al. 1,* doit avoir pour effet de rétablir l'état existant avant la création du dossier. Cela implique de supprimer toutes les données du patient de tous les systèmes consultables de la communauté (registres de documents, archives de documents, index des patients, etc.) et d'effacer de tous les systèmes le numéro d'identification du patient (annexe 2 ODEP-DFI, ch. 2.6, let. b). La responsabilité d'informer les autres communautés de la suppression du dossier électronique d'un patient (art. 21, al 3) incombe à la communauté de référence du patient. Les données historisées et les données contenues dans les systèmes primaires non consultables et les sauvegardes ne sont pas concernées.

En vertu du droit à l'autodétermination informationnelle, le patient peut décider lui-même du contenu de son dossier électronique et dispose pour cela des options mentionnées à l'*al. 2* (annexe 2 ODEP-DFI, ch. 2.7).

Options données au patient

Selon l'art. 3, al. 2, LDEP, les professionnels de la santé peuvent partir du principe que les patients

qui ont créé un dossier électronique souhaitent que leurs données y soient enregistrées. Selon l'*al. 2, let. a*, ODEP, le patient peut réfuter cette présomption au cas par cas et demander à tout moment à des professionnels de la santé de ne pas enregistrer certaines données médicales le concernant dans son dossier électronique. En règle générale, le patient fera usage de cette possibilité dans le cas concret où il sera mis en contact avec une institution de santé pour un traitement. Les communautés ont cependant la responsabilité de veiller au respect de ces dispositions et d'exiger leur application dans les institutions de santé.

Selon l'*al. 2, let. b*, le patient peut à tout moment exiger que certaines données soient exceptées de la suppression visée à l'al. 1, let. d, et restent ainsi disponibles pour une durée indéterminée.

L'*al. 2, let. c*, donne au patient le droit de faire effacer certaines données le concernant dans son dossier électronique. Techniquement, cela peut se faire à l'aide d'une fonction prévue à cette fin sur le portail d'accès de la communauté de référence du patient. Les communautés sont tenues d'exécuter en conséquence une telle instruction (transaction *Delete Document Set* [ITI-62] du « profil d'intégration IHE » *XDS Metadata Update* ; annexe 2 ODEP-DFI, ch. 2.9.13 et 2.9.14). Les inscriptions correspondantes dans les registres de documents doivent alors être effacées, de même que les données médicales contenues dans les lieux de stockage du dossier électronique du patient. En ce qui concerne les données médicales (par ex. des fichiers d'imagerie radiologique) que l'on consulte directement dans les lieux de stockage des systèmes primaires, seules les entrées correspondantes dans le registre de documents seront effacées pour ne pas enfreindre les obligations de documentation et de conservation auxquelles sont tenus les professionnels de la santé.

Prescriptions techniques relatives au transfert des données

Pour garantir l'interopérabilité ainsi que la sécurité et la protection des données conformément aux dispositions en vigueur lors des opérations de mise en ligne et de consultation, les communautés doivent se conformer aux prescriptions en matière de gestion et de transfert des données du dossier électronique du patient visées à l'*al. 3*, *let. a à d*. Ces prescriptions concrètes portent, par exemple, sur les types de supports admis (dont l'annexe 3 ODEP-DFI, ch. 8, donne une liste exhaustive), sur la recherche de patients dans l'index des patients, sur la communication avec le registre des documents, les archives de documents et la gestion des autorisations ainsi que sur la communication avec l'éditeur du moyen d'identification et avec les services de recherche visés aux art. 40 et 41. Le respect de ces règles essentielles pour l'interopérabilité, mais aussi pour la protection et la sécurité des données, est contrôlé dans le cadre de la procédure de certification pratiquée par les organismes compétents à l'aide d'un système de certification mis à disposition par l'OFSP (art. 28, al. 4). Ces exigences garantissent une interopérabilité technique et sémantique assurant une bonne communication entre toutes les composantes du système, mais aussi que chaque communauté dispose des mêmes interfaces standardisées pour les systèmes primaires à raccorder. Un adaptateur logiciel (« *eHealth-Connector* ») a été mis à la disposition des fabricants pour faciliter le raccordement conforme de systèmes primaires non compatibles IHE avec les interfaces à l'intérieur d'une communauté. Cet adaptateur est inutile pour les produits déjà équipés des fonctionnalités requises. Un raccordement standardisé avec les interfaces dans les communautés peut être considéré par les fournisseurs, les utilisateurs et les communautés comme une protection des investissements, qu'ils auront la garantie de pouvoir réutiliser.

Métadonnées

Les métadonnées décrivent de manière structurée (par ex. format technique du fichier, type de fichier, auteur, date de création, niveau de confidentialité) les données médicales ou les documents mis en ligne dans le dossier électronique du patient. Selon la *let. a*, il faut utiliser à cet effet les attributs et leurs valeurs ou les ensembles de valeurs définis à l'annexe 3 ODEP-DFI. Il s'agit en grande partie de listes de valeurs employées dans des codes sémantiques standardisés (par ex. la terminologie *Snomed CT*), qui permettent d'assurer une interopérabilité sémantique des métadonnées se rapportant aux données médicales. Pour que les métadonnées puissent être utilisées de manière uniforme dans l'ensemble de la Suisse et qu'un soutien technique soit garanti, la Confédération gère

un service de recherche des métadonnées autorisées selon l'*art. 39, let. c*. Seules les caractéristiques (code et désignation anglaise) énumérées à l'annexe 3 ODEP-DFI sont déterminantes sur le plan normatif. Les traductions dans les langues nationales et d'autres langues ainsi que les termes utilisés dans le langage courant seront publiés par eHealth Suisse sous forme de listes de synonymes.

Tous les types de données médicales qu'il est possible de classifier au moyen des métadonnées peuvent être mis en ligne sous la forme de documents non structurés (par ex. fichiers d'images ou PDF/A). Par contre, la *let. c* impose l'emploi des formats d'échange de données médicales prescrits à l'annexe 4 ODEP-DFI pour la mise en ligne de données médicales structurées par les professionnels de la santé.

Profils d'intégration

En vertu de la *let. c*, le transfert d'informations intra- et intercommunautaire doit utiliser les transactions des profils d'intégration listés dans l'annexe 5 ODEP-DFI : il s'agit de profils d'intégration conçus par *Integrating the Healthcare Enterprise* (IHE) avec les adaptations nationales (*national extensions*) correspondantes, ainsi que de profils d'intégration nationaux conçus par le DFI pour des cas d'application spécifiques. Un profil d'intégration est un guide technique pour l'exécution d'un cas d'application spécifique, qui garantit une interopérabilité technique et qui repose généralement sur des normes et des standard reconnus.

Les « profils d'intégration IHE » listés au ch. 1 de l'annexe 5 ODEP-DFI sont internationalement reconnus et donc conçus pour un usage universel. Afin que la plupart des exigences concrètes figurant dans la LDEP et le présent droit d'exécution puissent être respectées, il est nécessaire de les préciser davantage dans des spécifications et de les compléter (« adaptations nationales »). Elles stipulent, par exemple, que certaines recherches peuvent être effectuées en utilisant uniquement comme identificateur le numéro d'identification du patient, et non le NAVS13. L'annexe 5 ODEP-DFI, ch. 2, prévoit en outre des profils d'intégration nationaux conçus par le DFI pour tenir compte des particularités de l'architecture élaborée par eHealth Suisse pour le dossier électronique du patient, comme par exemple la décentralisation de la tenue des données et de la gestion des patients. Ainsi, le profil d'intégration national CH:ADR (*Authorisation Decision Request*) précise comment les informations requises pour obtenir une autorisation doivent être communiquées à la communauté de référence compétente pour décider d'accorder ou non l'accès, et comment le résultat de l'évaluation des règles (décision sur l'accès) est renvoyé à la communauté dont émane la demande. Le profil d'intégration national CH:PPQ (*Privacy Policy Query*), quant à lui, permet la modification de la configuration de gestion des autorisations par les patients et par les professionnels de la santé habilités. Ce profil d'intégration national comprend le format d'échange technique à utiliser pour importer la configuration de la gestion des autorisations en cas de changement de communauté de référence.

Les exigences communes à tous les profils d'intégration portent en particulier sur la garantie de l'intégrité et de la confidentialité des données transmises. Ainsi, pour garantir l'intégrité des messages électroniques, il faut employer des c*ertificats électroniques fiables permettant de vérifier l'authenticité des messages (*annexe 2 ODEP-DFI, ch. 2.9.21, let. b, 2.9.26, 2.9.28, let. b, et 2.9.29). Pour les mêmes raisons, l'horodatage des communications et des historiques doit utiliser l'heure légale diffusée en Suisse *par l'Institut fédéral de métrologie (METAS).* Les horloges de tous les systèmes informatiques pertinents doivent donc être synchronisées avec l'heure légale en Suisse (annexe 2 ODEP-DFI, ch. 2.9.30).

Données historisées

En application de l'art. 10, al. 1, let. b, LDEP, chaque traitement de données doit être consigné dans un historique. Pour que la protection des données puisse être contrôlée, en particulier par le patient, il faut offrir une traçabilité appropriée du traitement des données figurant dans le dossier électronique du patient grâce à une historisation claire et non modifiable de tous les événements pertinents pour la protection des données.

Les événements consignés dans l'historique sont notamment : la mise en ligne et la requête de données médicales, la modification de métadonnées (par ex. niveau de confidentialité), les modifications de la configuration de la gestion des autorisations ainsi que les décisions d'authentification et d'autorisation, y compris les données sur lesquelles se fondent ces décisions. Les historiques dans lesquels sont consignés les événements doivent contenir des informations sur qui a accédé à quelles données ou a créé quelles données, quand et comment. Lors de l'historisation, il convient de faire la distinction entre les accès résultant de l'utilisation du dossier électronique du patient et les accès technico-administratifs dans le cadre de l'exploitation du système (annexe 2 ODEP-DFI, ch. 4.13.3). Les exigences relatives aux données historisées consultables par les patients selon la *let. d* sont précisées à l'annexe 2 ODEP-DFI, ch. 2.10.

Ces données doivent être conservées durant dix ans en les protégeant par des moyens techniques ou organisationnels propres à empêcher toute possibilité de modification, puis supprimées à l'échéance (annexe 2 ODEP-DFI, ch. 2.10.7 et 2.10.8).

D'autres exigences d'historisation pertinentes à la protection et à la sécurité des données ont été fixées en relation avec l'art. 12, al. 4 pour des événements survenus lors de l'exploitation du système et sont précisées à l' annexe 2 ODEP-DFI, ch. 4.13.3, mais ne sont pas mises en ligne pour consultation par les patients. Les autres historisations effectuées dans le cadre de l'exploitation technique, qui sont sans rapport avec la protection ou la sécurité des données (par ex. enregistrement de paramètres d'exploitation ou d'autres grandeurs telles que fréquence des requêtes, temps de réponse ou volumes de données transmises) ne sont pas visées par ces prescriptions, mais peuvent être importantes pour l'identification d'incidents de sécurité au sens de l'*art. 12, al. 1, let. a*.

