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)

Version du 22 mars 2016

Table des matières

1 Partie générale

1.1 Contexte

Le Parlement a adopté la loi fédérale sur le dossier électronique du patient (LDEP ; RS 816.11, 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 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 projet 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 du patient et, le cas échéant, si les professionnels de la santé en charge de son traitement ont un accès complet ou limité à ses données.
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], à savoir les hôpitaux, les maisons de naissance et les établissements médico-sociaux qui facturent des prestations à la charge de l'assurance obligatoire des soins. Les hôpitaux doivent s'affilier à une communauté ou à une communauté de référence certifiée dans un délai de trois ans, les maisons de naissance et les établissements médico-sociaux dans un délai de cinq ans.

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.

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 a la possibilité d'attribuer des droits d'accès individuels.

[1] RS **832.10**

Identité électronique
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 une identité électronique délivrée par un éditeur certifié de moyens d'identification.

Numéro d'identification du patient
Un numéro d'identification généré de façon aléatoire est utilisé comme caractéristique d'identification supplémentaire (numéro d'identification du patient) afin de pouvoir réunir de manière correcte et complète les données et documents d'un patient saisis dans le dossier électronique du patient, 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 sécurisé des données, tous les participants (communautés, communautés de référence, éditeurs de moyens d'identification) doivent respecter des prescriptions minimales de sécurité. Une procédure de certification garantit le respect des critères techniques et organisationnels.

Services de recherche de données
La Confédération exploite les services de recherche centraux nécessaires à la communication entre les communautés, les communautés de référence et les portails d'accès. En outre, elle soutient la mise en place et la diffusion du dossier électronique du patient au moyen de mesures d'information et de coordination.

Aides financières
Par ailleurs, la Confédération soutient la constitution et la certification des communautés et des communautés de référence pendant trois ans en allouant des aides financières à hauteur de 30 millions de francs. Ces aides sont liées à la participation des cantons ou de tiers. 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 (p. 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 communications électroniques, et le règlement (CE) 2006/2004 relatif à la coopération entre

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

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

<table>
<tr><td rowspan="2">Au niveau du Conseil fédéral</td><td>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 : Dispositions finales</td><td>Ordonnance sur les aides financières au dossier électronique du patient (OFDEP)
- Section 1 : Dispositions générales
- Section 2 : Calcul des aides financières
- Section 3 : Procédure
- Section 4 : Entrée en vigueur</td></tr>
<tr><td></td><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 : Vérification de la clé de contrôle
- 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, adaptations nationales des profils d'intégration et profils d'intégration nationaux
- Annexe 6 : Indicateurs pour l'évaluation
- Annexe 7 : Exigences minimales applicables à la qualification du personnel des organismes de certification
- Annexe 8 : Prescriptions relatives à la protection des moyens d'identification</td><td></td></tr>
</table>

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

[4] JO L 337 du 18.12.2009, p. 11
[5] JO L 88 du 4.4.2011, p. 45
[6] JO L 257 du 28.8.2014, p. 73

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 au dossier électronique du patient (OFDEP).

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 (chap. 2), les communautés et communautés de référence (critères de certification ; chap. 3), les moyens d'identification (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 contient à l'*annexe 1* une description détaillée de la logique de la clé de contrôle, à suivre lors de la vérification de cette clé de contrôle selon l'art. 4, al. 2, ODEP, et indique la composition du numéro d'identification du patient pour la présentation sous forme écrite.

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. 9, al. 3, let. b) 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. 9, al. 3, let. c, 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. 9, al. 3, let. d, ODEP) de l'ODEP-DFI 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. A moyen ou à long terme, il est prévu de soumettre les adaptations nationales et les profils d'intégration nationaux complémentaires aux organisations nationales ou internationales correspondantes (IHE Suisse ou IHE International) pour qu'elles les approuvent en tant que normes officielles. L'annexe 5 représente donc une solution transitoire en ce qui concerne les adaptations nationales et les profils d'intégration nationaux.

L'*annexe 6* (cf. art. 21 ODEP) énumère les données que les communautés et les communautés de référence certifiées mettent à la disposition de l'Office fédéral de la santé publique (OFSP) pour lui permettre de procéder à l'évaluation selon l'art. 18 ODEP.

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

L'*annexe 8* définit les prescriptions applicables à la protection de moyens d'identification.

Par ailleurs, l'OFSP définira, sous forme de règlements du traitement des données, les interfaces servant à la communication entre la CdC et les communautés ou communautés de référence et la communication entre les communautés ou communautés de référence et les services de recherche de la Confédération.

1.3.3 Ordonnance sur les aides financières au 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'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. 9, al. 4, 29, al. 3, et 30, al. 4, 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 l'environnement de certification nécessaire à la vérification des normes, standards et profils d'intégration et veille à la bonne exploitation et au développement de ce système de test (art. 27, al. 3, let. c, ODEP).

L'OFSP élabore et exploite les services de recherche de données nécessaires au fonctionnement du dossier électronique du patient ou assure la surveillance des tiers chargés de mettre en place et d'exploiter ces services (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. 21 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* accrédite les organisations qui entendent procéder à des certifications selon la LDEP. Ce faisant, il s'assure que les programmes de contrôle mis en œuvre 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 *Centrale de compensation (CdC)* est chargée d'attribuer et de gérer le numéro d'identification du patient selon l'art. 5, al. 1. Elle veille à ce que la base de données d'identification existante de la CdC soit développée de manière à réponde 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 l'un des quatre niveaux de confidentialité ci-dessous aux données de son dossier électronique. Il choisit librement le niveau qu'il entend attribuer à telle ou telle donnée. Il dispose, par exemple, des possibilités suivantes (*let. à a d*) :

1) « Données utiles » : p. ex. 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.
2) « Données médicales » : données et documents importants, p. ex. rapports, résultats d'examens, traitements dispensés, etc.
3) « Données sensibles » : informations jugées sensibles par le patient et que seuls des professionnels de la santé au bénéfice d'un droit d'accès « étendu » peuvent consulter.
4) « Données secrètes » : 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. le commentaire relatif à l'art. 2).

Si le patient ne choisit aucun niveau de confidentialité, le niveau « données médicales » est systématiquement attribué aux nouvelles données enregistrées dans le dossier électronique du patient (*al. 2*). Cette configuration de base peut être modifiée par le patient (cf. le commentaire relatif à l'art. 3).

Les professionnels de la santé peuvent déroger à la configuration de base prévue à l'al. 2 et attribuer le niveau de confidentialité « données sensibles » aux données qu'ils saisissent dans le dossier électronique du patient (*al. 3*). Ils ont ainsi 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 le patient. C'est le cas, par exemple, face à un diagnostic stigmatisant pour le patient ou lorsque le professionnel de la santé, de par la connaissance qu'il a de son patient, estime que celui-ci considérera certaines informations comme sensibles.

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 des droits d'accès incombe aux communautés de référence. La réglementation applicable en cas d'urgence médicale doit être garantie 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. Les droit d'accès suivants sont prévus (*let. a à c*) :

a) « Limité » : accès au niveau de confidentialité « données utiles »
b) « Normal » : accès aux niveaux de confidentialité « données utiles » et « données médicales »
c) « Etendu » : accès aux niveaux de confidentialité « données utiles », « données médicales » et « données sensibles ».

Seul le patient a accès au niveau de confidentialité « Données secrètes ».

Si, lors de l'attribution des droits d'accès, le patient ne sélectionne aucun droit d'accès selon les let. a), b) ou c), le droit d'accès « normal » est attribué par défaut.

En vertu de l'*al. 3*, les droits d'accès 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. le commentaire relatif à l'art. 3).

Pour des considérations pratiques, des droits d'accès peuvent aussi être accordés de manière sommaire à des groupes de professionnels de la santé (p. ex. groupe interdisciplinaire d'experts [*tumor board*] ou service hospitalier). Cela suppose que le patient peut 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. 40 ODEP) et s'informer de sa composition. Les droits d'accès des groupes de professionnels de la santé sont fonction de l'appartenance au groupe (*al. 4*). 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.

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. 5)*. Ils ont alors accès aux niveaux de confidentialité « données utiles » et « données médicales ». 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. Le professionnel de la santé qui entend consulter en urgence le dossier électronique d'un patient doit fournir une justification au préalable. Celle-ci peut être enregistrée, par exemple, sous la forme de mots-clés dans un champ de texte qui apparaît sur l'interface utilisateur en cas d'accès en urgence. Par ailleurs, afin d'empêcher un recours abusif à l'accès en cas d'urgence, p. ex. attaques automatiques visant un terminal, le professionnel de la santé doit en plus confirmer l'accès pour urgence médicale au moyen d'une action manuelle, non reproductible automatiquement (cf. ch. 9.6 des critères techniques et organisationnels de certification). 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.

Etant 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 incombe à la communauté (cf. ch. 9.6 CTO). Elle peut être déléguée à l'institution de santé où l'accès en urgence a eu lieu ; elle 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 électronique ou SMS.

Art. 3 Options du patient

Les différentes options à la disposition du patient en ce qui concerne les niveaux de confidentialité et l'attribution de droits d'accès sont énoncées à l'*art. 3*. 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 la *let. a*, le patient a la possibilité de limiter les droits d'accès à une période de six mois. Il peut ainsi 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 automatiquement au bout de six mois. Cette manière de procéder réduit le risque d'« oublier » que des droits d'accès ont été accordés.

Selon la *let. b*, le patient a la possibilité de limiter, d'étendre ou d'exclure totalement le droit d'accès à son dossier électronique du patient en cas d'urgence médicale. Il peut, par exemple, limiter l'accès au niveau de confidentialité « données utiles » ou l'étendre au niveau de confidentialité « données sensibles ». Il peut aussi exclure totalement la possibilité d'accéder à son dossier électronique du patient en cas d'urgence médicale (cf. art. 9, al. 5, LDEP).

D'après la *let. c*, le patient a la possibilité de modifier le niveau de confidentialité attribué de manière standard aux nouvelles données enregistrées dans son dossier électronique du patient. Il peut changer la configuration de base de manière à ce que le niveau de confidentialité « données sensibles » soit attribué aux nouvelles données. Il peut en tout temps revenir à la configuration de base.

