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 sur les résultats de l'audition

Ordonnance sur le dossier électronique du patient (ODEP)

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

22 mars 2017

Table des matières

1. Contexte

La loi fédérale sur le dossier électronique du patient (LDEP ; RS 816.1) a été adoptée par le Parlement le 19 juin 2015. Il est prévu qu'elle entre en vigueur en 2017. Le Département fédéral de l'intérieur (DFI) a ouvert le 22 mars 2016 la procédure d'audition relative au droit d'exécution de la LDEP. L'audition a duré jusqu'au 29 juin 2016 et portait concrètement sur trois textes d'ordonnance : 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). L'ODEP règle les niveaux de confidentialité et les droits d'accès (chapitre 1), les prescriptions relatives à l'attribution et à la gestion des numéros d'identification du patient (chapitre 2), les exigences à l'égard des communautés et des communautés de référence (conditions de certification ; chapitre 3), les moyens d'identification (chapitre 4), la procédure d'accréditation (chapitre 5), la certification (chapitre 6) et les services de recherche de données (chapitre 7). L'ODEP-DFI concrétise l'ODEP. Elle règle tous les aspects techniques du dossier électronique du patient (DEP) et comprend neuf articles et huit annexes. L'OFDEP concrétise les prescriptions énoncées aux art. 20 à 23 LDEP, qui règlent les aides financières au niveau de la loi.

Le présent rapport contient exclusivement les réponses aux auditions sur l'ODEP et l'ODEP-DFI. Les résultats de l'audition sur l'OFDEP sont résumés dans un rapport à part.

2. Procédure d'audition et concept d'évaluation

Ce chapitre présente, d'une part, un tableau synoptique indiquant le nombre de prises de position reçues ainsi que leurs auteurs et, d'autre part, une description des principes d'évaluation pour le chapitre 3 (prises de position sur les différentes dispositions de l'ODEP et de l'ODEP-DFI).

2.1 Procédure d'audition

Tableau 1 : Aperçu des réponses reçues

Catégorie	Cantons, CDS	Partis	Associations faîtières de l'économie	Autres Organisations	Participants non officiels	**Total**
Nombre / Catégorie	27	3	3	30*	74**	137

Dans leurs réponses, *curafutura, l'ASA et la **VKZS ont renoncé expressément à prendre position

2.2 Principes d'évaluation

Les prises de position sont très nombreuses et très diverses.
Pour donner un tableau aussi complet que possible, elles ont été retranscrites sous forme résumée de la façon la plus exacte possible dans le présent rapport. Les prises de position détaillées reçues dans le cadre de la consultation peuvent être consultées sur :

https://www.bag.admin.ch/bag/fr/home/themen/strategien-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/bundesgesetz-elektronische-patientendossier/anhoerung-ausfuehrungsrechts-bundesgesetz-elektronische-patientendossier.html

Les prises de position concernant les différentes dispositions de l'OFDEP sont présentées au chapitre 3.

3. Prises de position sur les différentes dispositions de l'ODEP/ODEP-DFI

Ce chapitre présente les prises de position sur les différents articles du projet. Lorsque cela a été possible, les propositions de formulation ont été reprises telles quelles. Pour une meilleure lisibilité, les compléments proposés au texte législatif existant sont soulignés. Les souhaits généraux de modification, les demandes de suppression et les propositions de textes législatifs supplémentaires sont également mentionnés dans le texte, sans être spécialement mis en évidence.

3.1 ODEP

3.1.1 Chapitre 1 : Niveaux de confidentialité et droits d'accès

La *CCM*, *BüAeV*, *GAeSO*, *KAeG SG* et *HIN* estiment qu'il serait judicieux de compléter le chapitre 1 « Niveaux de confidentialité et droits d'accès » d'une disposition supplémentaire. Ils proposent un nouvel article intitulé « Saisie par les patients de leurs propres données » et formulé comme suit : « Les données que les patients saisissent eux-mêmes sont enregistrées à part dans le dossier électronique du patient. Par défaut, les nouvelles données enregistrées dans le dossier électronique du patient ont le niveau de confidentialité « données sensibles » et un droit d'accès « étendu ». La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* demandent en outre que le chapitre 1 soit renommé « Niveaux de confidentialité et accès au dossier électronique du patient ».