Pour que les patients puissent consulter à tout moment les historiques constitués de manière décentralisée, les communautés doivent mettre en ligne les données historisées, sous une forme consultable, sur le portail d'accès dédié aux patients (art. 18). Les adaptations nationales des profils d'intégration (profils IHE ATNA, XDS.b et XCA) pour la consultation des données historisées, qui sont listées l'annexe 5 ODEP-DFI, ch. 2, spécifient les transactions et le format technique d'échange à employer (annexe 2 ODEP-DFI, ch. 2.10.9). Le patient est ainsi à même de vérifier en permanence qui a accédé à son dossier électronique du patient et, en cas d'accès non autorisé, il peut engager une démarche juridique (cf. art. 24 LDEP).

L'*al. 4* prévoit que le DFI peut renoncer à faire traduire et à publier officiellement les annexes de l'ODEP-DFI, qui ne sont alors mentionnées que par titre et par référence. En vertu de l'art. 5, al. 1, de la loi fédérale du 18 juin 2004 sur les publications officielles (LPubl)[7], ne sont pas publiés dans le RO les textes qui ne touchent qu'un nombre restreint de personnes, ont un caractère technique et ne s'adressent qu'à des spécialistes, ou doivent être publiés dans un format qui n'est pas adapté à une publication dans le RO. Ces textes sont mis en ligne sur le site Internet de l'OFSP. Dans le cas de l'ODEP-DFI, on renonce à la publication des annexes 2 (Critères techniques et organisationnels de certification applicables aux communautés et aux communautés des référence), 3 (Métadonnées), 4 (Formats d'échange), 5 (Adaptations nationales des profils d'intégration et profils d'intégration nationaux) et 8 (Critères techniques et organisationnels de certification applicables aux éditeurs de moyens d'identification). Les annexes 5 et 8 en particulier sont des textes extrêmement techniques qui s'adressent à un cercle de destinataires très restreint, en l'occurrence les spécialistes responsables de l'implémentation des exigences techniques. En application de l'art. 14, al. 2, let. b, LPubl, on renonce en outre à traduire les annexes 3, 4, 5 et 8 dans les langues officielles vu que les personnes concernées les utilisent exclusivement dans la langue universellement en usage dans ce domaine, à savoir l'anglais. On courrait le risque d'erreurs d'interprétation et de perte d'informations à vouloir les traduire (art. 10, al. 4).

[7] RS **170.512**

L'art. 12, al. 2, LDEP prévoit que le Conseil fédéral peut habiliter l'OFSP à adapter les exigences de certification aux progrès techniques, mais il est de toute évidence plus judicieux que le DFI désigne spécifiquement les normes que l'OFSP doit adapter (al. 5).

Art. 11 Portail d'accès pour les professionnels de la santé

Le portail d'accès pour les professionnels de la santé doit satisfaire aux exigences énoncées à l'annexe 2 ODEP-DFI, ch. 3. Il faut par ex. que la présentation des données médicales du dossier électronique du patient reflète l'ensemble des informations pertinentes de manière correcte et exhaustive (annexe 2 ODEP-DFI, ch. 3.1). Cela s'applique en particulier à la présentation des données structurées, comme par exemple des formats d'échange de données médicales visés à *l'art. 10, al. 3, let. b*. Le portail d'accès doit en outre indiquer clairement si les données médicales ont été mises en ligne par un professionnel de la santé ou par le patient lui-même, quelles sont celles qui ne sont plus valables ou s'il existe éventuellement d'autres versions. Les professionnels de la santé qui ont mis en ligne des données médicales ne peuvent plus les supprimer, ceci afin d'en assurer la traçabilité. Ils peuvent cependant leur ajouter l'information statutaire « annulé » (*deprecated*). Cela permet par exemple de remplacer des données médicales contenant des informations erronées ou caduques par des données corrigées ou mises à jour. Les patients, mais aussi les autres professionnels de la santé, devraient toujours voir s'afficher uniquement la toute dernière version non annulée des données médicales ou d'un document sur le portail d'accès. L'historique des versions devrait cependant être également disponible au besoin.

Les portails d'accès doivent être conçus de manière à faciliter l'accès des personnes limitées en raison d'un handicap, de l'âge ou de la langue et offrir, par exemple, un logiciel de lecture vocale et des fonctionnalités accessibles sans souris. La norme déterminante est le niveau de conformité AA des Règles pour l'accessibilité des contenus 2.0 (*Web Content Accessibility Guidelines 2.0*). Comme beaucoup de ces règles améliorent la facilité d'utilisation en général, leur respect est un plus pour l'ensemble des utilisateurs (annexe 2 ODEP-DFI, ch. 3.2).

Pour des raisons d'interopérabilité et de sécurité des données, l'annexe 3 ODEP-DFI, ch. 8, donne une liste exhaustive des types de supports et des formats de fichiers admis dans le dossier électronique du patient (annexe 2 ODEP-DFI, ch. 3.3). Le portail d'accès doit offrir la possibilité de mettre en ligne, de rechercher et d'afficher les contenus de ces types de supports. D'autres exigences sont, d'une part, de pouvoir télécharger des données ou documents médicaux individuellement ou sous forme de sélection groupée (annexe 2 ODEP-DFI, ch. 3.3, let. c) et, d'autre part, d'avoir l'assurance que des formats d'échange comportant des données médicales structurées puissent non seulement être affichés et téléchargés sous une forme directement lisible (annexe 2 ODEP-DFI, ch. 3.3, let. d), mais soient aussi récupérables pour un éventuel traitement structuré dans leur format original (annexe 2 ODEP-DFI, ch. 3.3, let. e).

Pour que les professionnels de la santé soient en mesure de remplir leur obligation de documentation, le portail d'accès doit comporter une fonction de téléchargement permettant de sauvegarder des données médicales sur le système primaire des institutions de santé. Pour des raisons de sécurité, il importe de définir pour la recherche et le téléchargement de données médicales des limites supérieures exprimées en nombre de fichiers individuels (*rate limits*), dont le dépassement déclenche un dispositif de blocage adéquat ou des mesures de sécurité supplémentaires (annexe 2 ODEP-DFI, ch. 3.3, let. f). Un dépassement du plafond autorisé pourrait, par exemple, imposer de compléter d'abord un captcha (*completely automated public turing test to tell computers and humans apart*) afin de limiter les requêtes en masse illicites automatisées par des procédés techniques.

Art. 12 Protection et sécurité des données

L'*al. 1* impose aux communautés d'avoir un système de gestion de la protection et de la sécurité des données adapté aux risques, tel que décrit dans la norme ISO/IEC 27001:2013. Un système de gestion de la protection et de la sécurité des données conforme à la norme ISO/IEC 27001:2013 vise

à appréhender de manière coordonnée l'ensemble des risques pour la protection et la sécurité des données qui peuvent se présenter dans une communauté, permettant ainsi de planifier, de mettre en place, de contrôler et d'améliorer un ensemble complet de mesures de sécurité appropriées (directives, processus, procédures, structures organisationnelles ou encore fonctionnalités logicielles ou matérielles, etc.) dans le cadre d'un système de gestion intégré. Il doit être adapté à la complexité et à la taille de la communauté et, surtout, au volume des données particulièrement sensibles (notamment médicales) enregistrées par la communauté dans les dossiers électroniques de ses patients (annexe 2 ODEP-DFI, ch. 4.2.3).

Les communautés demeurent responsables d'assurer le respect des dispositions de cet article même lorsqu'elles confient des prestations à des entreprises sous-traitantes (annexe 2 ODEP-DFI, ch. 4.1).

Système de gestion de la protection et de la sécurité des données

Le système de gestion de la protection et de la sécurité des données des communautés doit définir et mettre en œuvre des mesures appropriées pour assurer la conformité aux présentes dispositions. Pour cela, il doit définir les responsabilités générales et spécifiques de gestion de la protection et de la sécurité des données, désigner les responsables respectifs et protéger de la perte, de la destruction et des falsifications toutes les notes prises en relation avec ces tâches.

Outre les éléments énoncés aux *let. a à c*, le système de gestion de la protection et de la sécurité des données des communautés doit comporter notamment un catalogue et un plan de traitement des risques (annexe 2 ODEP-DFI, ch. 4.2.3).

La *let. a* impose la mise en place de procédures techniques et organisationnelles de détection et de gestion des incidents de sécurité (annexe 2 ODEP-DFI, ch. 4.3). Comme il est impossible d'assurer une sécurité totale *a priori*, il est d'autant plus important de pouvoir au moins détecter rapidement les éventuels incidents de sécurité *a posteriori* pour y réagir en recourant à des mesures et à des processus préétablis, avec des règles de compétence claires. Cela peut être assuré par la mise en place d'un système SIEM (*Security Information and Event Management System*), qui détecte les anomalies dans le système et dans les schémas de traitement et garantit qu'elles sont traitées de manière appropriée sur le plan organisationnel et technique. Le SIEM a une structure spécifique à sa communauté ; il doit notamment tenir compte des risques spécifiques auxquels est exposée la communauté et de leur évolution et s'adapter en permanence à ses besoins. Ce système détecte et traite au minimum les cyberattaques ainsi que les hausses inhabituelles du nombre d'accès en écriture ou en lecture aux archives de documents, au registre des documents ou à l'index des patients qui font suspecter une utilisation abusive ou une attaque automatisée. Le système doit en outre repérer et traiter les mutations inhabituelles et critiques de droits d'accès dans la fonction de gestion des autorisations ou dans le système de gestion des identités et des accès (*Identity and Access Management,* IAM). L'annexe 2 ODEP-DFI comporte d'autres prescriptions à respecter, par exemple pour la détection et la gestion des failles de sécurité ou la protection contre les logiciels malveillants (annexe 2 ODEP-DFI, ch. 4.4 et 4.5).

En ce qui concerne la gestion des incidents de sécurité détectés, l'annexe 2 ODEP-DFI contient au ch. 4.3.3 des prescriptions relatives aux procédures de déclaration et de traitement des événements pertinents pour la protection et la sécurité des données. Il faut, par exemple, que des interlocuteurs soient désignés pour recevoir les déclarations au sein des communautés et dans les organisations d'exploitation et que des procédures d'urgence soient établies pour que, lorsque les conditions définies sont réunies, les systèmes concernés puissent être isolés des autres systèmes (stratégie d'endiguement ou *containment*). Il est en effet indispensable de pouvoir limiter l'étendue potentielle des dommages ou de ne pas mettre en danger d'autres parties du système qui seraient vulnérables. Afin de respecter l'obligation que leur impose l'*al. 3*, les communautés doivent en outre disposer de procédures d'escalade (déclaration) pour notifier à l'OFSP et à leur organisme de certification les événements particulièrement critiques pour la protection ou la sécurité des données et il leur incombe d'exiger et de contrôler le respect de ces procédures (annexe 2 ODEP-DFI, ch. 4.3.3, let. a, et

commentaire relatif à l'al. 3).

En ce qui concerne les failles de sécurité, l'annexe 2 ODEP-DFI souligne au ch. 4.4 la responsablité des communautés de pratiquer une gestion (préventive) des incidents de sécurité. Cela implique en particulier de traiter rapidement toute information sur des failles de sécurité connues ou nouvellement décelées dans les outils informatiques utilisés (par ex. des défauts de composants logiciels critiques), afin de pouvoir prendre – après évaluation – des mesures correctives appropriées telles qu'un « patch » sur le système défectueux (annexe 2 ODEP-DFI, ch. 4.13.2, let. d).