En vertu de la *let. d*, le patient peut interdire à certains professionnels de la santé l'accès à son dossier électronique du patient (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.

Le patient est systématiquement informé lorsqu'un professionnel de la santé intègre un groupe auquel il a attribué un droit d'accès (cf. le commentaire relatif à l'art. 8, let. f). Selon la let. e, il peut renoncer à recevoir cette information.

Lorsque le patient accorde un droit d'accès à un groupe de professionnels de la santé, les professionnels qui intègrent ce groupe par la suite reçoivent en principe automatiquement le droit d'accès accordé au groupe. Selon la *let. f*, le patient a la possibilité de supprimer cet automatisme et de décider que le droit d'accès ne s'applique pas aux nouveaux professionnels qui intègrent le groupe.

Selon la *let. g*, 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. h*, 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 intervenant dans le traitement. Le professionnel de la santé habilité peut uniquement transmettre des droits d'accès équivalents aux siens et non des droits plus étendus.

Chapitre 2 : Numéro d'identification du patient

Art. 4 Format du numéro d'identification du patient

L'*al. 1* définit le format et la composition du numéro d'identification du patient visé à l'*art. 4 LDEP* composé de 11 chiffres. Le numéro d'identification se compose d'un numéro à 10 chiffres et d'une clé de contrôle. Il doit être attribué de manière univoque à une personne inscrite dans le registre de la base de données d'identification de la CdC en excluant toute possibilité d'identifier cette personne ou son numéro d'assuré selon l'*art. 50c de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS ;* « NAVS13 »)

Afin de limiter les risques d'erreur, une saisie manuelle du numéro d'identification du patient est autorisée uniquement si une vérification de la clé de contrôle selon les prescriptions du DFI est réalisée *(al. 2)*. Les prescriptions en question sont énoncées à l'*annexe 1 ODEP-DFI*.

Art. 5 Demande d'attribution d'un numéro d'identification du patient

La constitution du dossier électronique incombe à la communauté de référence du patient (*art. 14 à 16*). 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 selon l'*art. 16, let. d* (*art. 4, al. 1, LDEP*). Les critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (CTO) de l'*annexe 2 ODEP-DFI* énoncent que les communautés de référence doivent utiliser à cet effet les données de la pièce d'identité selon l'*art. 23, al. 1*.

Les *al. 2* et *3* portent sur les critères de qualité lors de l'attribution du numéro d'identification du patient. En principe, les données visées à l'*al. 2* devraient suffire pour identifier un patient de manière univoque 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)*.

Art. 6 Consultation du numéro d'identification du patient

La consultation, c.-à-d. l'attribution (*art. 5*), la consultation et l'annulation (*art. 7*) du numéro d'identification du patient peut s'effectuer par voie électronique.

Art. 7 Annulation

Lorsqu'un patient révoque son consentement, son dossier électronique du patient est supprimé (*art. 20*). 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 d'identification du patient n'est dès lors plus disponible pour consultation selon l'*art. 6*.

Pour éviter les risques de confusion liés à une double attribution, les numéros d'identification annulés ne sont pas réattribués à nouveau (*al. 2*).

Chapitre 3 : Communautés et communautés de référence

Section 1 : Communautés

Art. 8 Gestion

En application de la *let. a*, les communautés doivent définir, documenter, mettre en œuvre et respecter des processus appropriés pour gérer les institutions de santé (p. ex. hôpitaux, pharmacies, cabinets médicaux, organisations d'aide et de soins à domicile, EMS) ainsi que les professionnels de la santé et les groupes de professionnels de la santé qui intègrent une communauté ou qui en sortent.

Les CTO qui constituent l'annexe 2 ODEP-DFI concrétisent, dans leur chap. 1, 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.

Gestion des institutions de santé

Processus d'entrée

Ce processus 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 (cf. ch. 1.1.2.1 et 4.9 CTO). Dans le cadre de ces conventions, 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 (cf. *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.

Processus de sortie

Lorsqu'une institution de santé quitte une communauté sans s'affilier à une autre communauté ou communauté de référence, la communauté en question doit s'assurer que les documents mis à disposition par l'institution de santé dans le lieu de stockage de la communauté ou de l'institution pour des dossiers électroniques sont supprimés. Il en va de même des entrées correspondantes dans le registre des documents (cf. ch. 1.1.3 CTO). Lorsque des documents sont appelés à être supprimés du dossier électronique du patient suite au départ d'une institution de santé, ces patients doivent en être informés avant l'effacement afin qu'ils puissent accéder eux-mêmes aux documents à supprimer et, s'ils le souhaitent, les enregistrer dans leur dossier électronique du patient en vertu de l'art. 8 LDEP et de l'art. 18 ODEP.

Selon la *let c*, 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. 40 sont à jour. 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) (cf. ch. 1.1.4 CTO).

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 travaillant dans les institutions de santé qui leur sont affiliées. Ces processus doivent porter sur les aspects visés aux *let. b à d* et garantir le respect d'autres prescriptions. 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 (cf. notamment ch. 4.9.1 CTO) de même que sur les risques et les mesures dans le domaine de la protection et de la sécurité des données. Les communautés doivent en outre à

mettre en place 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 (cf. ch. 1.2.2.1 CTO). Il faut également définir la procédure concrète à suivre lorsqu'un professionnel de la santé quitte une communauté (p. ex. suite à un changement d'emploi, à une cessation d'activité professionnelle ou à un décès). 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. Les communautés peuvent déléguer ces tâches 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. 23, sauf si elle peut être effectuée avec un moyen d'identification émis par un éditeur certifié selon l'art. 30. La communauté doit en outre s'assurer qu'il s'agit bien d'un professionnel de la santé au sens de l'art. 2, let. b, LDEP (cf. ch. 1.2.2.3 CTO). A 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. 23, al. 2, soit se fonder sur l'inscription dans un registre professionnel cantonal ou fédéral (p. ex. Registre des professions médicales universitaires [MedReg], Registre des professions de la psychologie [PsyReg] ou Registre des professions de la santé [NAREG]).

Aux termes de la *let. c*, 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. 40. Si le professionnel de la santé est inscrit dans un registre professionnel fédéral ou cantonal (p. ex. MedReg, NAREG, etc.), les informations du registre doivent être reprises dans le service de recherche (cf. ch. 1.2.2.5 CTO). Il est important, en particulier, de s'assurer que seuls sont enregistrés 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.

Selon la *let. d*, les professionnels de la santé peuvent accéder au dossier électronique du patient uniquement en utilisant un moyen d'identification valable, émis par un éditeur certifié selon l'art. 30. Peu importe que l'accès ait lieu via le portail d'accès pour les professionnels de la santé (art. 10) ou via d'autres systèmes (p. ex. accès intégré dans un système primaire). Cela signifie que les systèmes utilisés par des professionnels de la santé ou des auxiliaires pour accéder au dossier électronique du patient supportent une procédure d'authentification forte, qui prévoit au moins deux facteurs d'authentification, comme condition préalable au traitement des données du dossier électronique du patient (cf. ch. 1.4.3 CTO). Lorsqu'une communauté certifiée procède à une authentification conformément à une telle procédure, les autres communautés doivent la reconnaître comme fiable.

Les communautés ont l'obligation d'établir un lien fiable entre l'identificateur univoque figurant dans le moyen d'identification des professionnels de la santé et de leurs auxiliaires et l'identité de chacune de ces personnes enregistrée dans la communauté (cf. ch. 1.4.2 CTO). En règle générale, l'identificateur est transmis au point d'accès du portail par le fournisseur de services d'identité (l'éditeur du moyen d'identification) dans le contexte de l'authentification.

Les professionnels de la santé peuvent confier le traitement de données du dossier électronique du patient à des auxiliaires dans la mesure où le rattachement de ces auxiliaires au professionnel de la santé qui en est responsable est géré en interne par la communauté. Mais comme ces auxiliaires ne figurent pas dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40, les patients ne peuvent pas gérer leurs droits d'accès de manière indépendante avec la fonction de gestion des autorisations. L'identification des auxiliaires et leur accès au dossier électronique du patient est soumise aux dispositions de l'*art. 8, let. b et d* (cf. ch. 1.3 CTO).

Gestion de groupes de professionnels de la santé
Selon la *let. c*, 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. 40. Elles peuvent déléguer cette tâche aux institutions de santé qui leur sont affiliées. Il faut veiller non seulement à ce que les données soient exactes et à jour, mais aussi, en application de la *let. e*, à ce que chaque patient puisse identifier en tout temps la composition des groupes de professionnels de la santé vu qu'ils peuvent leurs attribuer des droits d'accès (*art. 2, al. 1*) et que les professionnels de la santé qui intègrent un groupe a posteriori peuvent bénéficier des droits d'accès accordés au groupe (*art. 2, al. 4*) (cf. ch. 1.5 CTO). C'est le cas uniquement si le patient a opté pour cette fonction en vertu de l'*art. 3, let. f*, ou s'il n'a pas exclu le professionnel de la santé concerné de tout accès à son dossier électronique du patient (cf. *art. 3, let. d*).

C'est pourquoi la *let. e* précise que la composition des groupes de professionnels de la santé doit être identifiable en tout temps. Pour qu'un patient ne se retrouve pas dans l'obligation d'habiliter tout un hôpital à accéder à son dossier électronique du patient parce qu'il connaît uniquement le service dans lequel il est pris en charge, mais pas le nom des professionnels de la santé impliqués dans son traitement, les CTO précisent que les groupes de professionnels de la santé doivent avoir une taille raisonnable, c'est-à-dire une taille permettant au patient de gérer de manière appropriée les niveaux d'accès des professionnels de la santé impliqués dans son traitement, sans devoir donner accès à son dossier à un nombre disproportionné de professionnels non concernés (cf. ch. 1.5.2.3 CTO).

Aux termes de la *let. f*, les patients doivent être informés lorsque des professionnels de la santé intègrent un groupe. Cela donne aux patients l'opportunité de vérifier, si nécessaire, la composition du groupe et, selon l'option choisie en vertu de l'art. 3, let. f, d'accorder au nouveau membre du groupe le droit d'accès dont il ne bénéficie pas automatiquement ou bien de retirer ou d'adapter le droit d'accès qu'il a obtenu automatiquement du fait de son intégration dans le groupe.