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».

La *SSIM* recommande la nomination d'un responsable de la protection des données et propose d'appliquer les dispositions de la loi sur la protection des données, ajoutant qu'il est important d'éviter une surréglementation. La *FMH* fait remarquer que ce sont les médecins qui suggèreront aux patients d'établir un dossier électronique et qui les informeront et les conseilleront à ce sujet, ce travail méritant d'être indemnisé. La *FMH* observe en outre à ce propos que le dossier électronique du patient doit contribuer à simplifier la communication entre patients et professionnels de la santé au lieu d'inciter à dresser des barrières. eHealth ainsi que le dossier électronique du patient sont censés accompagner les patients dans leur parcours médical, accélérer l'échange d'informations, renforcer la sécurité des patients et améliorer la cohésion entre ces derniers et les professionnels de la santé. Concrètement, on demande la création de centres pour l'établissement de dossiers électroniques du patient dont la fonction soit également d'informer les patients.

Al. 1 : Sept participants[1] estiment au vu du droit de la protection des données qu'il ne suffit pas de mentionner les types de données uniquement dans le rapport explicatif, raison pour laquelle ils préconisent d'introduire dans l'ordonnance des exemples illustrant les niveaux de confidentialité correspondant à chaque type de données. Ils font en outre une proposition concrète d'énoncé pour un alinéa complémentaire dans l'art. 1. Dans le même esprit, *FSAS*, *SWOR*, *Physioswiss* et l'*ASI* font remarquer que les informations sur les niveaux de confidentialité présentés dans le rapport explicatif sont nécessaires à la compréhension du classement, tant par les professionnels de la santé que par les patients.

[1] KDSBSON, DSBAG, privatim, BE, ZG, FR, AG

TG souhaite également une brève explication des niveaux de confidentialité. La *FMH* demande une désignation et une définition précises des niveaux de confidentialité, observant que les désignations actuelles posent des problèmes de terminologie et de traduction. *TI* souhaite une définition précise des types de données, soulignant que les exemples figurant dans le rapport explicatif ne sont pas exhaustifs et que les définitions devraient être introduites dans le texte de l'ordonnance. Six autres cantons[2] insistent eux aussi sur la nécessité de clarifier la terminologie et les différents exemples.

FSAS, *SWOR*, *Physioswiss* et l'*ASI* jugent raisonnable la proposition de ramener à quatre le nombre de niveaux de confidentialité, *H+* et *senesuisse* saluent également cette limitation. *K3* et *VZK* redoutent que les niveaux de confidentialité, les rôles et les droits d'accès ne soient trop compliqués pour le citoyen ordinaire et recommandent par conséquent de simplifier les droits d'accès et les niveaux de confidentialité. Six cantons[3] expriment le même souhait, évoquant le risque de décourager les patients. Six participants[4] jugent inappropriée la distinction entre « données utiles » et « données médicales », vu que ces deux termes n'expriment pas des degrés de confidentialité. Ainsi, une limitation à trois niveaux de confidentialité serait plus conforme à l'usage international. Ils demandent par conséquent l'adaptation du texte aux trois niveaux « normal » (données consultables par tous les professionnels de la santé), « restricted » (données sensibles ; consultables uniquement par des professionnels de la santé au droit d'accès étendu) et « very restricted » (données secrètes ; consultables uniquement par les patients et leurs représentants éventuels). *Tessaris* préconise également une limitation à trois niveaux de confidentialité, désignés respectivement par « open = free access », « limited access » et « secret = excluded access ». *ZH* se prononce également pour une renonciation à la distinction entre données utiles et données médicales. *STSAG* propose quant à elle une réduction à trois niveaux désignés par « utile/administratif », « médical » et « secret ». *ÄTG* et *HÄ CH* recommandent également d'examiner la possibilité de réduire de quatre à trois le nombre de niveaux de confidentialité. Ils précisent que toutes les données médicales devraient d'ores et déjà être classées comme sensibles, de sorte que les deux catégories b et c n'en feraient plus qu'une. *TI* est également d'avis que les données médicales doivent toujours être considérées comme des données sensibles et propose de les renommer « données sensibles », tandis que les « données sensibles » actuelles seraient renommées « données stigmatisantes (ou particulièrement sensibles) ». Six autres cantons[5] rappellent qu'il faut distinguer les catégories de données (administratives, utiles, médicales) et les niveaux de confidentialité (normal, stigmatisant, secret). De plus, en vertu de l'art. 3, let. c de la loi fédérale sur la protection des données, la catégorie « données sensibles » inclut entre autres les données de santé personnelles. La distinction entre données sensibles et données médicales dans le projet d'ordonnance est donc incompréhensible et infondée. Le texte doit être modifié en conséquence. Il doit en outre préciser ce que l'on entend par « données administratives » et mentionner qu'elles sont accessibles à tous les professionnels de la santé.