En application de la *let. b*, il faut prévoir notamment d'inventorier tous les éléments sensibles – éléments d'infrastructure informatique et recueils de données – que la communauté utilise pour le dossier électronique du patient (annexe 2 ODEP-DFI, ch. 4.6). Le registre visé à l'annexe 2 ODEP-DFI, let. j, doit inclure tous les systèmes primaires raccordés, afin de fournir une vue d'ensemble de tous les systèmes primaires qui échangent des données avec les dossiers électroniques des patients. Cet inventaire constitue une partie de l'« inventaire des équipements essentiels à l'évaluation et au traitement des risques » qu'il est prévu de créer dans le cadre du système de gestion de la protection et de la sécurité des données. Les éléments à inventorier sont encore précisés à l'annexe 2 ODEP-DFI, ch. 4.2.3, let. c, et comprennent, en plus des objets protégés en priorité (« objets de protection primaires ») que sont les données sensibles du dossier électronique du patient, les processus utilisés dans leur traitement, vu qu'ils jouent eux aussi un rôle direct dans la protection des données (ch. 4.2.3, let. c, al. i). S'y ajoutent les objets dits « de protection secondaires », à gérer également dans le cadre de la protection et de la sécurité des données. Il s'agit surtout des systèmes, infrastructures et applications, mais aussi des installations, structures organisationnelles (structures d'entreprise, responsabilités, etc.), personnes et processus dont le rôle est de protéger les objets de protection primaires (ch. 4.2.3, let. c, al. ii). Il est par exemple important de savoir quels sont les systèmes qui gèrent des données sensibles, qui les surveille et comment, et ce que deviennent les informations ou quels sont les processus réactionnels et les responsabilités engagés lorsqu'un traitement illicite des données a été décelé.

Comme les organisations et leurs équipements (outils informatiques, recueils de données, processus, structures organisationnelles, etc.) et donc aussi l'état des risques, sont soumis à des changements constants, toutes les modifications des équipements susmentionnés qui affectent la sécurité doivent être évaluées et documentées afin que le système de gestion de la protection et de la sécurité des données puisse travailler avec des données actuelles et exactes (annexe 2 ODEP-DFI, ch. 4.2.4). Tout comme l'« inventaire des équipements essentiels à l'évaluation et au traitement des risques », le catalogue des risques et le plan de traitement des risques doivent être tenus à jour (annexe 2 ODEP-DFI, ch. 4.2.5). La gestion des risques liés à la protection et à la sécurité des données représentant un enjeu stratégique pour toute organisation, le plan de traitement des risques doit être régulièrement revu et approuvé par la direction. Les consignes visant à assurer la protection et la sécurité des données doivent en outre être diffusées dans toute l'organisation.

En application de la *let. c*, les communautés doivent imposer des règles de protection et de sécurité des données aux institutions de santé qui leur sont affiliées et donc, indirectement, aux professionnels de la santé qui y travaillent et aux éventuels autres collaborateurs, par exemple au personnel du service informatique hospitalier ou à des tiers (annexe 2 ODEP-DFI, ch. 4.7 à 4.10). Les communautés doivent, par exemple, astreindre les institutions de santé qui leur sont affiliées à informer les professionnels de la santé ayant accès au dossier électronique du patient sur leurs tâches, droits et obligations liés au traitement des données correspondantes ainsi que sur les risques et les mesures destinées à garantir la protection et la sécurité des données (annexe 2 ODEP-DFI, ch. 4.7.1, let. b ; cf. aussi ch. 1.2.2, let. b, et 1.3.3, let. a).Les institutions de santé doivent être tenues par les communautés de garantir une configuration sûre des terminaux utilisés par les professionnels de la santé pour accéder au dossier électronique du patient (par ex. en utilisant des logiciels contre les programmes malveillants et des systèmes de protection des réseaux) (annexe 2 ODEP-DFI, ch. 4.7.1 et 4.7.2). Les institutions de santé doivent à leur tour imposer ces exigences aux

professionnels de la santé qui travaillent pour elles. L'annexe 2 ODEP-DFI, ch. 4.7.3, oblige les communautés à prendre les mesures organisationnelles et, s'il le faut, les mesures techniques nécessaires pour empêcher le traitement de données du dossier électronique du patient par des terminaux dont les configurations ne sont plus considérées comme sûres. Il s'agit par exemple de faire en sorte que les terminaux équipés de systèmes d'exploitation peu sûrs, et donc obsolètes parce que le fabricant a cessé d'en assurer le suivi, ne puissent plus accéder aux données du dossier électronique du patient.

Une communauté ne peut pas assurer la protection et la sécurité des données sans le concours des institutions de santé qui lui sont affiliées et d'éventuels fournisseurs de biens et services. C'est pourquoi il est impératif que les exigences en matière de protection et de sécurité des données spécifiées à la *let. c* soient respectées non seulement par les professionnels de la santé et le personnel de la communauté (par ex. le service d'assistance pour professionnels de la santé), mais aussi par les tiers auxquels elle pourrait faire appel (par ex. des sous-traitants ou des fournisseurs). L'annexe 2 ODEP-DFI fixe notamment des exigences au personnel technique et administratif de ces tierces parties pour la gestion des personnes ainsi que de leurs accès et droits d'utilisateur (annexe 2 ODEP-DFI, ch. 4.9). Des dispositions particulières s'appliquent aux utilisateurs « privilégiés », c.-à-d. bénéficiant d'autorisations système étendues (« administrateurs système ») pour les accès aux ensembles de données et systèmes particulièrement sensibles (annexe 2 ODEP-DFI, ch. 4.9.1). Ces « personnes-clés » présentent un risque potentiellement élevé pour la sécurité dans la mesure où elles peuvent contourner les mesures de sécurité en place. Elles doivent donc être connues du responsable de la protection et de la sécurité des données et gérées par celui-ci. Des exigences particulières s'imposent dans leur sélection et elles doivent répondre à des critères de sécurité clairement définis par les communautés.

Les communautés doivent également suivre des règles dans la gestion de leurs fournisseurs afin qu'un niveau élevé de sécurité puisse être maintenu en permanence pour tous les acteurs impliqués (communautés, institutions, fournisseurs et sous-traitants), quelle que soit la structure d'organisation adoptée (annexe 2 ODEP-DFI, ch. 4.9 et 4.10). Par exemple, les communautés ont l'obligation d'imposer le respect des exigences de protection et de sécurité des données tout au long de la chaîne d'approvisionnement, au cas où les fournisseurs mandateraient des sous-traitants (annexe 2 ODEP-DFI, ch. 4.9.4, let. a et e).

Responsable de la protection et de la sécurité des données

Selon l'*al. 2*, chaque communauté doit désigner un responsable de la protection et de la sécurité des données qui jouit d'une indépendance technique et organisationnelle. Cette personne doit posséder les compétences requises et disposer des ressources nécessaires pour accomplir ses tâches. Il lui incombe de concevoir, de mettre en œuvre et de contrôler les mesures visant à assurer la protection et la sécurité des données ainsi que d'appliquer des actions correctives dans le cadre de l'amélioration continue de la protection et de la sécurité des données de l'organisation (annexe 2 ODEP-DFI, ch. 4.11). Les communautés peuvent déléguer l'exercice opérationnel de cette fonction à des tiers, mais elles restent responsables de la conformité aux exigences.

Signalement d'incidents de sécurité

L'obligation instaurée par l'*al.* 3 de déclarer les incidents jugés importants pour la sécurité de l'information à l'OFSP a pour but de fournir des informations sur les points faibles découverts ou exploités dans l'organisation ou l'infrastructure informatique des différentes communautés. Ces informations seront analysées et évaluées en vue de prendre éventuellement des mesures visant à prévenir de nouveaux incidents. Il s'agit avant tout d'étendre les connaissances et l'expérience pour les communautés elles-mêmes, mais aussi pour l'OFSP en sa qualité d'autorité régulatrice dans le domaine de la protection et de la sécurité des données. De plus, l'évaluation régulière des incidents de sécurité peut faire apparaître d'éventuelles tendances au niveau des menaces rencontrées, permettant ainsi aux communautés d'adopter en temps utile des contre-mesures appropriées. En cas de grave mise en danger de la protection ou de la sécurité des données du dossier électronique du

patient, l'OFSP peut ordonner d'autres mesures en application de la cause de sauvegarde prévue à l'art. 37. Les communautés et leurs organisations sous-traitantes peuvent en outre, si elles le souhaitent, bénéficier des services de conseil et d'information de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération (MELANI). MELANI peut fournir à ses clients des informations précieuses sur les dangers actuels et les mesures appropriées pour y faire face, mais aussi faciliter les échanges d'informations entre les exploitants d'infrastructures critiques ou exposées à ces dangers.

Autres exigences applicables

En application de l'*al. 4*, le DFI définit à l'annexe 2 ODEP-DFI, ch. 4.12 à 4.18, des exigences supplémentaires en matière de protection et de sécurité des données qui portent, entre autres, sur les domaines suivants :

- cryptage de la communication et de l'enregistrement des données et gestion des clés cryptographiques (annexe 2 ODEP-DFI, ch. 4.12) ;
- sécurité d'exploitation, restauration des systèmes et historisation de l'exploitation des systèmes (annexe 2 ODEP-DFI, ch. 4.13). Les historiques technico-administratifs générés lors de l'exploitation des systèmes servent avant tout à vérifier le respect des prescriptions en matière de protection et de sécurité des données. C'est pourquoi elles ne doivent être accessibles qu'aux personnes ou organes chargés de surveiller l'application de ces dispositions (annexe 2 ODEP-DFI, ch. 4.13.3, let. g) et doivent être protégées de toute modification illicite ou inaperçue (annexe 2 ODEP-DFI, ch. 4.13.3, let. h) ;
- achat, développement sûr et maintenance des systèmes (annexe 2 ODEP-DFI, ch. 4.14) ;
- gestion des réseaux et des services réseau ainsi que des sessions réseau (annexe 2 ODEP-DFI, ch. 4.15 et 4.16) ;
- supports de stockage intermédiaires (annexe 2 ODEP-DFI, ch. 4.17) ;
- Accessibilité (annexe 2 ODEP-DFI, ch. 4.18).

Afin de garantir une sécurité maximale au dossier électronique du patient, y compris sur le plan du droit, l'*al. 5* stipule que les données ne peuvent être stockées que sur des supports de données situés en Suisse et régis exclusivement par le droit suisse. Pour cette même raison, elles ne peuvent être exploitées que par des personnes morales régies par le droit suisse (annexe 2 ODEP-DFI, ch. 4.19). Cette disposition exclut que les données du dossier électronique du patient soient soumises à des législations autres que le droit suisse, ce qui élimine d'emblée la possibilité de conflits avec des dispositions légales étrangères.

Art. 13 Service d'assistance pour les professionnels de la santé

Les communautés doivent s'assurer que tous les professionnels de la santé puissent contacter une assistance technique et fonctionnelle pour obtenir de l'aide dans l'utilisation du dossier électronique du patient (service d'assistance ou *service desk*). Des exigences et des règles spécifiques s'appliquent aux collaborateurs du service d'assistance (annexe 2 ODEP-DFI, ch. 5.1.2) : ils doivent être informés de leurs tâches, de leurs droits et obligations ainsi que des risques et des mesures en matière de protection des données et de sécurité de l'information ; de plus, ils doivent être assujettis à une obligation analogue au secret médical. L'accès à distance aux terminaux des professionnels de la santé est possible exclusivement si l'utilisateur en est informé et y consent ; il doit être documenté.