Art. 9 Tenue et transfert des données

Cet article régit, à l'*al. 1, let. a et b*, ainsi qu'à l'*al. 2, let. c*, la suppression des données qui, en vertu de l'al. 1, let. c, ne peuvent être enregistrées que dans des lieux de stockage « secondaires » exclusivement prévus à cet effet et qui, par conséquent, peuvent être enregistrées dans les systèmes primaires sous la forme de « copies » des documents originaux. Dans des cas exceptionnels reposant sur des raisons techniques (cf. explications ad art. 9, al. 1, let. c), les données ou les documents ne sont pas enregistrés sous la forme de copies, mais sont consultés directement dans les lieux de stockage des systèmes primaires. Dans ce cas, l'obligation de suppression porte uniquement sur l'entrée correspondante dans le registre des documents (*al. 1, let. a et b, et 2, let. c*).

Al. 1

La *let. a* énonce que les données enregistrées dans le dossier électronique du patient par les professionnels de la santé sont effacées au bout de dix ans. Cette disposition a pour but de ne pas surcharger le dossier électronique du patient et d'en faire un instrument utile et clairement structuré pour toutes les parties. Les données enregistrées par les patients ne sont soumises à aucun délai d'effacement.

La suppression d'un dossier électronique du patient selon l'*art. 20, al. 1,* a pour conséquence (*let. b*) que l'état antérieur à la constitution du dossier électronique du patient doit être rétabli. Pour cela, il faut supprimer toutes les données se rapportant au patient considéré dans tous les systèmes interrogeables de la communauté (registre des documents, lieux de stockage des documents, index des patients, etc.) (cf. ch. 2.1.1.2 CTO). La responsabilité d'informer les communautés de la suppression du dossier électronique d'un patient incombe à la communauté de référence de ce patient (cf. art. 20, al. 2, let. a, ch. 1). Les données historisées ainsi que les données stockées dans des systèmes primaires non consultables et dans des sauvegardes de sécurité ne sont pas concernées.

Pour des raisons de protection et de sécurité des données, la let. c stipule que les données du dossier électronique du patient pertinentes pour le traitement ne peuvent être enregistrées que dans des lieux de stockage « secondaires » que la communauté ou les institutions de santé réservent exclusivement à cet usage. Cela signifie que ces lieux de stockage doivent contenir uniquement des documents figurant dans des dossiers électroniques. Ainsi, les professionnels de la santé enregistrent dans ces lieux

de stockage une copie des données et documents créés dans leur système primaire. Cette disposition a pour but que les documents du dossier électronique du patient soient conservés séparément sur le plan technique des documents enregistrés dans les dispositifs de stockage « primaires » (cf. ch. 2.2 CTO). En effet, les données du dossier électronique du patient ne sont pas soumises aux mêmes obligations que les données des systèmes primaires en ce qui concerne la conservation et l'effacement. Par exemple, il faut les détruire au bout de dix ans (al. 1, let. a), les détruire en totalité si le dossier électronique du patient est supprimé (al. 1, let. b) ou, à la demande du patient, procéder à un effacement sélectif (al. 2, let. b et c). En effet, une utilisation hybride du lieu de stockage ou la cohabitation des dossiers électroniques avec d'autres ensembles de données (p. ex. le système d'archivage interne d'un hôpital) constituerait un risque excessif pour la protection et la sécurité des données car il serait impossible d'isoler suffisamment bien la partie du lieu de stockage réservée aux dossiers électroniques par rapport à des groupes d'utilisateurs et des zones de réseau multiples, ce qui créerait une « perméabilité » non contrôlable entre le dossier électronique du patient et les autres données. Que la séparation soit physique (matériel séparé) ou logique (base de données séparées, machine virtuelle, séparation des mandants, etc.), les lieux de stockage « secondaires » doivent pouvoir être isolés de manière étanche des dispositifs de stockage primaires de manière à garantir, par des moyens techniques, une étanchéité fiable excluant toute « perméabilité » accidentelle (« défaut d'isolation »).

Al. 2
Le principe de l'autodétermination en matière d'information confère au patient le droit de décider lui-même du contenu de son dossier électronique du patient. C'est en vertu de ce principe que le patient dispose des possibilités énoncées à l'*al. 2* (cf. ch. 2.3 CTO).

L'art. 3, al. 2, LDEP instaure une présomption : les professionnels de la santé peuvent partir du principe que le patient ayant constitué un dossier électronique du patient souhaite que les données le concernant y figurent. En vertu de l'*al. 2, let. a*, le patient peut signaler en tout temps aux professionnels de la santé les documents qui ne doivent pas apparaître dans son dossier électronique du patient : il a donc la possibilité de s'opposer à cet automatisme au cas par cas.

Aux termes de la *let. b*, le patient peut exiger que les documents devant être effacés à l'échéance du délai de dix ans (al. 1) restent accessibles dans son dossier électronique du patient pour une nouvelle période de dix ans.

La *let. c* ménage au patient le droit de faire effacer certaines données le concernant dans son dossier électronique du patient. Les entrées correspondantes dans le registre des documents doivent être effacées, de même que les documents enregistrés dans les lieux de stockage du dossier électronique du patient. En ce qui concerne les documents dont les lieux de stockage de la communauté ne contiennent pas de copie (*al. 1, let. c*), mais auxquels on accède en faisant une requête auprès du système primaire, seules les entrées correspondantes dans le registre des documents seront effacées afin de ne pas porter atteinte aux obligations de documentation et de conservation en vigueur incombant aux professionnels de la santé.

Al. 3
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 aux *let. a à e*. Ces prescriptions concrètes portent, par exemple, sur la recherche de patients dans l'index des patients, sur la communication avec le registre des documents, les lieux de stockage des documents et la gestion des autorisations pour consulter ou mettre en ligne des documents ainsi que sur la communication avec les services de recherche visés aux art. 39 et 40 et avec la base de données d'identification (UPI) de la CdC. 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. 27, al. 3, let. c*). Ce système permet, par exemple, de vérifier si les

spécifications applicables aux interfaces techniques ainsi qu'à la communication entre les communautés et les communautés de référence et avec la CdC et les services de recherche ont été respectées au niveau structurel et sémantique lors de la mise en œuvre.

Let. a (gestion des autorisations)
Selon la *let. a*, les communautés et les communautés de référence 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'octroi et à la transmission des droits d'accès conformément aux *art. 1 et 2, al. 5, ODEP* soient appliquées correctement et respectées (cf. ch. 2.4 CTO). Les communautés sont en particulier tenues d'appliquer aux données qu'elles détiennent les niveaux de confidentialité (cf. *art. 1*) que le patient a attribués via le portail d'accès de la communauté de référence (cf. ch. 2.4.1.1 CTO).

Les communautés ont également l'obligation de garantir que l'accès aux données enregistrées dans leurs lieux de stockage et dans leur registre de documents ne peut avoir lieu qu'en conformité avec les droits accordés, qu'elles auront préalablement demandés à la communauté de référence (cf. ch. 2.5 CTO). Cela suppose, par exemple, d'une part, l'application de la décision découlant de l'évaluation des règles, par exemple si un professionnel de la santé a effectivement le droit d'accès nécessaire pour accéder au document qu'il demande à consulter ; d'autre part, il faut tenir compte du fait qu'un accès en cas d'urgence médicale, par exemple, est limité aux niveaux de confidentialité « données utiles » et « données médicales », sauf si le patient a décidé de limiter, d'étendre ou d'exclure ce droit en vertu de l'*art. 3, let. b*, ce dont il faut également tenir compte. A titre de sécurité supplémentaire, par exemple pour repousser les tentatives d'interception (attaques *man-in-the-middle* ou *man-in-the-client*), les CTO prévoient que les accès en cas d'urgence soient possibles uniquement après une double confirmation, moyennant une interaction manuelle, non reproductible automatiquement (p. ex. saisie d'un mot de passe à usage unique ou d'un identifiant personnel (NIP) généré par un dispositif à jetons local ou *token*) (cf. ch. 2.6.1.2 CTO).

Les options du patient énoncées à l'*art. 3* donnent lieu à d'autres obligations pour les communautés. Ainsi, il faut s'assurer du niveau de confidentialité à attribuer à chaque nouveau document enregistré dans le dossier électronique du patient car il est laissé au choix du patient dans la communauté de référence (cf. *art. 3, let. c*).

Des explications plus poussées concernant les niveaux de confidentialité, les droits d'accès et les options du patient figurent dans le commentaire des *art. 1 à 3*.

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 scénarios de test automatisés (cf. ch. 2.7 CTO).

Let. b (métadonnées)
Les métadonnées décrivent de manière structurée (p. ex. format technique de fichier, type de document, auteur, date de création, niveau de confidentialité) les documents mis en ligne dans le dossier électronique du patient. Selon la *let. b*, il faut utiliser à cet effet les attributs et leurs valeurs ou 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 (p. ex. terminologie de *Snomed CT*), qui permettent d'assurer une interopérabilité sémantique des métadonnées se rapportant aux documents. 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. 38, al. 1, let. b*.

Let. c (formats d'échange)
Tous les types de documents qu'il est possible de classifier au moyen des métadonnées peuvent être mis à disposition sous la forme de documents non structurés (p. 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 structurées par les professionnels de la santé. Pour que les formats d'échange puissent être utilisés de manière uniforme dans l'ensemble de la Suisse et qu'un soutien technique soit garanti, la Confédération gère un service de recherche des formats d'échange autorisés selon l'*art. 38, al. 1, let. c*.

Let. d (profils d'intégration IHE, adaptations nationales des profils d'intégration IHE, profils d'intégration nationaux du DFI)
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 standards reconnus.

En vertu de l'*al. 3, let. d*, le transfert d'informations à l'intérieur des communautés ainsi qu'entre elles et les communautés de référence doit en principe utiliser les transactions des profils d'intégration listés dans l'annexe 5 ODEP-DFI : il s'agit de profils d'intégration conçus par IHE (*Integrating the Healthcare Enterprise*), avec les adaptations nationales correspondantes (*national extensions*), ainsi que de profils d'intégration nationaux conçus par le DFI pour des cas d'application spécifiques.