Tessaris précise que les « données médicales » correspondent au niveau « open – free access » et propose de retenir uniquement les niveaux de confidentialité « données médicales » (nouveau : lettre a), « données sensibles » (nouveau : lettre b) et « données secrètes » (nouveau : lettre c). *VGIch* et *SUVA* signalent que le niveau de confidentialité « données secrètes » est contraire aux objectifs du dossier électronique du patient et que la lettre d doit par conséquent être supprimée. *Senesuisse* et *H+* demandent que l'on vérifie la nécessité du niveau 4 trois à cinq ans env. après l'introduction du DEP. Alors que *senesuisse* fait remarquer que ce niveau ne contribue en rien aux objectifs de la Stratégie Cybersanté, *H+* observe que dans l'intérêt des patients, la préservation de la confidentialité et la protection des données doivent peser davantage que le libre échange des données. *IG eHealth* et *PH CH* déclarent avoir soutenu les cinq niveaux de confidentialité recommandés par eHealth Suisse et constatent que la suppression de la catégorie « données administratives » ouvre une faille dans la réglementation des accès aux informations dignes de protection dans le MID. *IG eHealth* précise néanmoins être en mesure de soutenir le choix des quatre niveaux de confidentialité, pour autant que la gestion des données sensibles du MID soit réglementée. *IG eHealth* et *PH CH* proposent que l'al. 1 soit complété

2 GE, VS, VD, JU, FR, NE
3 GE, VS, VD, JU, FR, NE
4 HIN, BINT, Integic, HL7, IHE, LUKS
5 GE, VS, VD, JU, FR, NE

d'une lettre supplémentaire destinée à réglementer l'accès aux données administratives sensibles. *TI* souhaite que l'on ajoute le niveau de confidentialité « données administratives » en précisant que le droit d'accès à ces données doit également être défini dans l'art. 2, al. 1.

IG eHealth, *PH CH*, *ZG* et *La Poste* demandent que la notion de « données » soit définie une fois pour toutes. *La Poste* conseille en outre de constituer un glossaire des termes et définitions. *NE* insiste également sur l'importance de définitions claires, notamment pour la sécurité juridique. De l'avis de sept participants[6], il importe de faire en sorte que des autorisations ne puissent être acquises au-delà du niveau du document. *IG eHealth* et *PH CH* proposent le nouvel énoncé suivant pour l'al. 1 : « […] attribuer aux données résumées dans un document l'un des trois […] ». *Integic* se prononce également pour une explication de la notion de « données » et renvoie à l'Annexe 3 de l'ODEP-DFI : Métadonnées, chap. 1.12 « Type de document ». *VGIch* souhaite que la notion de « données médicales » soit précisée ou que l'on choisisse un terme moins restrictif. *TI* demande que les définitions des données et documents relatives aux différents niveaux de confidentialité soient ajoutées directement au texte de l'ODEP.

