Ordonnance sur le dossier électronique du patient (ODEP)

Version du 22 mars 2016 pour l'audition

Le Conseil fédéral suisse,

vu la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP)[1],

arrête:

Chapitre 1 Niveaux de confidentialité et droits d'accès

Art. 1 Niveaux de confidentialité

[1] Le patient peut attribuer aux données de son dossier électronique du patient (dossier électronique) l'un des quatre niveaux de confidentialité suivants:

a. niveau de confidentialité «données utiles»;

b. niveau de confidentialité «données médicales»;

c. niveau de confidentialité «données sensibles»;

d. niveau de confidentialité «données secrètes».

[2] Par défaut, les nouvelles données enregistrées dans le dossier électronique du patient ont le niveau de confidentialité «données médicales».

[3] En dérogation à l'al. 2, le professionnel de la santé qui enregistre des données dans le dossier électronique peut leur attribuer le niveau de confidentialité «données sensibles».

Art. 2 Droits d'accès

[1] Le patient peut accorder à des professionnels de la santé ou à des groupes de professionnels de la santé les droits d'accès suivants:

a. «limité»: accès au niveau de confidentialité «données utiles»;

b. «normal»: accès aux niveaux de confidentialité «données utiles» et «données médicales»;

c. «étendu»: accès aux niveaux de confidentialité «données utiles», «données médicales» et «données sensibles».

[2] Si le patient ne fait aucune attribution explicite, le droit d'accès «normal» est valable par défaut.

[3] Les droits d'accès sont valables tant que le patient ne les a pas retirés.

[4] Le professionnel de la santé qui intègre un groupe reçoit les droits d'accès accordés à ce groupe. Ils lui sont retirés lorsqu'il quitte le groupe.

1 RS **816.11**

[5] En cas d'urgence médicale, les professionnels de la santé peuvent accéder aux données ayant les niveaux de confidentialité «données utiles» et «données médicales». Ils sont tenus de motiver cet accès au préalable.

Art. 3 Options du patient

Le patient peut:

a. choisir que les droits d'accès accordés en vertu de l'art. 2, al. 1, s'éteignent au bout de six mois;

b. limiter au niveau de confidentialité «données utiles», étendre au niveau de confidentialité «données sensibles» ou exclure totalement le droit d'accès à son dossier en cas d'urgence médicale;

c. choisir le niveau de confidentialité attribué aux nouvelles données enregistrées dans son dossier;

d. refuser tout accès à son dossier électronique à certains professionnels de la santé;

e. désactiver l'information prévue à l'art. 8, let. f;

f. choisir que les professionnels de la santé qui intègrent un groupe n'obtiennent pas automatiquement les droit d'accès accordés à ce groupe;

g. désigner un représentant;

h. habiliter des professionnels de la santé affiliés à sa communauté de référence à accorder en son nom des droits d'accès à d'autres professionnels de la santé; le professionnel de la santé habilité peut accorder tout au plus les droits d'accès qu'il possède.

Chapitre 2: Numéro d'identification du patient

Art. 4 Format du numéro d'identification du patient

[1] Le numéro d'identification du patient est un numéro à onze chiffres. Il se compose d'une clé de contrôle et d'un numéro à dix chiffres. Ce dernier peut être utilisé pour désigner une personne déterminée inscrite dans le registre de la banque de données d'identification de la centrale de compensation (CdC) visée à l'art. 71 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[2], en excluant toute possibilité de tirer des conclusions sur cette personne.

[2] La saisie manuelle du numéro d'identification du patient est autorisée uniquement si la clé de contrôle fait l'objet d'une vérification. Le Département fédéral de l'intérieur (DFI) fixe les prescriptions relatives à la création du numéro d'identification du patient et à la vérification de la clé de contrôle.

2 RS **831.10**

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

[1] Le numéro d'identification du patient est attribué par la CdC sur demande d'une communauté de référence.