Comme le stipule l'art. 27, al. 3, let. c, la conformité du transfert de données avec les profils d'intégration, leurs adaptations nationales et les profils d'intégration nationaux est vérifiée dans le cadre de la certification au moyen du système de certification. Les dispositions relatives au transfert de données portent, d'une part, sur les interfaces des systèmes primaires et des portails d'accès utilisés pour mettre à disposition et consulter des documents (acteurs IHE *Document Source* et *Document Consumer*) et, d'autre part, sur les interfaces avec d'autres systèmes utilisés à l'intérieur des communautés, comme par exemple les points d'accès (*gateways*), l'index des patients, les lieux de stockage de documents et les registres de documents. Il faut en outre vérifier la conformité de la communication avec les services de recherche visés à l'art. 38 ainsi qu'avec la CdC. 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 de produits (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 des interfaces toujours identiques 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.

Les profils d'intégration IHE (Integrating the Healthcare Enterprise) listés à l'annexe 5, chap. 1, ODEP-DFI sont des profils reconnus internationalement qui sont 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 concrétiser davantage dans des spécifications et de les compléter (« adaptations nationales »). Elles stipulent, par exemple, que certaines recherches peuvent être effectuées uniquement en utilisant le numéro d'identification du patient comme identificateur national, et non pas le NAVS13. Le chap. 2 de l'annexe 5 ODEP-DFI 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) sont renvoyées 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 certificats électroniques fiables permettant de vérifier l'authenticité des messages (cf. ch. 2.9.22 CTO). 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 (cf. ch. 2.9.25 CTO).

Let. e (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 personnelles 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 prescriptions relatives aux données historisées visées à l'*art. 9, al. 3, let. e, ODEP* se rapportent donc aux aspects pertinents pour la protection des données, qui font l'objet de dispositions concrètes dans les TOC (cf. ch. 2.10 CTO).

Les évènements consignés dans l'historique sont notamment : la mise en ligne et la requêtede documents, la modification de métadonnées (p. 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. L'historique consultable par le patient doit contenir au moins les informations suivantes (cf. ch. 2.10.4 CTO) :

- date et heure de l'accès ;
- identification de l'utilisateur ;
- identification du système depuis lequel l'accès a été effectué ;
- transaction effectuée (recherche, mise à disposition, lecture, écriture, mutation, etc.) ;
- contexte de la transaction (p. ex. accès d'urgence) ;
- dossier électronique du patient concerné ;
- données ou documents concernés.

Ces prescriptions ne concernent pas les autres historisations effectuées dans le cadre de l'exploitation technique qui sont sans rapport avec la protection ou la sécurité des données (p. ex. enregistrement de paramètres d'exploitation).

Pour que les patients puissent consulter à tout moment les historiques constitués de manière décentralisée concernant le traitement de leur dossier électronique du patient, les communautés doivent mettre en ligne les données historisées, sous une forme consultable, sur le portail d'accès dédié aux patients (cf. 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 au chap. 2 de l'annexe 5 ODEP-DFI, spécifient les transactions et le format technique d'échange à employer (cf. ch. 2.10.7 CTO). 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).

La génération des historiques technico-administratifs est, elle aussi, décentralisée dans les communautés. Ces données servent avant tout à vérifier le respect des prescriptions en matière de protection des données. C'est pourquoi elles doivent être accessibles uniquement aux personnes ou aux organes qui ont pour tâche de surveiller la mise en œuvre de ces prescriptions. Il faut les protéger en empêchant toute possibilité de modification par des moyens techniques ou organisationnels appropriés et les conserver durant dix ans (cf. ch. 2.10 CTO).

Art. 10 Portail d'accès pour les professionnels de la santé

Le portail d'accès pour les professionnels de la santé doit satisfaire aux exigences énoncées au chap. 3 CTO. Il faut, par exemple, que la présentation des données et des documents du dossier électronique du patient sur l'interface utilisateurs reflète l'ensemble des informations pertinentes de manière correcte et exhaustive (cf. ch. 3.2 CTO). Cela s'applique en particulier aux données structurées, comme par exemple les formats d'échange de données médicales visés à l'*art. 9, al. 3, let. c*. Le portail d'accès doit en outre indiquer clairement si un document a été mis à disposition par un professionnel de la santé ou par le patient lui-même, quels sont les documents qui ne sont plus valables ou encore s'il existe éventuellement d'autres versions d'un document.

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 (cf. ch. 3.3 CTO).

Pour des raisons d'interopérabilité et de sécurité des données, une liste exhaustive des types de fichier admis dans le dossier électronique du patient figure à l'annexe 3, chap. 8, ODEP-DFI (cf. ch. 3.4 CTO). Le portail d'accès doit offrir la possibilité de mettre en ligne ces types de fichier, de les rechercher et de les afficher. Les fichiers dans un autre format (p. ex. Word) doivent être convertis dans un format admis (p. ex. PDF/A) avant leur enregistrement dans le lieu de stockage.

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 les fichiers sur le système local. Pour des raisons de sécurité, il importe de définir pour la recherche et le téléchargement de documents des limites supérieures exprimées en nombre de documents (*rate limits*), dont le dépassement déclenche un dispositif de blocage adéquat ou des mesures de sécurité supplémentaires (cf. ch. 3.5.2. CTO). 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*) visant à limiter les requêtes en masse non autorisées et techniquement automatisées.

Art. 11 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 tel que décrit dans la norme ISO/IEC 27001:2013. Il doit être adapté à la complexité et à la taille de la communauté ainsi qu'au volume des données et des documents enregistrés par la communauté dans les dossiers électroniques de ses patients (cf. ch. 4.2 CTO). 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 (*plan, do, check, act* ; cf. chap. 4 à 10 de la norme ISO/IEC 27001:2013) un ensemble complet de mesures de sécurité appropriées (p. ex. des directives, des processus, des procédures, des structures d'organisation ou encore des fonctionnalités logicielles ou matérielles) dans le cadre d'un système de gestion intégré.

Outre les éléments énoncés aux *let. a à f*, 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 ainsi qu'un inventaire des moyens d'exploitation concernés (hardwares, software, fichiers de données, organisation structurelle, processus, etc.) (cf. ch. 4.2.2 CTO). De plus, toutes les modifications apportées aux moyens d'exploitation qui ont une incidence sur la sécurité doivent être évaluées et documentées.

Selon la *let. a*, 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 des données et la sécurité de l'information ainsi que d'appliquer des actions correctives (cf. ch. 4.3 CTO).

La *let. b* impose la mise en place d'un système de détection et de gestion des incidents de sécurité (cf. ch. 4.4 CTO). 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* et y réagir en recourant à des mesures et à des processus préétablis, avec des règles de compétence claires. A cet effet, les communautés doivent se doter d'un système SIEM (*Security Information and Event Management System*), qui détecte les anomales 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, dont la structure est adaptée à la communauté, détecte et traite au minimum les cyberattaques ainsi que les hausses inhabituelles du nombre d'accès en écriture ou en lecture aux lieux de stockage des documents, au registre des documents ou à l'index des patients, qui laissent supposer 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]). Les CTO comportent d'autres prescriptions à respecter par exemple en ce qui concerne la protection contre les logiciels malveillants ou la détection et la gestion des failles de sécurité (cf. ch. 4.6 et 4.7 CTO).

Concernant la gestion des incidents de sécurité détectés, les CTO formulent des prescriptions concrètes pour les procédures de déclaration et de traitement des événements pertinents pour la protection et la sécurité des données (ch. 4.5). 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 indispensable, en effet, 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'art. 11, al. 2, ODEP, les communautés doivent en outre disposer de procédures d'escalade 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 (cf. ch. 4.13 CTO).

Selon la *let. c*, il faut répertorier tous les éléments d'infrastructure informatique que la communauté utilise pour le dossier électronique du patient (cf. ch. 4.8.3 CTO). Le registre des systèmes primaires affiliés visé à la *let. d* a pour utilité de donner une vue d'ensemble de tous les systèmes primaires qui échangent des données avec les dossiers électroniques des patients (cf. ch. 4.8.3.8 CTO).

En application de la *let. e*, 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 membres du personnel, comme par exemple, le personnel du service informatique hospitalier (cf. ch. 4.9 CTO). 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. 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 (p. ex. en utilisant des logiciels contre les programmes malveillants et des systèmes de protection des réseaux) (cf. ch. 4.9.3 CTO). Les institutions de santé doivent à leur tour imposer ces exigences aux professionnels de la santé qui travaillent pour elles.

La 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 faut que ses exigences en matière de protection et de sécurité des données soient respectées non seulement par son personnel (p. ex. personnel du service d'assistance pour les professionnels de la santé), mais aussi par les éventuels tiers auxquels il est fait appel (p. ex. l'exploitant de la structure informatique de la communauté). C'est ce que prévoit la *let. f*. Les exigences qu'énoncent les CTO pour le personnel portent en particulier sur la gestion des personnes ainsi que de leurs accès et droits d'utilisateur (cf. ch. 4.10 CTO). 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 (cf. ch. 4.11 et 4.12 CTO). 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 (cf. ch. 4.11.5.5 CTO).

L'obligation de déclarer les incidents jugés importants pour la sécurité de l'information à l'organisme de certification et à l'OFSP qu'instaure l'*al. 2* 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 et les communautés de référence, mais aussi pour les organismes de certification et 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. Aux termes de l'*art. 36*, l'OFSP peut ordonner des mesures en cas de grave mise en danger de la protection ou de la sécurité des données du dossier électronique du patient. Les communautés et les communautés de référence ainsi que les organisations d'exploitation 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 des dangers.

En application de l'*al. 3*, le DFI complète, aux ch. 4.13 à 4.23 CTO, les prescriptions énoncées à l'*al. 1, let. a à f*, par des règles de protection et de sécurité des données qui portent, entre autres, sur les domaines suivants :

- sécurité d'exploitation, restauration des systèmes et historisation de l'exploitation des systèmes (cf. ch. 4.14 CTO) ;
- achat, développement et maintenance des systèmes (cf. ch. 4.15 CTO) ;
- cryptage de la communication et de l'enregistrement des données (cf. ch. 4.16 à 4.18 CTO) ;
- gestion des réseaux et des services réseau utilisés pour l'exploitation des systèmes (cf. ch. 4.19 à 4.22 CTO) ;
- accessibilité (cf. ch. 4.23 CTO).