Al. 2 : *KDSBSON* relève que de manière générale, les mesures de protection et de sécurité des données devraient être non pas recommandées, mais prédéfinies à l'aide de paramétrages techniques appropriés. Ce principe de « privacy by default » doit conduire à une définition plus restrictive des configurations de base. Concrètement, l'art. 1, al. 2 devrait stipuler l'attribution du niveau de confidentialité « données sensibles » aux nouvelles données, et dans l'art. 2, al. 2, les droits d'accès devraient être définis comme « restreints » par défaut. *DSBAG* fait les mêmes propositions et demande qu'elles soient examinées. De l'avis de *privatim*, le droit de la protection des données s'accommode mal du fait que (presque) « tous aient accès à tout » sans intervention des patients. Il faut parvenir à un accès différencié selon le principe de « privacy by default ». Ils proposent deux solutions concrètes, qui incluent elles aussi l'attribution aux nouvelles données du niveau de confidentialité « données sensibles ». *Integic* et *BINT* estiment également judicieux d'attribuer par défaut le niveau de confidentialité « restricted » aux nouvelles données. Ils proposent en outre que le patient ait l'option de confier au professionnel de la santé le soin de fixer le niveau de confidentialité. À défaut, ce niveau sera également défini comme « restricted ». *TG* indique que le niveau de confidentialité « données sensibles » ou « données secrètes » devrait être sélectionné comme paramètre par défaut. La *FMH* recommande de manière générale le choix d'un paramètre par défaut plus conforme aux besoins de la majorité des patients. *Tessaris* propose l'attribution du niveau « données sensibles » aux données nouvellement introduites dans le dossier électronique du patient sans mention d'un niveau de confidentialité.

Le thème de la « privacy by default » conduit *BS* à se demander s'il est possible de renoncer entièrement à une définition par défaut du niveau de confidentialité des données au moment de leur introduction. Selon eux, une attribution différenciée du niveau de confidentialité par le professionnel de la santé et l'établissement de soins, ainsi qu'un abandon de l'attribution générale du niveau « données sensibles », permettent d'éviter – ce qui serait souhaitable – que de nombreux professionnels de la santé titulaires d'un droit d'accès « normal » consultent des dossiers électroniques de patients sans y trouver des données. *FR* signale que le principe de « privacy by default » est en conflit avec les objectifs du dossier électronique du patient et qu'une pesée des intérêts est donc nécessaire. Dix participants[7] rejettent le principe de « privacy by default », qu'ils jugent inadapté aux objectifs. *SO* dit en outre partir du principe que les informations prévues et adéquates selon l'art. 3 LDEP incluent le niveau de confidentialité par défaut (ainsi que les droits d'accès par défaut visés à l'art. 2 al. 2 ODEP). *AR* déclare ne pas rejeter le principe de « privacy by default ». Dix participants[8] sont d'avis qu'il faut partir de l'hypothèse qu'une majorité de patients ne souhaitent pas gérer eux-mêmes les niveaux de confidentialité et que les professionnels de la santé doivent donc avoir l'option d'attribuer le niveau « données utiles ». Neuf participants[9] pensent en outre qu'il vaudrait la peine d'examiner les possibilités d'attribuer automatiquement, au moment de l'envoi, un niveau de confidentialité par défaut différent à chaque document sur la