[2] A cet effet, la communauté de référence communique à la CdC les données suivantes concernant le patient:

a. nom;

b. prénoms;

c. sexe;

d. date de naissance;

e. numéro d'assuré selon l'art. 50*c* LAVS[3].

[3] Si les données communiquées ne sont pas suffisantes pour attribuer un numéro d'identification, la CdC peut demander des données complémentaires à la communauté de référence.

Art. 6 Consultation du numéro d'identification du patient

Les communautés et communautés de référence peuvent faire une requête du numéro d'identification des patients auprès de la CdC par voie électronique.

Art. 7 Annulation

[1] Si le dossier électronique d'un patient est supprimé, son numéro d'identification est annulé dans la banque de données d'identification de la CdC.

[2] Un numéro d'identification annulé ne peut être attribué à nouveau.

Chapitre 3 Communautés et communautés de référence

Section 1 Communautés

Art. 8 Gestion

Les communautés sont tenues de gérer les institutions de santé, les professionnels de la santé et les groupes de professionnels de la santé qui leur sont affiliés. A cet effet, elles doivent en particulier:

a. régler les modalités d'entrée et de sortie;

b. identifier les professionnels de la santé;

c. assurer la mise à jour des données dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40;

3 RS **831.10**

d. s'assurer que les professionnels de la santé accèdent au dossier électronique du patient uniquement en utilisant un moyen d'identification valable émis par un éditeur certifié selon l'art. 30;

e. veiller à ce que chaque patient puisse identifier en tout temps la composition des groupes de professionnels de la santé;

f. informer les patients lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé.

Art. 9 Tenue et transfert des données

[1] Les communautés doivent garantir:

a. que les données enregistrées dans le dossier électronique du patient par les professionnels de la santé sont détruites au bout de dix ans;

b. que toutes les données du dossier électronique sont détruites en cas de suppression du dossier électronique en application de l'art. 20, al. 1;

c. que les données des dossiers électroniques sont enregistrées uniquement dans des lieux de stockage prévus exclusivement à cet effet.

[2] A la demande du patient, les communautés doivent:

a. s'abstenir d'enregistrer dans son dossier électronique des données déterminées le concernant;

b. s'assurer que les données visées à l'al. 1 restent accessibles pendant dix années supplémentaires;

c. détruire dans son dossier électronique des données déterminées le concernant.

[3] Le DFI fixe les autres prescriptions relatives à la gestion et au transfert des données du dossier électronique. Il règle en particulier:

a. l'application des art. 1 et 2, al. 5;

b. les métadonnées à utiliser;

c. les formats d'échange à utiliser;

d. les profils d'intégration à utiliser;

e. les prescriptions relatives aux données historisées.

[4] Le DFI peut décider de faire publier les prescriptions visées à l'al. 3 dans la langue d'origine et de renoncer à les faire traduire dans les autres langues officielles.

[5] L'Office fédéral de la santé publique (OFSP) peut adapter les prescriptions visées à l'al. 3 en fonction des progrès techniques.

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

Le DFI fixe les exigences applicables au portail d'accès destiné aux professionnels de la santé.

Art. 11 Protection et sécurité des données

[1] Les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données qui comprend en particulier les éléments suivants:

a. la désignation d'un responsable de la protection et de la sécurité des données;
b. un système de détection et de gestion des incidents de sécurité;
c. un registre des lieux de stockage des documents;
d. un registre des systèmes primaires liés aux communautés;
e. les prescriptions relatives à la protection et à la sécurité des données imposées aux institutions de santé affiliées et à leurs professionnels de la santé;
f. les exigences relatives à la protection et à la sécurité des données imposées au personnel et aux tiers.

[2] Les communautés sont tenues de signaler à l'organisme de certification et à l'OFSP les incidents survenus dans le système de gestion de la protection et de la sécurité des données ayant un impact en termes de sécurité.