Section 2 : Communautés de référence

Les commentaires suivants s'appliquent exclusivement aux dispositions de la section 2 de l'ODEP valables pour les communautés de référence (art. 14 à 21).

Art. 14 Exigences supplémentaires à l'égard des communautés de référence

Les communautés de référence, c'est-à-dire les communautés auprès desquelles les patients peuvent

ouvrir un dossier électronique du patient et en gérer les droits d'accès, doivent se conformer aux exigences énoncées aux art. 14 à 21 en plus des exigences formulées dans la section 1 (art. 9 à 13) pour les communautés en général.

Art. 15 Information du patient

Le consentement doit être précédé d'une information adaptée et objective du patient. La responsabilité en incombe à sa communauté de référence. Le patient doit être informé du but ainsi que du déroulement de la constitution et du fonctionnement du dossier électronique du patient de manière détaillée et en des termes qu'il comprend. Il doit pouvoir évaluer les conséquences liées à l'octroi du consentement, aux différents paramètres de la gestion des autorisations et à la révocation. En l'absence d'information ou si l'information est insuffisante, la portée et la validité du consentement sont réduites en conséquence.

L'information doit couvrir au moins les points mentionnés à l'*al. 1* (annexe 2 ODEP-DFI, ch. 6.1).

Aux termes de la *let. a*, le patient doit être informé des buts du dossier électronique du patient (annexe 2 ODEP-DFI, ch. 6.1.1), et notamment de ceux mentionnés à l'art. 1 LDEP (qualité du traitement, sécurité du patient, efficacité et compétence sanitaire). Pour apprécier objectivement les opportunités et les risques du dossier électronique du patient, il peut être intéressant d'être informé des buts pour lesquels le dossier électronique du patient n'est pas prévu en raison de limitations techniques ou juridiques (pas d'accès pour les assureurs, les employeurs et les autorités sanitaires).

Conformément à la *let. b*, les traitements de données en lien avec le dossier électronique du patient doivent être expliqués dans leurs grandes lignes (annexe 2 ODEP-DFI, ch. 6.1.2 à 6.1.5). Il s'agit en particulier des possibilités de traitement de données à la disposition, d'une part, des patients et de leurs représentants et, d'autre part, des professionnels de la santé autorisés et de leurs auxiliaires. Le droit d'accéder au dossier électronique du patient en cas d'urgence médicale et les conséquences d'une éventuelle exclusion de ce droit font partie des informations à fournir au patient.

Selon la *let. c*, l'information doit mentionner que la constitution du dossier électronique du patient est facultative, tout comme son utilisation. Aux termes de l'art. 3, al. 2, LDEP, on peut présumer que le patient qui a consenti à la constitution d'un dossier électronique du patient souhaite par principe que ses données médicales y soient enregistrées. Cela signifie qu'il doit expressément signaler au professionnel de la santé concerné les informations et traitements qui ne doivent pas figurer dans son dossier électronique du patient (annexe 2 ODEP-DFI, ch. 6.1.2, let a). Le patient doit également être informé qu'il peut révoquer son consentement en tout temps, sans avoir à respecter de conditions de forme ni à motiver sa décision (art. 3, al. 3 LDEP ; annexe 2 ODEP-DFI, ch. 6.1.3). Il doit être rendu attentif aux conséquences de cette révocation ; par exemple au fait que les données médicales contenues dans le dossier électronique qu'il a révoqué ne figureront pas dans son nouveau dossier électronique s'il venait à en rouvrir un (annexe 2 ODEP-DFI, ch. 6.1.3, let g), car un nouveau consentement est suivi de l'assignation d'un nouveau numéro d'identification du patient (cf. commentaire relatif à l'art. 8). Un dossier électronique du patient créé après révocation d'un premier dossier est donc un nouveau dossier vide auquel il s'agit de redonner un contenu.

La *let. d* précise que l'information doit permettre au patient de savoir, entre autres, comment et à qui des droits d'accès à certaines données médicales peuvent être accordés (cf. commentaires relatifs aux art. 1 à 4). Il s'agit en particulier de l'information sur les niveaux de confidentialité (annexe 2 ODEP-DFI, ch. 6.1.4) sur les droits d'accès (annexe 2 ODEP-DFI, ch. 6.1.5), sur les possibilités et options d'adapter, de suspendre et de limiter temporellement les droits d'accès en application de l'art. 4 ainsi que sur la possibilité d'interdire complètement à certains professionnels de la santé l'accès au dossier électronique du patient (liste d'exclusion ; art. 4, let. b).

En vertu de l'*al. 2,* le patient doit également être informé des dispositions de sécurité recommandées (annexe 2 ODEP-DFI, ch. 6.1.6). Ces recommandations concernent, par exemple, la manière d'utiliser

en toute sécurité le moyen d'identification et les informations d'authentification secrètes (par ex. les mots de passe), les risques auxquels sont exposés les patients et les comportements à adopter pour se protéger contre ces risques, y compris les tentatives d'escroquerie (par ex. ingénierie sociale, *phishing*, etc.), l'utilisation de terminaux et de navigateurs web fiables ou encore l'utilisation de programmes contre les logiciels malveillants et les menaces réseau.

Art. 16 Consentement

La loi dispose que le consentement doit être donné par écrit. L'*art. 16* précise que le consentement doit porter la signature du patient. La forme requise par la loi doit également être respectée lorsque le consentement est donné par voie électronique. Le code des obligations précise les conditions auxquelles une signature électronique est assimilée à une signature manuscrite : la signature utilisée doit être conforme aux exigences stipulées à l'art. 14, al. 2bis, CO[8] (signature électronique qualifiée au sens de la loi sur la signature électronique, SCSE[9]). Si cette condition est remplie, la forme écrite est réputée respectée. L'historisation des données permet de vérifier la validité de la signature électronique.

Art. 17 Gestion

Gestion des patients

En vertu de l'*al. 1*, les communautés de référence doivent définir, documenter, mettre en œuvre et respecter des processus adéquats pour l'ouverture, la gestion et la suppression du dossier électronique du patient ainsi que pour l'identification et l'authentification des patients (annexe 2 ODEP-DFI, ch. 8.1).

Aux termes de la *let. a*, les communautés de référence doivent régler les processus d'ouverture, de gestion et de suppression des dossiers électroniques et donc les modalités d'entrée et de sortie des patients de la communauté de référence. Le processus d'entrée est visé par les *let. b à d*, l'information des patients par l'*art. 15* et l'obtention du consentement par l'*art. 16*. Les dispositions de l'*art. 21* sont déterminantes pour le processus de suppression d'un dossier électronique de patient, tandis que les conditions d'un processus de changement de communauté de référence sont précisées à l'annexe 2 ODEP-DFI, ch. 8.5.

Si un patient demande à constituer ou à révoquer un dossier électronique du patient ou à changer de communauté de référence, il faut d'abord s'assurer qu'il s'agit de la bonne personne (annexe 2 ODEP-DFI, ch. 8.2). À cet effet, la communauté de référence doit identifier le patient avec certitude (*let. b*). L'annexe 2 ODEP-DFI, ch. 8.2.1, let. a, précise que, si l'identification ne peut se faire à l'aide d'un moyen d'identification émis par un éditeur certifié selon l'art. 31, elle doit être conforme aux exigences définies à l'art. 24, ce qui suppose une vérification d'identité au moyen de l'un des documents prévus par la loi sur les documents d'identité ou la loi sur les étrangers ou sur la base d'une demande munie d'une signature électronique qualifiée. Il est indispensable d'identifier le patient de manière certaine et aussi univoque que possible pour pouvoir lui attribuer un numéro d'identification correct en application de la *let. d*.

La *let. c* stipule que les communautés de référence doivent s'assurer que les patients et leurs représentants – comme les professionnels de la santé (art. 9, let. e) – accèdent au dossier électronique du patient uniquement en utilisant un moyen d'identification valable émis par un éditeur certifié selon l'*art. 31* (annexe 2 ODEP-DFI, ch. 8.3). Cela signifie que les voies d'accès et les terminaux utilisés par les patients pour accéder à leur dossier électronique doivent supporter une procédure d'authentification forte, adaptée aux progrès techniques et comportant au moins deux facteurs d'authentification.

[8] RS 202
[9] RS 943.03

Selon la *let. d*, les communautés de référence doivent se conformer aux dispositions des art. 6 et 7 pour demander à la CdC un numéro d'identification pour le patient qui souhaite ouvrir un dossier électronique (annexe 2 ODEP-DFI, ch. 8.2.1, let. d). En vertu de l'annexe 2 ODEP-DFI, ch. 8.2.1, let. b, une communauté de référence doit veiller à ce que l'on vérifie, avant l'ouverture d'un dossier électronique du patient, si le patient en question n'en possède pas déjà un et n'a donc pas de numéro d'identification du patient actif enregistré à la CdC. Cela garantit qu'un patient ne peut avoir qu'un seul dossier électronique du patient à la fois et que ses données médicales sont systématiquement enregistrées dans ce dossier uniquement.

L'annexe 2 ODEP-DFI contient en outre des prescriptions concernant la reprise des données démographiques de la CdC et des numéros d'identification des patients dans l'index des patients (annexe 2 ODEP-DFI, ch. 8.2.1, let. e) ainsi que l'attribution correcte selon l'art. 25, al. 1, ODEP de l'identificateur univoque du bon dossier électronique du patient (annexe 2 ODEP-DFI, ch. 8.2.2).

La *let. e* garantit que les patients ont la possibilité de changer de communauté de référence. À cet effet, l'annexe 2 ODEP-DFI, ch. 8.5.2, impose aux communautés de référence de garantir que la configuration individuelle du contrôle des autorisations (*policy configuration*) puisse être transférée à une nouvelle communauté de référence. Par ailleurs, les communautés de référence doivent aussi être en mesure de reprendre les configurations individuelles d'autres communautés de référence. Indépendamment de la manière dont elles mettent en œuvre et représentent la fonction de gestion des autorisations en interne sur le plan technique, les communautés de référence doivent pouvoir exporter leur configuration de gestion des autorisations dans un format interopérable (basé sur XACML) et importer une telle configuration en provenance d'une autre communauté de référence. Le format d'échange des configurations est le format d'échange technique du profil d'intégration national CH:PPQ du DFI défini à l'annexe 5 ODEP-DFI, ch. 2. Comme la configuration de gestion des autorisations ne peut être gérée que dans la communauté de référence à laquelle on appartient, les professionnels de la santé ne peuvent accorder des droits d'accès par délégation en application de l'art. 4, let. g, que s'ils sont enregistrés dans la communauté de référence du patient qui leur a délégué cette compétence. Le patient qui change de communauté de référence doit donc, s'il le souhaite, habiliter les professionnels de la santé de la nouvelle communauté de référence à accorder des droits d'accès en son nom. Il en va de même des représentants, qui doivent être à nouveau enregistrés.