6 IG eHealth, PH CH, K3, VZK, ZG, La Poste, SMCF
7 CDS, BL, GL, LU, OW, UR, SZ, NW, SO, SH
8 CDS, BL, GL, LU, OW, UR, SZ, NW, ZG, SH
9 CDS, BL, GL, LU, OW, UR, SZ, NW, SH

base de ses métadonnées. *HÄ CH* et *ÄTG* considèrent comme problématique la possibilité d'attribuer par défaut le niveau de confidentialité « données sensibles » aux nouvelles données, telle que prévue dans le paragraphe 2 du rapport explicatif. Elle pourrait en effet priver involontairement les professionnels de la santé d'une grande partie des informations médicales, de sorte que ce niveau de confidentialité ne doit pouvoir être attribué que manuellement dans des cas bien précis. *Santésuisse* fait remarquer que la disposition qui permet au patient d'attribuer le niveau de confidentialité qu'il veut à tout type de document peut créer la confusion. L'attribution d'un niveau de confidentialité sans droit d'accès à des informations importantes pourrait conduire à des situations médicales critiques. De telles situations pourraient être évitées par le signalement d'éventuelles informations supplémentaires à tous les professionnels de la santé autorisés à les consulter. *FR* propose en outre l'ajout d'un alinéa pour informer les patients sur les niveaux de confidentialité et assurer qu'ils en comprennent la signification.

La Poste et *IG eHealth* craignent que le mécanisme décrit à l'al. 2 ne soit pas applicable en la forme. Chaque document doit être préalablement examiné avant que l'on puisse lui attribuer un niveau de confidentialité. *La Poste* ajoute que les professionnels de la santé peuvent enregistrer localement en quelques secondes des documents nouvellement publiés et qu'un patient opérant un processus manuel n'est pas en mesure de l'empêcher. Le but doit donc être que les professionnels de la santé sachent d'avance le niveau de confidentialité que doivent avoir les documents. *La Poste* et *IG eHealth* soumettent la proposition concrète suivante pour l'énoncé de l'al. 2 : « Sauf instructions contraires du patient, les documents publiés par les professionnels de la santé possèdent le niveau de confidentialité "données médicales" ». *PH CH* propose un autre énoncé : « Sauf instructions contraires du professionnel de la santé, les nouvelles données sont enregistrées avec le niveau de confidentialité "données médicales" ».

VAKA demande que les patients puissent choisir un paramétrage leur permettant de définir le niveau « données accessibles normalement » pour tous les professionnels de la santé enregistrés et d'attribuer par défaut le niveau de confidentialité « données médicales » à tous les nouveaux documents. Il faut insister sur le fait que les personnes qui souhaitent garder le contrôle détaillé de leurs droits d'accès peuvent continuer à le faire. L'une des mesures de sécurité concevables de l'avis de *VAKA* serait que les patients reçoivent périodiquement une liste des personnes qui ont consulté leur dossier électronique. *Tessaris* demande que le patient puisse définir la nature et l'ampleur des nouvelles données saisies dans le dossier électronique du patient à la fin de son traitement. La saisie des données du traitement dans le dossier électronique du patient doit en outre faire l'objet d'un accord écrit à signer par le patient. Les données saisies doivent être codées à l'aide des meilleures techniques actuelles. De plus, on doit pouvoir demander la reprise des données de traitements précédents dans le dossier électronique du patient. *ZH* fait remarquer qu'aucune réglementation n'est prévue pour les cas d'incapacité de discernement. Il faut introduire des dispositions réglementant la relation avec les personnes incapables de discernement dans le droit d'exécution ou, à tout le moins, ajouter des réflexions à ce sujet dans le rapport explicatif. Il importe également de réglementer la gestion des dossiers électroniques de patients adolescents ou jeunes adultes, notamment le moment et les modalités de la transmission du contrôle du dossier au patient par ses parents.