[3] Le DFI fixe les exigences applicables à la protection et à la sécurité des données.

[4] Les dispositifs de stockage des données doivent être situés en Suisse et régis par le droit suisse.

Art. 12 Service d'assistance pour les professionnels de la santé

Les communautés doivent désigner un service d'assistance destiné aux professionnels de la santé afin de les aider dans l'utilisation du dossier électronique.

Section 2 Communautés de référence

Art. 13 Exigences supplémentaires à l'égard des communautés de référence

En plus des prescriptions prévues dans la section 1, les communautés de référence doivent respecter les prescriptions énoncées dans la présente section.

Art. 14 Information du patient

[1] Avant d'ouvrir un dossier électronique, la communauté de référence est tenue d'informer le patient en particulier sur les points suivants:

a. le but du dossier électronique;
b. les principes généraux du traitement des données;
c. les conséquences du consentement et la possibilité de le révoquer;
d. l'attribution des droits d'accès.

[2] Elle doit recommander au patient des mesures de protection et de sécurité des données.

Art. 15 Consentement

La communauté de référence doit obtenir le consentement du patient à la tenue d'un dossier électronique. Le consentement doit porter la signature du patient.

Art. 16 Gestion

[1] Les communautés de référence doivent:

a. régler les modalités d'entrée et de sortie des patients;

b. identifier les patients;

c. s'assurer que les patients et leurs représentants accèdent au dossier électronique uniquement en utilisant un moyen d'identification valable émis par un éditeur certifié selon l'art. 30;

d. demander les numéros d'identification des patients conformément aux art. 5 et 6;

e. prévoir des procédures régissant le changement de communauté de référence.

[2] Les communautés de référence doivent veiller à l'application de l'art. 2, al. 1 à 4, et de l'art. 3.

Art. 17 Portail d'accès pour les patients

Le DFI fixe les exigences applicables au portail d'accès destiné aux patients.

Art. 18 Disponibilité des données enregistrées par les patients

Le DFI fixe les exigences applicables à l'utilisation des données enregistrées par les patients via le portail d'accès.

Art. 19 Service d'assistance pour les patients

Les communautés de référence doivent désigner un service d'assistance destiné aux patients afin de les aider dans l'utilisation de leur dossier électronique.

Art. 20 Suppression du dossier électronique **du patient**

[1] La communauté de référence supprime le dossier électronique du patient dans les cas suivants:

a. révocation du consentement du patient à la tenue de son dossier électronique;

b. personne n'a accédé au dossier électronique du patient durant dix ans, ou

c. décès du patient.

[2] A cet effet, la communauté de référence doit supprimer tous les droits d'accès au dossier électronique du patient correspondant et:

a. en cas de suppression:

1. informer de la suppression toutes les communautés ainsi que la CdC dans un délai approprié,
2. conserver la révocation de consentement durant dix ans;

b. en cas d'inutilisation selon l'al. 1, let. b informer le patient de la suppression de son dossier électronique trois mois avant d'y procéder.

Section 3 Données à fournir pour l'évaluation

Art. 21

[1] Les communautés et communautés de référence sont tenues de mettre régulièrement des données à la disposition de l'OFSP pour l'évaluation selon l'art. 18 LDEP.

[2] Le DFI fixe les données à fournir.

Chapitre 4 Moyens d'identification

Art. 22 Exigences applicables au moyen d'identification

Le moyen d'identification doit:

a. satisfaire au niveau de confiance 3 de la norme ISO/IEC 29115:2013(E)[4];

b. être conçus de façon à pouvoir être utilisés uniquement par la personne autorisée;

c. utiliser une procédure d'authentification conforme aux progrès techniques comportant au moins deux facteurs d'authentification, et

d. avoir une durée de validité d'au maximum dix ans.