Mise en œuvre de la gestion des autorisations

Aux termes de l'*al. 2*, les communautés de référence doivent remplir les critères techniques et organisationnels requis pour garantir l'application des dispositions selon l'art. 2, al. 1 à 4 et 3 (cf. commentaires y relatifs ainsi que l'annexe 2 ODEP-DFI, ch. 8.6).

L'application de l'art. 4, let. f, (désignation d'un représentant) comprend, outre un volet technique, un volet organisationnel imposant des tâches précisées à l'annexe 2 ODEP-DFI, ch. 8.4. Les représentants n'ont pas besoin de posséder un numéro d'identification ni un dossier électronique du patient propres, mais ils sont tenus d'avoir leur propre moyen d'identification, émis par un éditeur certifié selon l'art. 31, pour accéder au dossier électronique du patient de la personne qu'ils représentent. Les personnes qui représentent des patients doivent elles aussi être informées des fonctionnalités de base du dossier électronique du patient ainsi que des possibilités, des droits et des obligations associés à l'utilisation du dossier électronique du patient (annexe 2 ODEP-DFI, ch. 8.4.2, let. b). Pour protéger les droits de la personnalité du patient représenté, il faut s'assurer que son représentant est correctement identifié et qu'il est bien en droit de représenter le patient en vertu des dispositions du droit civil. Comme le patient, son représentant doit être identifié de manière certaine et les dispositions qui s'appliquent à ce sujet sont analogues. Si l'identification du représentant du patient ne peut se faire à l'aide d'un moyen d'identification émis par un éditeur certifié selon l'art. 31, elle doit également être conforme aux exigences définies à l'art. 24 (annexe 2 ODEP-DFI, ch. 8.4.2, let. a). Il faut en outre garantir que le représentant a accès au dossier électronique du patient uniquement pendant la durée de validité de sa représentation (annexe 2 ODEP-DFI, ch. 8.4.2, let. d). Parmi les

applications possibles de cette disposition, on peut penser à la représentation d'un enfant ou d'une personne âgée par l'un de ses proches ou par une autre personne de confiance si le patient ne possède pas les capacités techniques ou intellectuelles voulues pour gérer son dossier électronique du patient de manière autonome.

Art. 18 Portail d'accès destiné aux patients

Le portail d'accès destiné aux patients doit satisfaire aux exigences énoncées à l'annexe 2 ODEP-DFI, ch. 9.1 à 9.5. Il s'agit pour l'essentiel des mêmes exigences que celles qui s'appliquent au portail d'accès destiné aux professionnels de la santé visé à l'art. 11, plus particulièrement de celle de la let. a régissant la mise en œuvre des différentes possibilités d'attribution des niveaux de confidentialité et d'octroi des droits d'accès (en vertu de l'art. 1, al. 1 et art. 2, al. 1) ainsi que sur les options offertes au patient (art. 4, let. a à e, et g), auxquelles s'ajoute la représentation de la composition des groupes de professionnels de la santé (annexe 2 ODEP-DFI, ch. 9.1.1, let. c).

Il faut que la présentation des données du dossier électronique du patient sur l'interface utilisateurs du portail d'accès pour les patients soit également correcte et exhaustive et, par exemple, montre clairement si des données médicales ont été mises en ligne par un professionnel de la santé ou par le patient (annexe 2 ODEP-DFI, ch. 9.2).

La *let. b* porte sur les exigences de présentation des données historisées du patient après traitement dans toutes ses communautés et communautés de référence (ch. 9.3 de l'annexe 2 ODEP-DFI). En vertu de l'art. 10, al. 3, let. d, les patients doivent avoir la possibilité de consulter à tout moment, sur le portail d'accès qui leur est destiné, les données historisées suite au traitement de leur dossier électronique (annexe 2 ODEP-DFI, ch. 9.3 et 2.10). Comme les données historisées au sens de l'annexe 2 ODEP-DFI, ch. 2.10, peuvent avoir été générées dans plusieurs communautés, il faut les récupérer auprès des différentes communautés concernées et les mettre en ligne sous une forme consolidée et lisible sur le portail d'accès pour que le patient puisse les y consulter. La présentation des données historisées à des fins de consultation est conforme aux adaptations natonales des profils d'intégration visées à l'art. 5, let. b, ODEP-DFI.

La *let. c* dispose que le portail d'accès pour les patients doit leur offrir en particulier la possibilité d'exclure des données médicales vouées à la destruction (art. 10, al. 2, let. b), ou au contraire de supprimer certaines données médicales du dossier électronique du patient en application de l'art. 10, al. 2, let. c (annexe 2 ODEP-DFI, ch. 9.4.1). Pour ce qui est des données saisies par le patient, l'annexe 2 ODEP-DFI, ch. 9.4.3, précise que le portail d'accès doit faire une distinction claire entre les fonctions clés du dossier électronique du patient et les fonctionnalités qui ne sont pas réglementées par la LDEP et ses dispositions d'exécution. Il importe en particulier de s'assurer que des données du dossier électronique du patient ne puissent pas être transférées automatiquement et sans l'accord explicite du patient dans des secteurs fonctionnels ou des supports de données situés « en dehors » du dossier électronique du patient, ce qui exclurait ces données du champ de validité de la LDEP.

Les portails d'accès doivent être conçus de manière à faciliter l'accès des personnes handicapées ou limitées en raison de l'âge ou de la langue et répondre, en vertu de la let. d, aux mêmes exigences que les portails d'accès pour professionnels de la santé selon l'art. 11 (annexe 2 ODEP-DFI, ch. 3.2).

Art. 19 Données saisies par les patients

Le patient a la possibilité de saisir lui-même, via le portail d'accès, ses propres données médicales dans son dossier électronique du patient (art. 10, al. 2, let. b, ch. 3, LDEP), sans que ceux-ci soient soumis à un délai d'effacement (annexe 2 ODEP-DFI, ch. 10.1.2).

Pour des raisons de sécurité des données, entre autres, il n'est pas permis de conserver des données enregistrées par le patient lui-même sur les supports d'archivage d'institutions de santé affiliées. Pour cette raison, l'annexe 2 ODEP-DFI, ch. 10.1.1, impose aux communautés de référence de mettre à

disposition des supports d'archivage internes dédiés aux données enregistrées par les patients. L'espace de stockage fourni à cet effet doit être suffisant.

L'annexe 2 ODEP-DFI, ch. 10.2, prévoit en outre la possibilité pour le patient d'exporter du système les documents de son dossier électronique du patient, y compris les métadonnées utilisées pour leur description. Cela permet, par exemple, de sauvegarder les données exportées sur un support physique, c'est-à-dire hors ligne. Il faut que les données exportées puissent être remises à disposition dans le dossier électronique du patient sans travail excessif en cas de besoin. Cela correspond à la conception actuelle de l'archivage des documents qui ne sont pas directement utiles dans la situation de traitement en cours. Cette mesure contribue en outre à accroître la protection et la sécurité des données. Afin d'éviter tout doublon lors de la réimportation, il faut soit coupler la fonction d'exportation à une suppression des données exportées, soit appliquer une procédure appropriée permettant de reconnaître les duplicata après réimportation. Pour éviter que l'intégrité des données ne subisse des atteintes (par ex. lors d'une manipulation hors ligne), il faut prévoir une procédure appropriée (par ex. fonction de hachage cryptographique, comme SHA-3) permettant de vérifier l'intégrité des données exportées avant leur remise à disposition. Grâce à la procédure appliquée en cas d'exportation, on vérifiera alors si l'intégrité des données a été préservée avant de les remettre à disposition (annexe 2 ODEP-DFI, ch. 10.2.3).

Art. 20 Service d'assistance pour les patients

Les communautés de référence doivent s'assurer que tous les patients, à l'instar des professionnels de la santé (art. 13), puissent contacter une assistance technique et fonctionnelle pour obtenir de l'aide et du soutien dans l'utilisation de leur dossier électronique du patient (service d'assistance ou *service desk*). Le personnel des services d'assistance dédiés aux patients est soumis aux mêmes règles que celui des services d'assistance destinés aux professionnels de la santé ; ces services ont également les mêmes obligations d'historisation (annexe 2 ODEP-DFI, ch. 5). En cas de recours ou de conflit, les interlocuteurs actuels de la Confédération et des cantons dans ce domaine (préposés à la protection des données) sont les instances de recours ou de médiation.

Art. 21 Suppression du dossier électronique du patient

En vertu de l'*al. 1*, la communauté de référence supprime le dossier électronique du patient dans le cas où ce dernier révoque son consentement à la tenue de son dossier électronique. Pour cela, il est important de s'assurer que le patient qui révoque son consentement a été identifié avec certitude (annexe 2 ODEP-DFI, ch. 12.2.2, let. a). Afin d'assurer la traçabilité, la déclaration de révocation doit être conservée pendant dix ans.

La communauté de référence peut supprimer un dossier électronique au plus tôt deux ans après le décès du patient (*al. 2*). Cette règle vise au respect du principe de proportionnalité. Les dossiers électroniques de patients décédés ne doivent pas être conservés pour une durée indéterminée. Une communauté de référence qui apprend le décès d'un patient doit pouvoir supprimer son dossier électronique à l'échéance d'un délai de protection de deux ans. Cela ne l'oblige pas pour autant à enquêter activement sur son statut de vie ou sur la date de son décès, par exemple. De même, ni la CdC, ni les registres cantonaux des communes ne sont tenus de déclarer les décès aux communautés et aux communautés de référence. Les cantons sont cependant libres d'inscrire une telle obligation de déclaration dans leur droit cantonal, au besoin en utilisant le NAVS13 – sous réserve de la base légale nécessaire.

L'*al. 3* prévoit que lorsqu'une communauté de référence a supprimé un dossier électronique du patient, elle doit supprimer sans délai tous les droits d'accès au dossier et informer la CdC, ainsi que toutes les autres communautés et communautés de référence, de la suppression dudit dossier. Le choix des moyens de transmission et des canaux d'information est laissé à la discrétion de la communauté de référence, qui doit toutefois garantir que l'information parvient aux destinataires et ne contient pas d'informations médicales. Il faut alors que la totalité des données détenues par la

communauté de référence et par l'ensemble des autres communautés soient effacées, comme l'exige l'art. 10, al. 1, let. e (annexe 2 ODEP-DFI, ch. 12.4, let. c, et ch. 2.6, let. b).

Section 3 : Évaluation et recherche

Art. 22

L'évaluation a pour objet et but de surveiller l'adéquation, l'efficacité et l'économicité des mesures adoptées en vertu de la LDEP (art. 18 LDEP). Elle repose, entre autres, sur un système de monitoring qui fournit les données nécessaires à l'évaluation. Afin de garantir la disponibilité des données, l'*al. 1* prévoit que les communautés et les communautés de référence doivent mettre à la disposition de l'OFSP des données utilisant des pseudonymes aux fins d'évaluation. De plus, en vertu de l'*al. 2*, le DFI fixe les données à fournir ainsi que les échéances.

D'autres sources importantes de données pour l'évaluation sont, par exemple, les données des services de recherche visés à l'art. 39, plus particulièrement ceux du service de recherche des institutions de santé et des professionnels de la santé (*al. 3*), ainsi que les documents fournis par les organismes à certifier ou les bureaux de certification dans le cadre d'une certification LDEP (*al. 4*).