Un aspect appelle des explications particulières : le choix des mesures pour mettre en œuvre les exigences en matière de cryptage des données doit se baser sur les risques et, notamment, tenir compte du volume de données à protéger. Il convient tout d'abord de sélectionner des algorithmes et des procédures cryptographiques sûrs, mais aussi en particulier d'utiliser un ou plusieurs niveaux de cryptage en fonction des risques (p. ex. cryptage des disques, des bases de données ou des applications). On a renoncé dans un premier temps à imposer dans les présentes dispositions d'exécution un cryptage systématique des contenus transmis (et pas seulement du canal de transmission) de terminal à terminal (*end-to-end-encryption* [E2EE]). En effet, il est actuellement impossible d'apporter des réponses défini-

tives à un certain nombre de questions sur la mise en œuvre des prescriptions techniques et organisationnelles dans l'architecture décentralisée du dossier électronique du patient. Cette architecture présente une complexité particulière en raison du fait qu'il ne s'agit pas d'une communication classique de point à point ou de point à multipoint, pour lesquelles il existe déjà des procédures établies, mais d'un accès partagé à des données mises à disposition de manière décentralisée et asynchrone avec plusieurs participants autorisés en mode dynamique.

Il faudra réévaluer en permanence les risques dans le domaine de la protection et de la sécurité des données en raison de l'augmentation du volume de données enregistrées dans le dossier électronique du patient en Suisse et des nouvelles possibilités de protection mais aussi d'attaque offertes par les progrès techniques. De nouvelles mesures devront être proposées, au fil des révisions des CTO, pour assurer la protection et la sécurité des données. Il est évident que le recours à un cryptage fort et aussi étendu que possible, idéalement de bout en bout, constitue un moyen particulièrement approprié pour échapper à un grand nombre de menaces. Il est donc recommandé d'anticiper le recours à des technologies de ce type, en particulier dans la conception de nouveaux environnements, d'autant qu'elles permettent de réduire grandement voire d'éliminer totalement d'autres risques. Ces mesures rendront superflues certaines mesures par ailleurs coûteuses (p. ex. dans le domaine organisationnel) et les économies ainsi réalisées compenseront en partie d'éventuels coûts supplémentaires.

Pour garantir une sécurité maximale au dossier électronique du patient, l'*al. 4* stipule que les données ne peuvent être stockées que sur des dispositifs de stockage exploités par des personnes morales qui accomplissent cette prestation sous le régime du droit suisse, dont l'activité est régie par le droit suisse exclusivement et qui fournissent la totalité de leurs prestations à l'intérieur du territoire suisse (cf. ch. 4.24 CTO). 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 complications dues à des dispositions de loi étrangères.

Art. 12 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 (cf. ch. 5.1.2 CTO) : 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

Art. 13 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 20* en plus des exigences formulées dans la section 1 (art. 8 à 12) pour les communautés en général.

Art. 14 Information du patient

Le consentement doit être précédé d'une information adaptée et objective du patient. L'information est fournie par la 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 porte au moins sur les points suivants (cf. ch. 6.1 CTO) :

Aux termes de la *let. a*, le patient doit être informé du but du dossier électronique du patient (cf. ch. 6.1.1 CTO). On pense ici en particulier aux aspects présentés dans le commentaire de 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 (p. ex. pas de communication point à point) 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 (cf. ch. 6.1.2 CTO). Il s'agit en particulier des possibilités de traitement de données à la disposition, d'une part, des patients et, d'autre part, des professionnels de la santé autorisés. 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 (cf. ch. 6.1.2.2 CTO). 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 ; cf. ch. 6.1.3.5 CTO). A ce sujet, il importe de préciser que les documents contenus dans un dossier électronique du patient qui a été révoqué ne figureront pas dans le nouveau dossier électronique du patient qui sera établi si le patient donne de nouveau son consentement car un nouveau consentement suppose l'assignation d'un nouveau numéro d'identification du patient (cf. ch. 6.1.3.6 CTO).

Aux termes de la *let. d*, l'information doit permettre au patient de savoir comment et à qui des droits d'accès peuvent être accordés (cf. ch. 6.1.4 CTO). L'information doit porter, entre autres, sur la configuration attribuée par défaut aux niveaux de confidentialité (*art. 1, al. 2*) et aux droits d'accès (*art. 2, al. 2*) lors de la constitution du dossier électronique du patient ainsi que sur les possibilités de les modifier (voir le commentaire de l'art. 3), sur la possibilité de modifier ou de retirer des droits d'accès et sur la manière de procéder 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. 9, al. 3, LDEP).

En vertu de l'*al. 2,* le patient doit également être informé des dispositions de sécurité recommandées (cf. ch. 6.1.5 CTO). Ces précisions concernent, par exemple, la manière d'utiliser en toute sécurité l'identité électronique, le moyen d'identification et les mots de passe, les risques auxquels sont exposés les patients et les comportements à adopter pour se protéger contre ces risques (p. 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. 15 Consentement

La loi dispose que le consentement doit être donné par écrit. L'*al. 1* 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. Il faut pour cela que les exigences soient conformes à l'art. 14, al 2bis, CO[7] (signature électronique qualifiée au sens de la loi sur la signature

[7] RS 220

électronique, SCSE[8]). 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. 16 Gestion

En vertu de l'*al. 1*, les communautés de référence doivent définir, documenter, mettre en œuvre et respecter des processus adéquats pour la gestion des patients (cf. ch. 8 CTO).

Aux termes de la *let. a*, les communautés de référence doivent régler les processus de constitution 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. 14* et l'obtention du consentement par l'*art. 15*. Le processus de sortie doit obéir aux prescriptions de l'art. 20, s'il s'agit d'une suppression du dossier électronique du patient, ou aux dispositions du ch. 8.4 CTO concrétisant le changement de communauté de référence (*let. e*).

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 (cf. ch. 8.2 CTO). A cet effet, la communauté de référence doit identifier le patient avec certitude (*let. b*). Le ch. 8.2.2 CTO 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. 30*, elle doit être conforme aux exigences définies à l'*art. 23*. 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. 8, let. d) – accèdent au dossier électronique du patient uniquement en utilisant un moyen d'identification valable émis par un éditeur certifié selon l'art. 30 (cf. ch. 8.3 CTO). Concrètement, cela signifie que le traitement des données du dossier électronique du patient ne peut se faire que via des portails d'accès et sur des terminaux qui supportent une procédure d'authentification forte conforme à l'état actuel de la technique et prévoyant au moins deux facteurs d'authentification de catégories différentes (p. ex. « savoir » et « avoir ») comme condition préalable au traitement.

Selon la *let. d*, les communautés de référence doivent se conformer aux dispositions des *art. 5 et 6* pour demander à la CdC un numéro d'identification pour le patient qui souhaite ouvrir un dossier électronique du patient. Ces dispositions, qui sont concrétisées sous le ch. 8.2.2.2 CTO, exigent des communautés de référence la garantie qu'un dossier électronique du patient est ouvert uniquement lorsqu'il est préalablement établi que la personne concernée n'en possède pas déjà un et que, par conséquent, cette personne ne possède pas de numéro d'identification du patient actif auprès de la CdC. Cela garantit qu'un patient ne peut avoir qu'un seul dossier électronique du patient à la fois et que ses données et ses documents sont systématiquement enregistrés dans ce dossier.

Les CTO contiennent 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 (cf. ch. 8.2.2.6 CTO) ainsi que l'attribution de l'identificateur univoque du moyen d'identification au bon dossier électronique du patient (cf. ch. 8.2.2.4 CTO). L'attribution d'une identité électronique à un dossier électronique du patient peut aussi avoir lieu de manière indirecte : par exemple, le portail d'accès peut associer l'identité électronique du patient à un code utilisateur local (*portal ID*), qui est associé au numéro d'identification du patient dans l'index des patients.

La *let. e* garantit que les patients ont la possibilité de changer de communauté de référence. A cet effet, le ch. 8.4.2.1 CTO 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

[8] RS 943.03

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, chap. 2, ODEP-DFI. 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. 3, let. h*, 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 (cf. ch. 8.4.2.2 CTO). Il en va de même des représentants, qui doivent être de nouveau enregistrés.

Aux termes de l'*al. 2*, les communautés de référence doivent remplir les critères techniques et organisationnels requis pour garantir l'application de l'*art. 2, al. 1 à 4*, et de l'*art. 3* (cf. commentaire de ces dispositions et ch. 8.5 à 8.7 CTO).

L'application de l'*art. 3, let. g*, (désignation d'un représentant) comprend, outre un volet technique, un volet organisationnel imposant des tâches concrétisées sous le ch. 8.8 CTO, raison pour laquelle elles sont expliquées ici. En vertu de l'*art. 3, let. g*, les communautés de référence doivent garantir au patient la possibilité de désigner un représentant. 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. 30, 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 (cf. ch., 8.8.3.3 CTO). 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. 30*, elle doit également être conforme aux exigences définies à l'*art. 23* (cf. ch. 8.8.3.1 CTO). Il faut en outre garantir que le représentant a accès au dossier électronique du patient uniquement pendant la durée de validité de sa représentation (cf. ch. 8.8.3.5 CTO). 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. 17 Portail d'accès pour les patients

Le portail d'accès pour les patients doit être conforme aux exigences énoncées à l'annexe 2 ODEP-DFI (cf. ch. 9 CTO). 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. 10* (cf. commentaire de l'art. 10). D'autres spécifications portent plus particulièrement sur la présentation des informations du dossier électronique du patient sous une forme adaptée aux patients, sur la mise en œuvre des différentes possibilités d'attribution des niveaux de confidentialité et d'octroi des droits d'accès selon les *art. 1 et 2* ainsi que sur les options offertes au patient (*art. 3*). Ne sont pas concernées les dispositions des *art. 1, al. 2 et 3, art. 2, al. 4 et 5, et art. 3, let. g*, qui n'ont pas pour objet des fonctions directes du portail d'accès pour les patients.