Art. 23 Vérification d'identité

[1] L'éditeur est tenu de vérifier l'identité de la personne qui demande un moyen d'identification. Pour établir son identité, le demandeur doit présenter un document d'identité conforme à la loi du 22 juin 2001 sur les documents d'identité[5] ou un titre de séjour conforme aux art. 41 à 41*b* de la loi fédérale du 16 décembre 2005 sur les étrangers[6] ou encore déposer par voie électronique une demande sur laquelle est apposée une signature électronique qualifiée selon la loi fédérale du 19 décembre 2003 sur la signature électronique[7].

4 Cette norme peut être achetée auprès de l'Association suisse de normalisation (snv.ch) ou consultée gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne
5 RS **143.1**
6 RS **142.20**
7 RS **943.03**

[2] Si le moyen d'identification demandé est destiné à authentifier un professionnel de la santé, il faut en outre vérifier si ce dernier a la qualité de professionnel de la santé au sens de l'art. 2, let. b, LDEP.

[3] La vérification de l'identité des demandeurs visée à l'al. 1 et la vérification de la qualité de professionnel de la santé visée à l'al. 2 peuvent être déléguées à des tiers.

Art. 24 Données du moyen d'identification

[1] L'éditeur du moyen d'identification saisit les données suivantes concernant le demandeur en se référant à la pièce d'identité fournie:

a. nom;

b. prénoms;

c. sexe;

d. date de naissance;

e. numéro de la pièce d'identité fournie conformément à l'art. 23, al. 1.

[2] S'agissant d'un professionnel de la santé, il peut en outre saisir un numéro d'identification (GLN[8]).

[3] Il peut transmettre les données visées aux al. 1 et 2 aux portails d'accès à des fins d'identification.

[4] Il informe le demandeur des dispositions de sécurité à respecter lors de l'utilisation du moyen d'identification.

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

[1] Le moyen d'identification peut être renouvelé avant l'expiration de sa durée de validité.

[2] Lors du renouvellement du moyen d'identification, l'éditeur vérifie l'identité du demandeur conformément à l'art. 23.

Art. 26 Blocage du moyen d'identification

Le titulaire du moyen d'identification peut bloquer celui-ci irrévocablement à tout moment.

8 *Global Location Number*

Chapitre 5 Accréditation

Art. 27 Critères

[1] L'accréditation est régie par l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation (OAccD)[9] et elle est conforme à la norme ISO/IEC 27006:2015[10], sauf si la présente ordonnance en dispose autrement.

[2] Des accréditations séparées sont requises pour la certification:

a. des communautés et des communautés de référence, d'une part;

b. des éditeurs de moyens d'identification, d'autre part.

[3] L'organisme de certification doit remplir les critères de l'OAccD et, de surcroît, disposer d'une organisation et d'une procédure de contrôle déterminées. Les points suivants doivent notamment être réglés:

a. les critères d'évaluation ou d'essai utilisés pour vérifier le respect des critères de certification;

b. le déroulement de la procédure, spécialement la procédure en cas de constat d'irrégularités;

c. l'utilisation du système de certification mis à disposition par l'OFSP pour examiner le transfert des données des communautés et communautés de référence.

[4] Le DFI fixe les exigences minimales applicables à la qualification du personnel qui réalise les certifications.

Art. 28 Procédure d'accréditation

Le Service d'accréditation suisse fait appel à l'OFSP pour la procédure d'accréditation ainsi que pour le contrôle, la suspension ou le retrait d'une accréditation.

Chapitre 6 Certification

Section 1 Critères de certification

Art. 29 Communautés et communautés de référence

[1] La procédure de certification a pour but de vérifier si les communautés remplissent les critères de certification énoncés aux art. 8 à 12 et si les communautés de référence remplissent les critères de certification énoncés aux art. 8 à 20.

[2] Le DFI règle les modalités des critères de certification.

[3] L'OFSP adapte les critères de certification en fonction des progrès techniques.