Chapitre 4 : Moyens d'identification

Pour accéder à leur dossier électronique du patient, les patients et les professionnels de la santé ont besoin d'un moyen d'identification, conformément à l'art. 7 LDEP, délivré par un éditeur certifié selon l'art. 31.

La certification des éditeurs de moyens d'identification et les exigences techniques minimales prévues quant au niveau de sécurité garantissent la fiabilité du moyen d'identification ; elles donnent la certitude que la personne qui se réclame d'une certaine identité est bien celle à laquelle cette identité a été attribuée.

L'édition et la gestion des moyens d'identification tout au long du cycle de vie se basent sur le déroulement décrit dans la norme ISO/IEC 29115:2013, et dont les phases successives sont l'enregistrement et la gestion des moyens d'identification et leur utilisation dans les activités opérationnelles. Une bonne gestion du cycle de vie du moyen d'identification est importante pour la fiabilité de l'authentification. Ce cycle de vie comprend des procédures partielles telles que la création du support d'une identité électronique, sa personnalisation, son initialisation, son rattachement au titulaire ainsi que l'édition, l'activation, la révocation et le renouvellement de cette identité électronique.

Ces étapes peuvent se dérouler dans des ordres différents tant qu'il est avéré que la sécurité est assurée. Par exemple, l'étape de saisie des données d'identité suivie du rattachement à l'identité électronique peut avoir lieu après l'édition du moyen d'identification. On pourrait imaginer le déroulement suivant : un patient ou un professionnel de la santé obtient d'un éditeur certifié un moyen d'identification doté d'un identifiant électronique univoque et d'un mécanisme d'authentification d'accès fiable. Dans un deuxième temps, la personne active le moyen d'identification en fournissant la preuve qu'elle dispose des facteurs d'authentification nécessaires (par ex. mot de passe secret). Pour terminer, d'autres caractéristiques d'identification personnelles sont associées en toute sécurité au moyen d'identification. Cette démarche peut s'effectuer via un entretien personnel ou une identification par vidéo. Il n'y a donc pas besoin d'établir à nouveau les supports d'identité électronique déjà délivrés – tels que la carte d'assuré selon l'art. 42a de la loi fédérale du 18 mars 1994[10] sur l'assurance-maladie – pour satisfaire aux prescriptions énoncées aux art. 23 – 27.

[10] RS 832.10

Art. 23 Exigences applicables

Les exigences applicables à l'enregistrement et à la gestion des moyens d'identification ainsi que les critères de protection pour l'authentification sont définis dans la norme ISO/IEC 29115:2013 pour les différents niveaux de confiance. Plus le niveau de confiance est élevé, plus on peut se fier à l'identité déclarée par la personne qui s'authentifie auprès d'un participant au système à l'aide du moyen d'identification qui lui a été délivré.

Selon la *let. a*, le niveau de confiance 3 (« confiance élevée ») s'applique à la fois aux moyens d'identification des patients et des professionnels de la santé. Lorsqu'un moyen d'identification électronique répond aux exigences d'un niveau de confiance de degré supérieur, on suppose que celles d'un niveau inférieur sont également remplies.

Le niveau de confiance 3 ne requiert pas que la personne se présente en personne pour l'enregistrement du moyen d'identification. Cependant, il y a lieu de s'assurer que la pièce d'identité produite est valable et qu'elle concerne bien la personne en question ou le demandeur. Des dispositions doivent donc être prises pour réduire les risques que l'identité d'un demandeur diffère de l'identité revendiquée, dans le cas, par ex., de pièces d'identité perdues, volées, suspendues, révoquées ou échues (art. 24, al. 1).

Selon la *let. b*, sur le plan technique et organisationnel, le moyen d'identification doit être conçu de manière à garantir que son titulaire soit le seul à pouvoir l'utiliser. Par exemple, il ne doit pas être possible de transférer les données cryptées protégées qui y figurent sur un autre système ou support, par ex. en captant des mots de passe transmis en clair.

La procédure prévue à la *let. c* doit combiner au moins deux techniques d'authentification et correspondre aux progrès techniques. Des procédures combinant les facteurs « savoir » (par ex. mot de passe secret) et « possession » (par ex. possession d'une carte à puce ou d'une carte SIM dédiée comme support du matériel codé) sont courantes.

En vertu de la *let. d*, la durée de validité du moyen d'identification ne doit pas dépasser cinq ans.

Art. 24 Vérification d'identité

L'éditeur vérifie l'identité de la personne qui sollicite un moyen d'identification sur la base d'une pièce d'identité valable selon la loi fédérale sur les documents d'identité (RS 143.1) ou la loi fédérale sur les étrangers (RS 142.20). Pour les demandes par correspondance, le demandeur adresse à l'éditeur la copie certifiée authentique d'une pièce d'identité (par ex. « identification jaune » de La Poste ou procédure d'identification par vidéo). Une confirmation de l'identité ou des caractéristiques d'identité au moyen d'une signature électronique qualifiée selon la loi sur la signature électronique (RS 943.03) a la même valeur.

Dans l'optique de disposer d'un vaste réseau de services d'enregistrement en Suisse, l'éditeur du moyen d'identification peut déléguer à des tiers la vérification de l'identité d'un demandeur (al. 2). Les exigences auxquelles doit satisfaire le service d'enregistrement (*registration authority*) sont définies à l'annexe 8 ODEP-DFI, ch. 4.2 (« Objectifs de sécurité portant sur l'environnement »).

Art. 25 Données

Selon l'*al. 1*, L'éditeur du moyen d'identification attribue au demandeur un identificateur univoque (eID). Cet identificateur est nécessaire pour établir un lien entre l'identité de la personne membre de la communauté ou de la communauté de référence et celle de l'éditeur.

L'éditeur conserve la tâche d'enregistrer les données d'identification des patients (*al. 2*) et des professionnels de la santé (*al. 3*) à des fins de preuve et de vérification d'identité. L'identificateur visé

à l'*al. 1* et les données d'identification énoncées à l'*al. 2, let. a à d, et à l'al. 3* peuvent être communiquées aux portails d'accès internes des communautés et des communautés de référence dans la réponse d'authentification aux fins de vérification et d'attribution de l'identité.

Le moyen d'identification peut également servir à confirmer la qualification professionnelle des professionnels de la santé (art. 9, al. 2, let. b et d). À cet effet, l'éditeur saisit et confirme le GLN du professionnel de la santé (art. 25, al. 3, let. a). Selon l'*al. 3, let. b*, la preuve que le demandeur est réellement un professionnel de la santé au sens de l'art. 2, let. b, LDEP doit être établie au préalable. L'éditeur procède à cet effet à une comparaison méticuleuse des données personnelles avec celles d'un registre fédéral ou cantonal (registre des professions médicales, registre national des professions de la santé, etc.), ce qui permet de s'assurer que le titulaire du moyen d'identification possède la formation appropriée, reconnue au niveau fédéral ou cantonal et dispose – s'il s'agit d'un professionnel indépendant – d'une autorisation cantonale de pratiquer.

L'éditeur du moyen d'identification peut déléguer à des tiers (*Registration Authority* – centre d'enregistrement) le soin de confirmer les données d'identification du « professionnel de la santé ». La vérification de l'identité par l'éditeur ou par le centre d'enregistrement est réglée à l'annexe 8 ODEP-DFI, ch. 4.2.

L'*al. 5* oblige les éditeurs à informer les demandeurs des dispositions de sécurité à respecter lors de l'utilisation du moyen d'identification. Ces précisions comprennent la manière de gérer en toute sécurité les mots de passe, l'information concernant le traitement et la communication de données d'identification à des tiers.

Art. 26 Renouvellement

À l'échéance de la durée de validité du moyen d'identification (cinq ans au maximum, art. 23, let. d), celui-ci doit être renouvelé. L'*al. 2* énonce, en dérogation à la norme ISO/IEC 29115:2013, qu'une vérification de l'identité selon le niveau de confiance 3 doit également être effectuée pour un renouvellement du moyen d'identification (art. 23).

Art. 27 Blocage

Le titulaire d'un moyen d'identification doit à tout moment pouvoir faire bloquer celui-ci temporairement ou définitivement pour l'accès au dossier électronique du patient. Comme rien ne s'oppose à ce que le moyen d'identification soit utilisé pour l'authentification en dehors du dossier, l'éditeur doit prévoir des procédés techniques pour empêcher une authentification valable au portail d'accès des patients et des professionnels de la santé. Parallèlement, l'éditeur doit prévoir des dispositions ayant pour effet d'empêcher un blocage non autorisé.

Chapitre 5 : Accréditation

Art. 28 Critères

L'organisme de certification d'une communauté, d'une communauté de référence, d'un portail d'accès ou d'un éditeur de moyens d'identification doit être reconnu apte à l'audit et à la certification de systèmes de management par le SAS. L'accréditation est régie par l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation (OAccD)[11]. L'art. 7, al. 1, de cette ordonnance dispose que l'organisme de certification doit remplir les exigences internationales en la matière. Pour les organismes de certification effectuant des examens dans le cadre du dossier électronique du patient, ces exigences découlent par exemple de la norme ISO/IEC 17021:2015, qui régit l'accréditation pour la certification de systèmes de management (cf. annexe 2 OAccD).

[11] RS **946.512**

Les communautés, les communautés de référence et les éditeurs de moyens d'identification doivent accomplir différentes tâches qui sont examinées dans le cadre de la certification. C'est la raison pour laquelle les organismes concernés doivent répondre à des exigences différentes et obtenir chacun leur propre accréditation (*al. 2*).

L'*al. 3* concrétise la notion de procédure de contrôle. Cette procédure comprend les critères d'évaluation et d'examen appliqués pour vérifier le respect des critères de certification (*let. a*) ainsi que des indications sur le déroulement de la procédure de certification (y compris la vérification et le renouvellement de la certification ; *let. b*).

L'*al. 4* stipule que le système de certification mis à disposition par l'OFSP pour s'assurer du respect des prescriptions relatives au transfert de données des communautés et des communautés de référence (interopérabilité) doit être utilisé. Ce système de certification permet de vérifier si, en pratique, une communauté ou une communauté de référence devant fait l'objet d'une certification est en mesure de communiquer avec d'autres communautés ou communautés de référence certifiées.

Selon l'*al. 5*, le DFI fixe les exigences applicables à la qualification du personnel chargé de réaliser les certifications (cf. annexe 6 ODEP-DFI). Relevons à ce propos qu'il n'existe pas de formation standard dans le domaine de l'informatique médicale et de la protection des données et que les experts en la matière sont relativement rares. Par conséquent, l'expérience pratique doit être prise en considération.

Art. 29 Procédure

L'implication de l'OFSP est censée garantir, d'une part, l'accès du Service d'accréditation aux connaissances spécialisées de l'administration fédérale et, d'autre part, la possibilité pour l'OFSP de discuter des modalités de l'accréditation avec le SAS.

Chapitre 6 : Certification

Section 1 : Critères

Art. 30 Communautés et communautés de référence

Un organisme de certification accrédité selon l'art. 28 vérifie si une communauté ou une communauté de référence remplit les critères de certification. Les communautés de référence doivent remplir les critères de certification applicables aux communautés (art. 9 à 13) mais également ceux énoncés aux art. 14 à 21 (*al. 1*).

L'*al. 2* délègue au DFI la compétence de régler en détail les critères de certification, ce qui permet de réglementer les différents points au niveau législatif approprié.