Il faut que le portail d'accès fasse 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 (cf. ch. 9.1 CTO). 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 dispositifs de stockage situés « en dehors » du dossier électronique du patient.

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 un document a été mis à disposition par un professionnel de la santé ou par le patient (cf. ch. 9.2 CTO). La présentation des métadonnées prescrites par le DFI selon l'annexe 3 ODEP-DFI doit utiliser les termes et expressions préconisés pour la langue choisie (FR/DE/IT ; *defined terms*) ~~ou leur équivalent anglais~~ (cf. ch. 9.2.1.7 CTO).

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 (cf. ch. 9.3 CTO). 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.

Sur le portail d'accès qui leur est destiné, les patients doivent en outre avoir la possibilité de consulter à tout moment les données historisées suite au traitement de leur dossier électronique du patient (*art. 10, al. 1, let. b, LDEP*) (cf. ch. 9.6 CTO). Comme les données à consigner dans l'historique peuvent être générées dans plusieurs communautés, il faut que toutes les données historisées soient récupérées auprès des différentes communautés concernées (cf. commentaire ad *art. 9, al. 3, let. e*) et mises en ligne sous une forme consolidée et lisible sur le portail d'accès afin que le patient puisse les y consulter. La présentation des données historisées à des fins de consultation obéit aux spécifications visées à l'art. 5, let. c, ODEP-DFI.

Art. 18 Disponibilité des données enregistrées par les patients

Le patient a la possibilité de saisir lui-même, via le portail d'accès, ses propres documents 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 (cf. ch. 10.1.2 CTO).

Pour des raisons de sécurité des données, il n'est pas permis de conserver les documents enregistrés par le patient lui-même dans les lieux de stockage des institutions de santé affiliées. Les communautés de référence doivent donc mettre à disposition des lieux de stockage internes dédiés aux données enregistrées par les patients. L'espace de stockage fourni à cet effet doit être suffisant.

Le ch. 10.2 CTO 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. Pour éviter que l'intégrité des données subisse des atteintes (p. ex. lors d'une manipulation hors ligne), il faut prévoir une procédure appropriée (p. 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 (cf. ch. 10.2.2 CTO).

Art. 19 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. 12*), 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 (cf. chap. 11 CTO). 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. 20 Suppression du dossier électronique du patient

Le dossier électronique du patient d'un patient est supprimé, aux termes de l'*al. 1*, lorsque le patient révoque son consentement à la tenue de son dossier électronique du patient, s'il n'y a eu aucun accès au dossier électronique du patient pendant dix ans ou en cas de décès du patient. Cette suppression implique que toutes les données doivent être effacées en vertu de l'*art. 9, al. 1, let. b* (cf. ch. 12.1 CTO).

L'*al. 2* et les dispositions concrètes énoncées aux ch. 12.3 et 12.4 CTO régissent les mesures que la communauté de référence doit mettre en œuvre en cas de suppression d'un dossier électronique du patient. Après avoir identifié de manière sûre le patient qui révoque son consentement (cf. ch. 12.3.1.1 CTO), la communauté de référence doit s'assurer que tous les droits d'accès au dossier électronique du patient à supprimer sont retirés sans délai (*al. 2)*. Les communautés et communautés de référence doivent alors s'assurer que l'ensemble des données et des documents enregistrés dans le dossier électronique du patient sont effacés conformément à l'art. 9, al. 1, let. b (cf. commentaire de cette disposition). De plus, la communauté de référence du patient est tenue d'informer de la révocation, de manière fiable et dans un délai convenable, l'ensemble des communautés (*al. 2, let. a, ch. 1*) ainsi que la CdC afin qu'elles puissent effacer les données et les documents associés à ce dossier électronique du patient dans leurs systèmes respectifs. Afin d'assurer la traçabilité, la déclaration de révocation doit être conservée durant dix ans par la communauté de référence (*al. 2, let. a, ch. 2*).

Pour appliquer le principe de l'économicité des données, les dossiers électroniques auxquels il n'a pas été accédé pendant dix ans sont supprimés (*al. 1, let. b*). En vertu de l'*al. 2, let. b*, le patient est informé de la suppression à venir de son dossier trois mois au préalable afin qu'il ait l'opportunité de s'y opposer à l'effacement.

Lorsqu'une communauté de référence apprend le décès d'un patient (al. 1, let. c), elle doit, comme en cas de révocation, supprimer le dossier électronique du patient et en informer la CdC et les autres communautés. 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. 9, al. 1, let. b. La définition des procédures applicables doit respecter les prescriptions du droit civil, en particulier en ce qui concerne les droits des proches concernant les données du dossier électronique du patient.

Section 3 : Données à fournir pour l'évaluation

Art. 21

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 sur un système de monitoring qui fournit les données nécessaires à l'évaluation. Les indicateurs à relever sont énumérés à l'annexe 6 ODEP-DFI. Il s'agit en particulier de données concernant le nombre de professionnels de la santé et de patients affiliés auprès de la communauté ou de la communauté de référence, mais aussi des données relatives à l'octroi des droits d'accès. Il s'agit également de données concernant le nombre de documents et de types de documents mis à disposition ainsi que des données sur l'utilisation du dossier électronique du patient par les professionnels de la santé et par les patients. Comme ces données se rapportent au fonctionnement courant des communautés et des communautés de référence, leur collecte ne leur impose pas de travail supplémentaire. Dans la mesure où les indicateurs permettent d'établir un lien avec des professionnels de la santé ou des patients individuels, les données doivent être communiquées à l'OFSP sous une forme anonymisée.

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. 30*.
La certification des éditeurs de moyens d'identification et les exigences techniques minimales prévues quant au niveau de sécurité sont déterminantes pour la fiabilité du moyen d'identification. Elles fournissent la certitude que la personne, patient ou professionnel de la santé, qui demande un moyen d'identification est effectivement celle à laquelle cette identité a été attribuée.

La gestion d'un moyen d'identification tout au long du cycle de vie se base sur le déroulement décrit dans la norme ISO/IEC 29115:2013 pour la demande, l'édition et la révocation des moyens d'identification ainsi que pour les objectifs de contrôle des procédures d'authentification. Les moyens d'identification contiennent des références d'authentification secrètes et publiques (*credentials*), p. ex. fichiers secrets de mots de passe, clés secrètes, certificats publics ou autres données d'identification, mémorisées en toute sécurité comme objet de données sur un hardware (p. ex. terminal mobile, tablette, PC, etc.) ou un autre support (p. ex. carte à puce). A l'aide de ce moyen d'identification, contrôlé par son titulaire, celui-ci s'authentifie auprès d'un participant au système fiable (portails d'accès de communautés ou de communautés de référence, mais aussi systèmes primaires connectés exploités par des professionnels de la santé pour accéder au dossier électronique du patient et portails d'accès d'éditeurs de moyens d'identification). L'édition de moyens d'identification comprend, entre autres, des procédures partielles comme l'initialisation, la demande, l'enregistrement et la saisie et vérification de l'identité. La gestion des moyens d'identification prévoit elle aussi des procédures partielles, notamment la création, la personnalisation, l'initialisation et le rattachement des références d'authentification à la personne ainsi que l'édition, l'activation, la révocation et le renouvellement.
Ces procédures partielles peuvent être regroupées ou se dérouler dans des ordres différents.
Par exemple, l'étape de saisie des données d'identité peut être suivie de l'étape personnalisation après édition du moyen d'identification, ou alors le moyen d'identification a déjà été personnalisé au moment de l'édition. 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 (p. 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 via une procédure. Des supports d'identité électronique déjà délivrés, comme la carte d'assuré selon l'art. 42*a* de la loi fédérale sur l'assurance-maladie (RS 832.10), peuvent ainsi servir à remplir, après coup, les exigences auxquelles doivent satisfaire les moyens d'identification selon l'ODEP.

Art. 22 Exigences applicables aux moyens d'identification

Les exigences applicables aux procédures d'identification, à l'édition et à la gestion des moyens d'identification, les règles techniques de procédure, les exigences à l'égard des moyens d'identification pour le processus d'authentification et les critères de protection applicables aux services concernés figurent dans la norme ISO/IEC 29115:2013 pour ce qui est des 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 (p. ex. portail d'accès d'une communauté ou d'une communauté de référence) 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, p. ex., de pièces d'identité perdues, volées, suspendues, révoquées ou échues (cf. *art. 23, al. 1*).

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, p. ex. en captant des mots de passe transmis en clair (*let. b*).

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 » (p. ex. mot de passe secret) et « possession » (p. 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 dix ans.

Art. 23 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 (p. ex. « identification jaune » de La Poste ou procédure d'identification par vidéo certifiée). 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. 3*). Les exigences auxquelles doit satisfaire le service d'enregistrement (*registration authority*) sont définies dans le profil de protection selon l'art. 30, al. 2 (*chap. 4.2 Objectifs de sécurité portant sur l'environnement)*.

Le moyen d'identification peut également servir à confirmer les données du « professionnel de la santé » (cf. *art. 8, let. b et d)*. A cet effet, l'éditeur saisit et vérifie l'identifiant (GLN) du professionnel de la santé (cf. *art. 24, al. 2*). Selon l'*al. 3*, 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. Cela peut se faire, par exemple, en comparant les données personnelles de la personne avec celles figurant dans le registre des professions médicales pour les titulaires d'un diplôme ou d'un titre postgrade fédéral ou délivré à l'étranger et reconnu selon la loi fédérale du 23 juin 2006 sur les professions médicales universitaires (RS 811.11). L'éditeur du moyen d'identification peut déléguer à des tiers le soin de confirmer les données du « professionnel de la santé » (*al. 3*). Cette preuve pourrait être fournie par les associations professionnelles ou les institutions de santé concernées de la communauté ou de la communauté de référence.

Art. 24 Données du moyen d'identification

L'éditeur enregistre les données d'identification des patients (*al. 1*) et des professionnels de la santé (*al. 1 et 2*) à des fins de preuve et de vérification d'identité. Ces données peuvent être transmises accompagnées du moyen d'identification aux portails d'accès des communautés et communautés de référence (*al. 3*).