9 RS **946.512**

10 Cette norme peut être achetée auprès de l'Association suisse de normalisation (snv.ch) ou consultée gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne

4 Les milieux intéressés sont consultés au sujet des modalités visées à l'al. 2 et des adaptations visées à l'al. 3.

Art. 30 Editeurs de moyens d'identification

1 Les éditeurs de moyens d'identification doivent:

a. être en mesure d'émettre et d'administrer des moyens d'identification conformément exigences établies aux art. 22 à 26;

b. s'assurer que leur personnel possède les connaissances techniques, l'expérience et les qualifications requises;

c. utiliser des systèmes et des produits informatiques fiables et qui sont exploités de manière sûre;

d. garantir la protection et la sécurité des données par des mesures organisationnelles et techniques appropriées et assurer les contrôles correspondants.

2 Le DFI édicte des prescriptions relatives à la protection des moyens d'identification et à la procédure d'authentification de ces moyens. Elles sont conformes à la norme ISO/IEC 15408:2009[11] et correspondent au niveau d'évaluation 2.

3 Le DFI règle les modalités des critères de certification. L'OFSP peut édicter des recommandations à ce sujet.

4 L'OFSP adapte les critères de certification en fonction des progrès techniques.

5 Les milieux intéressés sont consultés au sujet des modalités visées à l'al. 3 et des adaptations visées à l'al. 4.

Section 3 Procédure de certification

Art. 31 Déroulement

1 L'organisme de certification procède à un pré-audit pour vérifier si le demandeur est préparé à la procédure de contrôle; ce faisant, il inventorie et évalue la documentation du demandeur.

2 Dans l'audit de certification qui suit, il vérifie l'efficacité des mesures prises par le demandeur sur la base de ses critères d'évaluation ou d'essai

3 Il délivre le certificat si le pré-audit et l'audit de certification montrent que la communauté, la communauté de référence ou l'éditeur de moyens d'identification remplit les exigences énoncées respectivement aux art. 8 à 12, 8 à 20 et 22 à 26.

11 Cette norme peut être achetée auprès de l'Association suisse de normalisation (snv.ch) ou consultée gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne

Art. 32 Déclaration à l'OFSP

[1] L'organisme de certification déclare à l'OFSP dans un délai approprié tous les cas de certification, de recertification, de suspension ou de retrait de certificat et met à disposition les données requises pour la saisie dans le service de recherche des communautés et communautés de référence certifiées visé à l'art. 39.

[2] L'OFSP publie un registre des certificats délivrés.

Art. 33 Surveillance

[1] L'organisme de certification est tenu de vérifier annuellement si les critères de certification sont toujours remplis.

[2] Si, dans le cadre de la surveillance, l'organisme de certification constate des écarts substantiels par rapport aux critères de certification, par exemple concernant le respect de conditions ou de charges, il en informe l'OFSP.

Art. 34 Durée de validité

Le certificat est établi pour une durée de trois ans.

Art. 35 Déclaration d'adaptations techniques ou organisationnelles substantielles

[1] Les communautés, les communautés de référence et les éditeurs de moyens d'identification sont tenus de déclarer à l'organisme de certification des adaptations techniques ou organisationnelles substantielles.

[2] L'organisme de certification décide si les adaptations signalées sont examinées dans le cadre de la surveillance, d'une recertification ordinaire ou d'une recertification extraordinaire.

Art. 36 Clause de sauvegarde

En cas de grave mise en danger de la protection ou de la sécurité des données du dossier électronique du patient, l'OFSP peut:

a. refuser provisoirement à des communautés et communautés de référence l'accès au dossier électronique du patient;

b. interdire l'utilisation de certains moyens d'identification;

c. ordonner une recertification extraordinaire.

Section 4 Sanctions

Art. 37

[1] L'organisme de certification peut suspendre ou retirer un certificat, notamment s'il constate des défaillances graves dans le cadre de la surveillance (art. 33). Une défaillance grave est constatée en particulier lorsque:

a. des critères de certification substantiels ne sont plus remplis, ou

b. un certificat est utilisé fallacieusement ou abusivement.