Selon l'*al. 3*, la compétence de modifier les critères de certification en fonction des progrès de la technique est transférée à l'OFSP par le DFI (cf. commentaire relatif à l'art. 10, al. 5).Cette disposition est importante en particulier en ce qui concerne les critères de certification dans le domaine de la tenue et du transfert des données (art. 10) ainsi que la protection et la sécurité des données (art. 12).

Art. 31 Éditeurs de moyens d'identification

L'*al. 1* énonce l'ensemble des exigences auxquelles doivent satisfaire les éditeurs de moyens d'identification.

La *let. a* se réfère aux art. 23 à 27, que doivent observer les éditeurs de moyens d'identification. Ces derniers doivent notamment garantir en particulier que les moyens d'identification du niveau de confidentialité 3 répondent à la norme ISO/IEC 29115:2013 (art. 23, que l'identité du demandeur est vérifiée (art. 24 et que les attributs d'identité du titulaire du moyen d'identification sont corrects (art. 25).

L'éditeur doit s'assurer au moyen de procédures adaptées que le personnel et les sous-mandataires possèdent tous une formation, des qualifications et une expérience suffisantes pour effectuer les tâches qui leur sont confiées (*let. b*).

La *let. c* énonce que les systèmes et produits informatiques exploités doivent être fiables. La notion de fiabilité met l'accent sur le soin apporté au développement des produits en question et la confiance qu'un utilisateur peut leur accorder en termes de sécurité.

L'éditeur doit garantir que des contrôles techniques sont effectués lors de l'établissement des moyens d'identification et que des mesures organisationnelles sont prises pour assurer la protection et la sécurité des données (*let. d*). Il est notamment fait référence ici à la surveillance permanente des installations nécessaires à l'établissement des moyens d'identification, à la protection contre des accès non autorisés de manière à assurer par exemple que seuls des collaborateurs autorisés ont accès à des domaines traitant de données personnelles, de données cryptées ou d'autres informations sensibles. L'éditeur de moyens d'identification est tenu d'utiliser des méthodes éprouvées garantissant la protection et la sécurité des données.

Les critères techniques et organisationnels de certification des moyens d'identification et de leurs éditeurs sont concrètement formulés sous la forme d'un « profil de protection » dans l'annexe 8 ODEP-DFI (al. 2).Le profil de protection sert à formuler des critères de sécurité à l'égard d'une classe de produits (dans les domaine des softwares et hardwares entre autres) et en particulier, selon la présente ordonnance, à l'égard de tous les moyens d'identification admis pour le dossier électronique du patient.

La cible d'évaluation (*Target of Evaluation* [TOE]) du profil de protection comprend le moyen d'identification proprement dit, le fournisseur d'identité (*Identity Provider*) pour l'identification et l'authentification ainsi que les interfaces techniques nécessaires et les canaux de communication pour l'authentification au portail d'accès des communautés et des communautés de référence. Durant le processus de certification, l'organisme de certification relève et examine les paramètres de conformité aux exigences de sécurité en appliquant à cette fin un niveau d'évaluation (*Evaluation Assurance Level*, [EAL]). L'examen porte sur les domaines « Development », « Life-Cycle Support », « Security Target Evaluation » et « Vulnerability Assessment ». Le niveau d'évaluation EAL 2 fixé l'annexe 8 ODEP-DFI, ch. 5.4, signifie que la TOE fait l'objet d'une vérification fonctionnelle et structurelle.

L'*al. 2* délègue au DFI la compétence de régler en détail les critères de certification, ce qui permet de réglementer les différents points au niveau législatif approprié.

Selon l'*al. 3*, la compétence de modifier les critères de certification en fonction des progrès de la technique est transférée à l'OFSP par le DFI (cf. commentaire relatif à l'art. 10, al. 5).On pense en particulier à l'adaptation d'exigences à caractère éminemment technique pour les critères de certification d'éditeurs de moyens d'identification.

Section 2 : Procédure de certification

Art. 32 Déroulement

Cet article régit le déroulement de la procédure de certification (qui se base sur la norme ISO/IEC 17021:2015) et définit les différentes étapes de la procédure par ordre chronologique.

La vérification visée à l'*al. 1* permet à l'organisme de certification d'évaluer, sur la base de la documentation qui lui a été remise, si la communauté, la communauté de référence ou l'éditeur de moyens d'identification est suffisamment préparé en vue de la procédure de contrôle. Cette précaution permet à la fois d'éviter des frais inutiles et d'augmenter les chances de réussite de l'audit de certification.

Dans le cadre de l'audit de certification visé à l'*al. 2*, l'organisme de certification vérifie également sur place si la communauté, la communauté de référence ou l'éditeur de moyens d'identification respecte les critères de certification.

Il délivre le certificat (*al. 3*) si, après avoir examiné la documentation et procédé à l'audit de certification, il parvient à la conclusion que la communauté, la communauté de référence ou l'éditeur de moyens d'identification remplit les critères fixés.

L'al. 4 dispose qu'un nouvel audit de certification (renouvellement de la certification) doit être réalisé avant l'expiration du certificat. Les exigences applicables à un renouvellement de la certification sont les mêmes que celles de l'audit de certification visé à l'al. 2. Cette procédure vise à assurer l'exploitation sans interruption d'une communauté, d'une communauté de référence ou d'un éditeur de moyens d'identification en empêchant l'expiration d'un certificat, ce qui aurait pour conséquence que l'organisation visée devrait être exclue de la participation au dossier électronique du patient.

Art. 33 Communication et publication des certificats délivrés

Afin d'assurer l'échange intercommunautaire de données, l'*al. 1* stipule que les communautés et communautés de référence certifiées doivent être enregistrées auprès du service de recherche des communautés et des communautés de référence certifiées visées à l'art. 40. Pour cette raison, toute certification acceptée doit être communiquée à l'OFSP, afin que celui-ci puisse effectuer la saisie correspondante (art. 40, al. 2). Les suspensions et les retraits de certification doivent également être communiqués sans délai pour que la communauté ou la communauté de référence concernée puisse être bloquée dans le service de recherche des communautés et des communautés de référence certifiées et, partant, être exclue de la participation au dossier électronique du patient.

En plus de saisir les données dans le service de recherche des communautés et des communautés de référence certifiées, l'OFSP publie un registre des certificats délivrés (al. 2). Ce registre permet aux patients d'avoir une vue d'ensemble des communautés et des communautés de référence qui proposent un dossier électronique du patient selon la LDEP et quels sont les éditeurs de moyens d'identification certifiés.

Art. 34 Procédure de vérification

Selon l'*al. 1*, l'organisme de certification vérifie chaque année si les critères de certification sont toujours pleinement remplis. S'il constate que cela n'est pas le cas, il en informe l'OFSP qui, en vertu de l'art. 37, al. 1, let. c, peut ordonner un renouvellement extraordinaire de la certification. Si l'inobservation des critères de certification concerne des domaines partiels isolés, l'examen peut se limiter à ces éléments. L'organisme de certification a en outre la possibilité de prendre des sanctions si les critères exigés à l'art. 38, al. 1, sont remplis.

L'organisme de certification doit informer l'OFSP de tout écart substantiel constaté afin que celui-ci puisse identifier rapidement les éventuels points faibles du droit d'exécution et, le cas échéant, prendre les mesures nécessaires.

Art. 35 Durée de validité

Le certificat est établi pour une durée de trois ans. L'art. 36 et l'art. 37, al. 1, let. c, demeurent réservés. La procédure de renouvellement de la certification doit être engagée avant l'échéance du certifi-

cat si la communauté ou la communauté de référence entend échanger des données sans interruption dans le cadre du dossier électronique du patient ou si l'éditeur de moyens d'identification souhaite continuer à exercer ses fonctions auprès des communautés et des communautés de référence. Le renouvellement de la certification s'aligne sur les dispositions prévues à l'art. 32.

Art. 36 Obligation de signaler les adaptations techniques ou organisationnelles substantielles

En vertu de l'*al. 1*, toute adaptation substantielle doit être signalée à l'organisme de certification. Sont notamment considérées comme des adaptations techniques ou organisationnelles substantielles les procédures nouvelles ou modifiées (en rapport avec la certification), les adaptations apportées à l'infrastructure informatique assurant l'échange intercommunautaire des données des communautés et des communautés de référence ou encore la modification de la procédure d'authentification pour les éditeurs de moyens d'identification.

Selon l'*al. 2*, l'organisme de certification décide s'il y a lieu d'examiner ces adaptations dans le cadre de la vérification prévue à l'*art. 34,* d'un renouvellement de la certification ou d'un renouvellement extraordinaire de la certification au sens de l'*art. 37, al. 1, let. c*. La vérification et le renouvellement de la certification s'effectuent au rythme habituel, le renouvellement extraordinaire doit intervenir le plus rapidement possible. Si la situation l'exige, une communauté ou une communauté de référence peut être exclue du dossier électronique du patient aussi longtemps que la procédure de renouvellement extraordinaire n'a pas abouti. L'exclusion peut être prononcée par l'organisme de certification sur la base de l'art. 38 (sanctions) ou par l'OFSP sur la base de l'art. 37 (clause de sauvegarde) lorsque l'organisme de certification lui signale des écarts substantiels par rapport aux critères de certification selon l'art. 34.

Art. 37 Clause de sauvegarde

L'application de la clause de sauvegarde est indépendante d'une éventuelle faute de la part d'une communauté, d'une communauté de référence ou d'un éditeur de moyens d'identification. On peut notamment penser à des situations dans lesquelles une interruption immédiate de la communication intercommunautaire se justifie du fait de menaces significatives dans le domaine des technologies de l'information et de la communication TIC (par ex. virus, chevaux de Troie, etc.) ou encore lorsque l'utilisation de certains moyens d'identification peut compromettre le dossier électronique du patient du patient. En revanche, lorsqu'une communauté, une communauté de référence ou un éditeur de moyens d'identification enfreint les critères de certification, l'art. 38 s'applique.

La *let. a* permet à l'OFSP de refuser provisoirement l'accès au dossier électronique du patient à des communautés et à des communautés de référence qui présentent un risque pour la protection et la sécurité des données. Lorsque la communauté ou la communauté de référence concernée a apporté la preuve que le ou les facteurs de risque ont été supprimés, l'enregistrement de données dans le service de recherche des communautés et communautés de référence peut à nouveau être activé.

En vertu de la *let. b,* l'OFSP a la possibilité d'interdire l'utilisation de moyens d'identification qui présentent un problème de sécurité au niveau collectif. En d'autres termes, il ne s'agit pas de bloquer le moyen d'identification d'un patient ou d'un professionnel de la santé en particulier, mais d'interdire une technologie qui ne satisfait pas (pour le moment) aux normes de sécurité.

L'OFSP peut ordonner un renouvellement extraordinaire de la certification au sens de la *let. c* lorsqu'une communauté ou une communauté de référence déclare un incident survenu dans le système de gestion de la protection et de la sécurité des données ayant un impact sur la sécurité (art. 12, al. 3) et que cet incident permet de penser que les critères de certification ne sont plus remplis. Un renouvellement extraordinaire peut également être ordonnée si, dans le cadre de la procédure de vérification visée à l'art. 34, l'organisme de certification constate qu'une communauté, une communauté de

référence ou un éditeur de moyens d'identification ne remplit plus les critères de certification ou s'il existe une suspicion fondée qu'ils ne sont plus respectés.