Selon l'*al. 4*, l'éditeur doit informer le demandeur des dispositions de sécurité à respecter lors de l'utilisation du moyen d'identification. Ces précisions concernent, par exemple, 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 ou encore les conditions générales dans le cadre d'une déclaration de protection des données.

Art. 25 Renouvellement de la durée de validité du moyen d'identification

A l'échéance de la durée de validité du moyen d'identification de dix ans au maximum (cf. *art. 22, 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. 26 Blocage du moyen d'identification

Le titulaire du moyen d'identification peut à tout moment en demander le blocage pour empêcher l'accès au dossier électronique du patient. L'éditeur du moyen d'identification doit s'assurer que la personne à l'origine de la demande a qualité pour effectuer cette démarche ; il doit prendre les dispositions nécessaires pour empêcher un blocage non autorisé. Les moyens d'identification qui ont été bloqués ne peuvent être ni renouvelés ni prolongés. L'ordonnance ne prévoit pas de suspension provisoire du moyen d'identification. Les éditeurs de moyens d'identification doivent immédiatement prendre les dispositions nécessaires pour empêcher une authentification après blocage (p. ex. en élaborant des listes de certificats bloqués ou en mettant en place d'autres procédures pour valider la réponse d'authentification valable).

Chapitre 5 : Accréditation

Art. 27 Critères

Selon l'*al. 1*, les exigences auxquelles doivent satisfaire les organismes de certification se fondent essentiellement sur la norme ISO/IEC 17021:2015 Évaluation de la conformité -- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management dont les modalités d'application sont régies à l'art. 7, al. 1, et à l'annexe 2 de l'ordonnance sur l'accréditation et la désignation (OAccD ; RS 946.512). Ces dispositions définissent notamment le principe d'indépendance ainsi que la procédure de certification et d'examen des produits. Une réglementation supplémentaire dans le cadre de la présente ordonnance n'est donc pas nécessaire. En vertu de l'art. 13, al. 1, let. a, LDEP, la certification peut uniquement être effectuée par des organismes accrédités.

Etant donné que la certification des communautés et des communautés de référence se fonde sur des éléments choisis de la norme ISO/IEC 27001:2013, ISO/IEC 27006:2015:2013 constitue une base supplémentaire pour l'accréditation.

Selon l'art. 22, let. a, ODEP, la certification d'éditeurs de moyens d'identification s'effectue en correspondance avec les prescriptions de la norme ISO/IEC 29115:2013 ; ainsi, ce standard est également déterminant dans le cadre de l'accréditation d'organismes de certification qui proposent des certifications pour les éditeurs de moyens d'identification.

Les communautés, les communautés de référence et les éditeurs de moyens d'identification accomplissant des tâches spécifiques, les vérifications effectuées dans le cadre de la certification portent pour chacun d'eux sur des contenus différents. C'est aussi la raison pour laquelle les organismes concernés doivent répondre à des exigences différentes en termes d'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 surveillance et la recertification ;

let. b). La *let. c* stipule en outre 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. 4*, le DFI fixe les exigences applicables à la qualification du personnel chargé de réaliser les certifications (cf. annexe 7, 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. 28 Procédure d'accréditation

Cette disposition concrétise l'art. 11, al. 1 et 2, OAccD, en ce sens qu'elle prévoit le concours de l'OFSP.

Chapitre 6 : Certification

Section 1 : Critères de certification

Art. 29 Communautés et communautés de référence

Un organisme de certification accrédité selon l'art. 27 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. 8 à 12) mais également ceux énoncés aux art. 13 à 20.

L'*al. 2* délègue au DFI la compétence de régler en détail les critères de certification.

La compétence de modifier les critères de certification en fonction des progrès de la technique incombe à l'OFSP sur la base de l'art. 12, al. 2, LDEP (*al. 3*). Cette disposition est importante en particulier en ce qui concerne les critères de certification dans le domaine des données et de la transmission des données (art. 9) ainsi que la protection et la sécurité des données (art. 11).

Section 2 : Editeurs de moyens d'identification

Art. 30 Editeurs de moyens d'identification

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

Au moyen de procédures adaptées, l'éditeur s'assure que le personnel et les sous-mandataires possèdent 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, à l'assurance 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 applique des méthodes éprouvées en matière de protection et de sécurité des données ainsi que des procédés préconisés selon les normes ISO/IEC 27000 et 20000.

Les services d'identification et d'authentification des éditeurs de moyens d'identification ainsi que les portails d'accès des communautés et communautés de référence doivent répondre à des critères de sécurité précis. La norme ISO/IEC 29115:2013 contient une liste non exhaustive d'éléments pouvant entraver le bon déroulement de la procédure d'authentification. Des critères de sécurité sont prévus pour chaque élément répertorié, sans préciser pour autant lesquels doivent être remplis dans une situation donnée, la manière de procéder, à quel moment intervenir et les combinaisons voulues.

En vertu de l'*al. 2*, le DFI concrétise la mise en œuvre de ces critères au niveau des prestations, des applications, des moyens d'identification et des installations de l'éditeur en élaborant un profil de protection (exigences de sécurité fonctionnelles) selon les normes ISO/IEC 15408-1:2009, 15408-2:2008 et 15408-3:2008 (cf. annexe 8 ODEP-DFI). Ce profil doit correspondre au niveau d'évaluation 2 (cf. infra).

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. Contrairement aux critères de sécurité spécifiques applicables aux produits ou aux fabricants, le profil de protection sert de cahier des charges pour les critères applicables dans l'environnement considéré et définit le degré de contrôle de leur mise en œuvre.

La cible d'évaluation (*Target of Evaluation* [TOE]) du profil de protection comprend le moyen d'identification proprement dit (références d'authentification et caractéristiques d'identification qui figurent sur les équipements), le fournisseur d'identité (*Identity Provider*) pour l'identification et l'authentification ainsi que les interfaces techniques nécessaires et les canaux de communication pour une authentification fiable au portail d'accès des communautés et des communautés de référence. Des canaux à créer pour des composants externes hors TOE et des canaux entre les composants du TOE peuvent également relever des éléments supportés par les fonctions de sécurité pour assurer une exploitation sûre. L'environnement d'intervention prévu a aussi son importance et doit répondre à différents critères. Les exigences posées pour l'exploitation en toute sécurité du fournisseur d'identité correspondent à la norme ISO/IEC 27001:2013.

Le degré de contrôle de la mise en œuvre des exigences de sécurité est défini dans la norme ISO/IEC 15408-3:2008 au moyen d'*assurance packages* (niveaux d'évaluation [*evaluation assurance level*, EAL]). Ces niveaux couvrent notamment les domaines *development*, *life-cycle support*, *security target evaluation* ou *vulnerability assessment*. Pour l'examen du TOE, il y a lieu d'appliquer les directives prévues pour les différentes classes d'assurance en garantissant le respect des exigences définies à l'égard de l'environnement du TOE. A cet effet, les données correspondantes sont relevées et vérifiées dans la procédure de certification.

Section 3 : Procédure de certification

Art. 31 Déroulement

La procédure de certification prévue à l'art. 31 s'inspire de la norme ISO/IEC 17021:2015 et définit, par ordre chronologique, les différentes étapes de la procédure.

Le pré-audit visé à l'*al. 1* permet à l'organisme de certification d'évaluer, sur la base de la documentation qui 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 selon l'*al. 2*, l'organisme de certification vérifie également sur place si les prescriptions selon la présente ordonnance sont respectées.
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 énoncés.

Art. 32 Déclaration à l'OFSP

Afin d'assurer l'échange intercommunautaire de données, les communautés et communautés de référence certifiées doivent être enregistrées auprès du service de recherche des communautés et communautés de référence certifiées au sens de l'art. 39 (*al. 1*). Pour cette raison, toute certification acceptée doit être annoncée à l'OFSP.

Les suspensions et les retraits de certification doivent également être annoncés sans délai pour que la communauté ou communauté de référence concernée puisse être bloquée dans le service de recherche des communautés et communautés de référence certifiées.

Outre à l'enregistrement des données dans le service de recherche des communautés et communautés de référence certifiées (*al. 1*), l'OFSP procède à la publication d'un registre des certificats délivrés (*al. 2*). Ce registre permet aux patients d'avoir une vue d'ensemble des communautés et communautés de référence qui proposent un dossier électronique du patient selon la LDEP et quels sont les éditeurs de moyens d'identification certifiés.

Art. 33 Surveillance

Selon l'*al. 1*, l'organisme de certification vérifie annuellement 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. 36, let. c, peut ordonner une recertification extraordinaire. Si l'inobservation des critères de certification concerne des domaines partiels isolés, l'examen peut se limiter à ces éléments.

Art. 34 Durée de validité

Le certificat est établi pour une durée de trois ans. Les art. 33, al. 2, 35 et 36, let. c, demeurent réservés. La procédure de recertification doit être engagée avant l'échéance du certificat si la communauté ou la communauté de référence entend pouvoir 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. La recertification s'aligne sur les dispositions prévues à l'art. 31.

Art. 35 Déclaration d'adaptations techniques et organisationnelles à caractère substantiel

Si une communauté, une communauté de référence ou un éditeur de moyens d'identification déclare des adaptations selon l'*al. 1*, l'organisme de certification décide, conformément à l'*al. 2*, s'il y a lieu de les examiner dans le cadre de la surveillance selon l'*art. 33*, d'une recertification ou d'une recertification extraordinaire selon l'*art. 36, let. c*. La surveillance et la recertification s'effectuent au rythme habituel, la recertification 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 recertification extraordinaire n'a pas abouti. L'exclusion peut être prononcée par l'organisme de certification sur la base de l'art. 37 (sanctions) ou par l'OFSP sur la base de l'art. 36 (clause de sauvegarde) lorsque l'organisme de certification lui signale des écarts substantiels par rapport aux critères de certification selon l'art. 33.

Sont considérées comme des adaptations techniques ou organisationnelles à caractère substantiel en particulier des procédures nouvelles ou modifiées (en rapport avec la certification), des adaptations apportées à l'infrastructure informatique assurant l'échange intercommunautaire des données des communautés et communautés de référence ou encore une modification de la procédure d'authentification pour les éditeurs de moyens d'identification.