[2] En cas de litige concernant une suspension ou un retrait, l'évaluation et la procédure sont régies par les dispositions du droit civil applicables aux relations contractuelles entre l'organisme de certification et la communauté, la communauté de référence ou l'éditeur de moyens d'identification titulaire du certificat concerné.

[3] En cas de suspicion fondée qu'une communauté, une communauté de référence ou un éditeur de moyens d'identification titulaire d'un certificat ne remplit pas les critères de certification, l'OFSP peut:

a. ordonner que l'organisme de certification procède à un examen;

b. suspendre la validité ducertificat;

c. retirer le certificat.

Chapitre 7 Services de recherche de données

Section 1 Généralités

Art. 38

[1] Les services de recherche contiennent:

a. les données de référence concernant:
   1. les communautés et les communautés de référence,
   2. les institutions de santé et leurs professionnels de la santé autorisés à traiter les données du dossier électronique du patient;

b. les métadonnées (art. 9, al. 3, let. b);

c. les formats d'échange (art. 9, al. 3, let. c);

d. les identificateurs d'objet (OID) enregistrés pour le dossier électronique du patient.

[2] L'OFSP pourvoit à la constitution, à l'exploitation et au développement des services de recherche.

Section 2: Contenu

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

[1] Le service de recherche des communautés et communautés de référence certifiées contient les données suivantes les concernant:

a. désignation;

b. identifiant univoque (GLN);

c. identificateur d'objet (OID);

d. certificat assurant une authentification sûre par rapport aux autres communautés et communautés de référence;

e. adresse internet du point d'accès.

[2] L'OFSP vérifie et saisit ces données dans le service de recherche des communautés et communautés de référence.

Art. 40 Service de recherche des institutions de santé et des professionnels de la santé

Les communautés et communautés de référence saisissent dans le service de recherche des institutions de santé et des professionnels de la santé les données suivantes:

a. concernant les institutions de santé et les groupes de professionnels de la santé:
   1. désignation et adresse,
   2. GLN,
   3. OID;

b. concernant les professionnels de la santé:
   1. données personnelles,
   2. GLN,
   3. désignation et adresse de l'institution de santé dans laquelle ils travaillent ou du groupe de professionnels de la santé auquel ils appartiennent.

Section 3 Transfert de tâches à des tiers

Art. 41 Contrat de prestations

[1] L'OFSP peut déléguer à des tiers la constitution et l'exploitation des services de recherche moyennant un contrat de prestations.

[2] Le contrat de prestations règle en particulier:

a. les objectifs à atteindre;

b. les exigences de protection et de sécurité des données;

c. l'étendue et les modalités de l'indemnisation par la Confédération;

d. les conséquences de l'inexécution du contrat;

e. les modalités de compte rendu périodique.

3 Le tiers à qui des tâches ont été déléguées est tenu d'informer l'OFSP sans délai de tout changement substantiel.

Art. 42 Emoluments

1 Les communautés et communautés de référence s'acquittent d'un émolument forfaitaire annuel de 13 500 francs.

2 Pour le reste, les dispositions de l'ordonnance générale sur les émoluments du 8 septembre 2004[12] sont applicables.

Art. 43 Surveillance

1 La surveillance des tiers auxquels l'exploitation de services de recherche a été déléguée incombe à l'OFSP.

2 La surveillance comprend en particulier:

a. la vérification périodique du respect des prescriptions visées à l'art. 41, al. 2;

b. l'obtention de comptes rendus périodiques;

c. le contrôle sur place du respect du contrat de prestations.

Chapitre 8 Dispositions finales

Art. 44 Abrogation et modification d'autres actes

Art. 45 Entrée en vigueur

La présente ordonnance entre en vigueur le ....

12 RS **172.041.1**