Tant qu'une communauté ou communauté de référence n'a pas passé avec succès la procédure de renouvellement de la certification, il est possible, selon l'ampleur des éléments à vérifier, qu'elle ne puisse plus participer à l'échange de données dans le cadre du dossier électronique du patient.
Pour les éditeurs de moyens d'identification, cela peut signifier que tant qu'ils n'ont pas passé avec succès la procédure de renouvellement extraordinaire de la certification, ils ne pourront pas identifier ou authentifier des professionnels de la santé ou des patients.

Selon l'*al. 2*, l'OFSP peut demander à l'organisme de certification ou à l'organisme titulaire d'un certificat les documents nécessaires à la certification ou au renouvellement de la certification. Ce n'est que sur la base de ces documents que l'OFSP sera, le cas échéant, en mesure d'identifier une mise en danger grave du dossier électronique du patient et de prendre les mesures qui s'imposent.

Section 3 : Sanctions

Art. 38

Si l'organisme de certification constate des défaillances graves dans le cadre de la procédure ordinaire de vérification (art. 34), il peut suspendre ou retirer la certification (*al.1).* Est notamment considérée comme une défaillance grave le fait que des critères essentiels de la certification ne sont plus remplis (let. a). Pour des communautés ou des communautés de référence cela serait le cas, par exemple, si l'on constatait de manière répétée que l'intégration des moyens d'identification ne fonctionne par parfaitement, que le système de gestion des accès ou le système de gestion des autorisations est défectueux, que la communication intercommunautaire n'est pas assurée ou encore que le portail d'accès refuse à une personne autorisée l'accès au dossier électronique du patient ou qu'il permet à une personne non autorisée d'y accéder. Ces défaillances entraînent le blocage de l'enregistrement dans le service de recherche des communautés et des communautés de référence certifiées (art. 40, al. 2). La *let. b* s'applique aux cas où un certificat est utilisé fallacieusement ou abusivement. C'est notamment le cas si un patient est trompé quant à la signification du certificat, par exemple lorsqu'une communauté de référence prétend être certifiée pour l'émission de moyens d'identification.

L'*al.* 2 précise expressément qu'en cas de litige, la procédure et l'appréciation matérielle de la situation sont régies par les dispositions de droit civil applicables.

En vertu de l'*al. 3*, l'OFSP peut ordonner à l'organisme de certification de procéders à un examen. L'office dispose ainsi de la base légale lui permettant d'agir, dans l'intérêt de la sécurité du dossier électronique du patient du patient, à l'encontre de communautés et de communautés de référence certifiées ou d'éditeurs certifiés de moyens d'identification en cas de suspicion fondée d'inobservation des critères de certification.

Chapitre 7 : Services de recherche de données

Section 1 : Généralités

Aux termes de l'art. 14 LDEP, l'OFSP gère les services de recherche de données qui fournissent uniformément à l'échelle nationale les données de référence nécessaires à la communication entre les communautés, les communautés de références et les portails d'accès. Ce chapitre de l'ODEP traite des exigences de contenu et d'utilisation des services de recherche ainsi que des conditions régissant leur exploitation.

Art. 39

Les données des services de recherche visées aux *let. a à d* sont indispensables à une communication conforme à la loi entre les communautés et les communautés de référence.
Le service de recherche des communautés et des communautés de référence visé à la *let. a* gère en particulier les données techniques nécessaires à la communication électronique avec les points d'accès correspondants. Afin de garantir l'intégrité des données électroniques des points d'accès, le service contient également les clés officielles permettant aux communautés et aux communautés de référence de vérifier l'authenticité des informations livrées par d'autres points d'accès (art. 40, al. 1, let. c).

Les informations relatives aux institutions de santé et aux professionnels de la santé habilités à traiter les données du dossier électronique du patient sont gérées par le service de recherche en application des *let. a et b*. L'appartenance des professionnels de la santé à des groupes de professionnels de la santé y figure également. Sur la base de ces informations, le patient peut attribuer les droits d'accès aux professionnels de la santé ou aux groupes de professionnels de la santé selon l'art. 2, al. 1)

Le service de recherche des métadonnées visé à la *let. c* contient les métadonnées à utiliser selon l'art. 9, al. 5, let. a, pour une description structurée des données enregistrées dans le dossier électronique du patient. Les valeurs et plages de valeurs des métadonnées sont définies à l'annexe 3 ODEP-DFI.

Le service de recherche visé à la *let. d* contient les OID nécessaires aux communautés et aux communautés de référence.

La responsabilité incombant à l'OFSP au titre de la gestion des services de recherche selon l'art. 14, al. 1, LDEP, couvre la mise en place, l'exploitation et le développement des services de recherche.

L'OFSP définit, lors de la constitution des services de recherche de données, les interfaces standard par lesquelles les communautés et communautés de référence certifiées peuvent obtenir ou fournir des données.

Section 2 : Contenu

Art. 40 Service de recherche des communautés et des communautés de référence

Pour permettre à l'OFSP de gérer les communautés et communautés de référence certifiées conformément à l'art. 33, al. 1, les organismes de certification doivent lui communiquer les informations énoncées à l'al. 1. Outre la désignation (*let. a*) et l'OID (*let. b*), d'autres données sont nécessaires pour servir à authentifier en toute sécurité les points d'accès des communautés et des communautés de référence certifiées ainsi que les informations qu'elles livrent (*let. c et d*). Ces données permettent de s'assurer que la source d'une information appartient légitimement à l'espace de confiance du dossier électronique et que la communication établie est fiable. Cette vérification doit être faite régulièrement, de manière à pouvoir interrompre rapidement l'échange de données avec un participant qui n'est plus digne de confiance.

Seul l'OFSP est habilité à traiter ces données (al. 2), les communautés et communautés de référence ayant uniquement le droit de les consulter.

Art. 41 Service de recherche des institutions de santé et des professionnels de la santé

Selon l'art. 9, let. d, les communautés et les communautés de référence doivent s'assurer que les données figurant dans le service de recherche des institutions de santé et des professionnels de la santé sont à jour. Le service de recherche est doté d'une interface standard par laquelle les données

du registre central des institutions de santé et des professionnels de la santé peuvent être tenues à jour et rendues disponibles à d'autres communautés et communautés de référence. L'*art. 41* précise les données que doivent fournir les communautés et les communautés de référence.

Parmi les données sur les institutions de santé et les groupes de professionnels de la santé visées à l'*al. 1, let. a*, figurent en particulier leur nom et leur adresse (*ch. 1*), l'OID (*ch. 2*) et, pour les institutions de santé, le numéro d'enregistrement (numéro REE) visé dans l'ordonnance du 30 juin 1993[12] sur le Registre des entreprises et des établissements (*ch. 3*). Les communautés et les communautés de référence doivent demander l'OID visé au ch. 2 pour les institutions de santé qui leur sont affiliées. Elles peuvent gérer elles-mêmes d'autres OID subordonnés à leur propre identificateur pour désigner les groupes faisant partie d'une institution de santé (art. 8, al. 1).

L'enregistrement du numéro REE visé au *ch. 3* est nécessaire au recoupement des données de l'institution de santé avec les statistiques officielles de l'OFS pour la collecte de données dans le processus d'évaluation de la loi (art. 22, al. 3).

Parmi les données sur les professionnels de la santé visées à la *let. b* figurent notamment leurs renseignements personnels (*ch. 1*), l'OID contenant le GLN (*ch. 2*) ainsi que le nom et l'adresse des institutions de santé ou des groupes de professionnels de la santé auxquels ils sont affiliés (*ch. 3*). L'OID mentionné au *ch. 2* est composé de l'OID commun aux Global Location Numbers (2.51.1.7) et du GLN spécifiquement attribué au professionnel de la santé. Pour un professionnel de la santé dont le GLN est 7601000000000, l'OID complet est donc 2.51.1.7.7601000000000.

En vertu de l'*al. 2*, les autres données à fournir au service de recherche auprès des institutions de santé et des professionnels de la santé sont définies dans le supplément 1 à l'annexe 5 de l'ODEP-DFI, ch. 1.10.

Art. 42 Service de recherche de l'OID

Les OID (identificateurs d'objet) sont des chaînes de chiffres organisées hiérarchiquement qui servent à attribuer un code unique à l'échelle mondiale à n'importe quel type d'objets, par ex. institutions, systèmes, documents, informations, certificats, classifications, etc. Le nœud d'identificateurs « eHealth-CH; 2.16.756.5.30 », dont la gestion incombe depuis le 1er janvier 2011 à la fondation RefData en sa qualité de bureau d'enregistrement des OID, a été désigné pour assurer un traitement uniforme de l'enregistrement, de l'attribution et de l'utilisation des identificateurs d'objet dans le domaine de la santé. L'enregistrement d'OID spécifiques au domaine de la santé sous « eHealth-CH » permet d'éviter la création d'autres sous-arborescences en lien avec le système de santé sous le nœud OID national. Selon le concept d'utilisation des identificateurs d'objet élaboré par eHealth Suisse, les organisations doivent avoir la possibilité de créer leurs propres OID et être en mesure d'élaborer et de gérer sous leur propre responsabilité d'autres OID dans le cadre de leur structure. Pour leur part, les titulaires d'OID sont tenus de publier leurs identificateurs d'objet dans le respect des dispositions de la protection des données lorsqu'ils référencent leurs domaines d'objet au moyen des OID. Les objets référencés dont la référence OID permet d'établir un lien avec l'état de santé d'une personne sont considérés comme particulièrement sensibles.

La gestion des OID est assurée depuis le 1er janvier 2011 par la fondation RefData en sa qualité de bureau d'enregistrement des OID. Les communautés et les communautés de référence peuvent y demander et y rechercher des OID à utiliser en application de l'art. 9, al. 1 (communauté ou communauté de référence) et al. 2, let. c (institution de santé). Les OID des groupes de professionnels de la santé sont gérés par les communautés et les communautés de référence elles-mêmes. L'OID d'un professionnel de la santé se déduit à partir de son GLN (cf. commentaire de l'art. 41).

[12] RS 431.903

Art. 43 Émoluments

Partant de l'hypothèse que la Suisse comptera une dizaine de communautés et de communautés de référence, il paraît raisonnable de fixer l'émolument annuel à 40 000 francs. La somme récoltée permettra un refinancement des coûts pour la constitution et l'exploitation des services de recherche sur une période de dix ans (*al. 1*). Cet émolument est forfaitaire, étant donné que les services de recherche de données sont utilisés dans une même mesure par toutes les communautés et communautés de référence. De plus, le volume de données à traiter par une communauté ou une communauté de référence pour le calcul des coûts est négligeable, la mise en place des services de recherche absorbant la plus grosse part des frais.

Pour le reste, les dispositions de l'ordonnance générale sur les émoluments du 8 septembre 2004 (RS 172.041.1), dans laquelle figurent en particulier des instructions relatives à la facturation, à l'échéance et à la prescription, sont applicables aux termes de l'*al. 2*.

Chapitre 8 : Entrée en vigueur

Art. 44

La LDEP et son droit d'exécution (ODEP, ODEP-DFI et OFDEP) entrent en vigueur le 15 avril 2017.