Art. 36 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 (p. 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. 37 s'applique.

La *let. a* permet à l'OFSP de refuser provisoirement à des communautés et communautés de référence qui présentent un risque pour la protection et la sécurité des données l'accès au dossier électronique du patient.
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 faculté d'interdire l'utilisation de moyens d'identification qui présentent un problème de sécurité au niveau collectif.

L'OFSP peut ordonner une recertification extraordinaire selon la *let. c* lorsque des communautés ou communautés de référence déclare un incident survenu dans le système de gestion de la protection et de la sécurité des données ayant un impact en termes de sécurité (art. 11, al. 2) et que cet incident permet de penser que les critères de certification ne sont plus remplis.
La recertification peut également être ordonnée si, dans le cadre de sa surveillance, 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 recertification, 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 recertification extraordinaire, ils ne pourront pas identifier ou authentifier des professionnels de la santé ou des patients.

Section 4 : Sanctions

Art. 37

Si l'organisme de certification constate des défaillances graves dans le cadre de son activité de surveillance courante (art. 33), 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. Pour des communautés ou 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 communautés de référence certifiées (cf. art. 39, al. 2).

Les sanctions sont déjà prévues dans la norme ISO/IEC 17021:2015. Etant donné que l'accréditation se fonde essentiellement sur cette norme, cette disposition revêt un caractère purement déclaratoire, qui doit néanmoins être inscrite dans l'ordonnance par souci de clarté. Ainsi, la réglementation de la suspension ou du retrait d'une certification ne doit pas non plus être précisée dans l'ordonnance. Il convient de préciser ici que cette disposition *ne confère pas* aux organismes de certification la compétence de rendre des décisions. 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 que l'organisme de certification procède 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. 38

Les données des services de recherche visées aux *let. a à d* sont indispensables pour que la communication entre les communautés et les communautés de référence soit conforme à la loi. Selon la *let. c*, le service de recherche assure en outre l'interopérabilité sémantique des formats d'échange médicaux structurés. Ces formats sont mis uniformément à la disposition des communautés et des communautés de référence de l'ensemble du pays par l'intermédiaire des services de recherche. Les services de recherche ne gèrent pas de données médicales.

Les données du service de recherche des communautés et communautés de référence certifiées visées à la *let. a, ch. 1,* gèrent en particulier les données techniques de 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 des données permettant aux communautés et communautés de référence de vérifier l'authenticité des informations livrées par d'autres points d'accès (cf. art. 39, al. 1, let. d).

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 et mises à disposition par le même service de recherche (*al. 1, let. a, ch. 2*). 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.

Les métadonnées présentent sous forme structurée les documents mis en ligne dans le dossier électronique du patient (p. ex. type de fichier, type de document, auteur, date de création, niveau de confidentialité). Le service de recherche des métadonnées autorisées selon l'*al. 1, let. b*, contient les métadonnées à utiliser selon l'art. 9, al. 3, let. c, pour décrire les documents du dossier électronique du patient. Il contient les attributs de métadonnées définis à l'annexe 3 ODEP-DFI, qui doivent donc obligatoirement être utilisés pour les documents, ainsi que les valeurs ou domaines de valeur admis. Des listes de valeurs de codes sémantiques normalisés (p. ex. issus de la terminologie *Snomed CT*) pouvant assurer l'interopérabilité des métadonnées documentaires sont souvent utilisées.

Le service de recherche des formats d'échange selon l'al. 1, let. c, permet de consulter les formats d'échange et les ensembles de données ou composants indépendants qui doivent être utilisés pour définir de nouveaux formats d'échange médicaux structurés applicables à l'échange de données dans le cadre du dossier électronique du patient. Avant de pouvoir utiliser les nouveaux formats d'échange médicaux dans le dossier électronique du patient, le DFI doit les avoir intégrés dans l'annexe 3 de l'ODEP-DFI.

Les identificateurs d'objet (*Object Identifier* [OID]) 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, p. 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.

L'*al. 2* précise que 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.

Dans le cadre de la constitution des services de recherche, l'OFSP définit des interfaces standard via lesquelles les communautés et les communautés de référence certifiées se procurent (services de recherche selon l'art. 38, al. 1, let. a à d) ou fournissent (art. 38, al. 1, let. a, ch. 2) des données. Les coûts afférents au raccordement à l'interface standard ou liés aux modifications requises pour exploiter ces interfaces, de même que les autres coûts en rapport avec les interfaces standard sont à la charge des communautés et communautés de référence.

Section 2 : Contenu

Art. 39 Service de recherche des communautés et communautés de référence certifiées

Pour permettre à l'OFSP de gérer les communautés et communautés de référence certifiées conformément à l'art. 32, al. 1, les organismes de certification doivent lui communiquer les informations énoncées à l'*al. 1*. Il s'agit du nom et des coordonnées des communautés et communautés de référence (*let. a*), des identifiants univoques (*Global Location Number* [GLN] ; *Object Identifier* [OID]), mais aussi des données nécessaires servant à authentifier en toute sécurité les points d'accès des communautés et

communautés de référence certifiées et les informations qu'elles livrent (*let. d* et *e*). 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. A cet effet, les communautés et les communautés de référence doivent acquérir des certificats électroniques valables (voir ch. 2.9.22 CTO) et présenter les données correspondantes à l'organisme de certification qui, après certification, les transmet à l'OFSP.

L'exactitude des données d'authentification (al. 1, let. d et e) revêt une importance toute particulière à l'égard de l'intégrité des données échangées. Pour cette raison, 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. 40 Service de recherche des institutions de santé et des professionnels de la santé

Ce service de recherche regroupe celui des institutions de santé (*Health Organisation Index* [HOI]) et celui des professionnels de la santé (*Health Professional Index* [HPI]) dans un système commun (*Health Provider Directory* [HPD]). Il permet de savoir quelles institutions de santé (p. ex. hôpitaux, pharmacies, cabinets médicaux, services d'aide et de soins à domicile, EMS) sont membres d'une communauté ou d'une communauté de référence certifiée et quels professionnels de la santé rattachés à des communautés et communautés de référence certifiées ont accès au dossier électronique du patient et à quelles institutions ils appartiennent. Selon l'art. 2, al. 1, la combinaison des données peut être utilisée à la fois pour accorder des droits d'accès à des professionnels de la santé distincts ou à des groupes de professionnels de la santé, p. ex. à l'ensemble des professionnels d'un service hospitalier.

Selon les droits de traitement des données, à définir dans le règlement correspondant, les organismes autorisés ont la possibilité d'enregistrer et de consulter des données dans le service de recherche des institutions de santé et des professionnels de la santé systématiquement dans des formats définis au moyen de l'interface standard mise à disposition par l'OFSP. Conformément à l'art. 9, al. 3, en relation avec l'art. 8, let. c, les communautés et communautés de référence certifiées doivent garantir que les données enregistrées dans le service de recherche des institutions de santé et des professionnels de la santé sont à jour.

Selon la *let. a*, les communautés et communautés de référence certifiées s'assurent que l'enregistrement des institutions et groupes de professionnels de la santé relevant de leur domaine de responsabilité contient les données visées aux ch. 1 à 3. Elles sont libres de faire figurer dans le service de recherche des groupes interinstitutionnels (p. ex. groupe interdisciplinaire d'experts [tumor board]) ou des petites sous-unités d'une organisation en tant que groupes de professionnels de la santé.

En vertu de la *let. b*, les communautés et communautés de référence certifiées s'assurent que l'enregistrement des professionnels de la santé des institutions relevant de leur responsabilité contient les données visées aux ch. 1 à 3.

Section 3 : Transfert de tâches à des tiers

Art. 41 Contrat de prestations

Conformément à l'art. 19 LDEP, la Confédération peut déléguer à des tiers l'exécution des tâches énoncées à l'art. 14, al. 1 et 2, LDEP. L'*al. 1* précise que la délégation de tâches se fonde sur un contrat de prestations.

L'*al. 2* énonce les éléments qui doivent impérativement figurer dans le contrat de prestations. Relevons, en particulier, les dispositions régissant la protection et la sécurité des données (*let. b*). D'une part, les

informations enregistrées dans les services de recherche peuvent en soi constituer des données sensibles (p. ex. données personnelles de professionnels de la santé dans le *service de recherche des institutions de santé et des professionnels de la santé*) ; d'autre part, une atteinte à l'intégrité de certaines données figurant dans les services de recherche peut entraîner des dommages secondaires (p. ex. accès non autorisé à des données médicales, code sémantique erroné). La disponibilité et l'efficacité des services de recherche font partie intégrante de la sécurité des données ; à ce titre, elles doivent également être réglementées dans les contrats de prestations.

Selon la *let. e,* les tiers mandatés sont tenus de rendre compte périodiquement de leur activité selon les critères définis dans le contrat de prestations.

L'*al. 3* énonce que les tiers mandatés informent l'OFSP sans délai de tout changement substantiel par rapport aux dispositions du contrat de prestations.

Art. 42 Emoluments

Partant de l'hypothèse que la Suisse comptera 20 communautés et communautés de référence, les émoluments à verser annuellement sont fixés à 20 000 francs. Cela permet un refinancement des coûts pour la constitution et l'exploitation des services de recherche sur une période de dix ans (*al. 1*).

L'*al. 2* énonce que, 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, s'appliquent.

Art. 43 Surveillance

La surveillance des tiers mandatés incombe à l'OFSP (*al. 1*).

La surveillance exercée par l'OFSP est précisée à l'*al. 2* : l'office vérifie tous les ans que les dispositions du contrat de prestations sont respectées (*let. a*) et se fait remettre périodiquement des comptes rendus (*let. b*). Dans des cas dûment fondés, il est aussi habilité à effectuer des contrôles sur place (*let. c*). Le respect des dispositions relatives à la protection et à la sécurité des données est particulièrement visé étant donné qu'une violation des obligations dans ce domaine peut avoir d'importantes conséquences en termes de sécurité des patients et de respect des droits de la personnalité.

Chapitre 8 : Dispositions finales

Art. 45 Entrée en vigueur

L'entrée en vigueur est prévue début 2017.