Al. 3 : *Integic*, *HL7* et *IHE* reprochent à cette disposition de se substituer à une décision du patient. Ils demandent, à l'instar de *Bleuer* et de *Tessaris*, la suppression pure et simple de l'al. 3. À défaut, *Integic* exige un addendum stipulant l'obligation de porter de nouvelles données « very restricted » à la connaissance du patient. L'*OSP* et *FRC* font valoir qu'il est important de recueillir l'accord du patient. *OSP* propose l'énoncé suivant : « […] dans le dossier électronique du patient peut, avec l'accord du patient, leur attribuer […] » et *FRC* l'énoncé suivant : « […] le dossier électronique du patient peut, avec l'accord du patient, leur attribuer le niveau de confidentialité "données sensibles" ». Un énoncé similaire est proposé par *pharmaSuisse* : « […] dans le dossier électronique du patient peut, sur mandat d'un patient, leur attribuer […] ». Cela peut par ex. se produire dans le cadre du consentement à la tenue d'un dossier électronique du patient conformément à l'art. 15. *K3* et *VZK* soulignent l'impossibilité qu'un seul professionnel de la santé soit chargé de l'enregistrement des données et documents d'un patient dans un hôpital et demandent donc que l'al. 2 soit complété comme suit : « […] le professionnel de la santé ou

le groupe de professionnels de la santé qui enregistre des données dans […] ». *PKS* relève qu'un hôpital doit être en mesure de faire attribuer automatiquement des niveaux de confidentialité à des documents par une application utilisée par plusieurs professionnels de la santé et leurs auxiliaires. *PKS* et *UDC* demandent la suppression de la restriction au niveau de confidentialité « données sensibles ». *Tessaris* propose un nouvel article : « Le patient peut modifier en tout temps le niveau de confidentialité des données enregistrées dans son dossier électronique. La modification est automatiquement signalée aux professionnels de la santé responsables du traitement. »

En ce qui concerne l'article 2, *H+* et *senesuisse* déclarent saluer l'approche consistant à définir dans la configuration de base un droit d'accès « normal » en absence de souhait spécifique du patient. L'extension à des niveaux supplémentaires doit être rejetée par souci de simplicité. HIN, qui s'exprime également sur l'art. 2, propose de le compléter comme suit : « Sauf autre restriction de la part du patient, un professionnel de la santé peut déléguer les droits d'accès qui lui sont attribués à des auxiliaires dans la mesure où le rattachement de ces auxiliaires au professionnel de la santé est géré en interne par la communauté. » Ils souhaitent par ailleurs le complément suivant à l'art. 3 : « Le patient peut interdire à un professionnel de la santé de déléguer ses droits d'accès à des auxiliaires ».

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.

[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.

HIN et *santésuisse* répètent des remarques déjà formulées à propos de l'art. 1 et la *FMH* sa prise de position exprimée en introduction à ce même article. *PH CH* et *IG eHealth* souhaitent un al. 6 qui ait le contenu suivant : « Les professionnels de la santé de la communauté de référence du patient sont habilités à attribuer des droits d'accès à d'autres collègues en son nom ; ils ne peuvent attribuer que des droits d'accès qu'ils possèdent eux-mêmes. » La *CCM*, *BüAeV* et *GAeSO* proposent l'alinéa supplémentaire suivant pour l'art. 2 :« Sauf autre restriction de la part du patient, un professionnel de la santé peut déléguer les droits d'accès qui lui sont attribués à des auxiliaires dans la mesure où le rattachement de ces auxiliaires au professionnel de la santé est géré en interne par la communauté. » L'*OSP* demande l'introduction des alinéas supplémentaires suivants : Al. 6 : « Le patient doit pouvoir consulter en tout temps l'historique conformément à l'art. 8, al. 1 LDEP ». Al. 7 : « En cas de litige, la preuve de la légitimité d'accès est à la charge du professionnel de la santé. » *Physioswiss* approuve expressément les alinéas 1 à 4. *TI* observe qu'un professionnel de la santé qui a créé un document sans disposer d'un droit d'accès au dossier électronique du patient devrait pouvoir rectifier ultérieurement une erreur éventuelle. La *SSIM* fait remarquer que cette disposition fait endosser au patient la responsabilité d'une rétention d'informations susceptible de compromettre le cas échéant la sécurité du traitement. Dans le même esprit, *STSAG* demande que les responsabilités soient désignées dans un alinéa supplémentaire pour les cas où des données seraient classées secrètes par le patient. Elle se prononce en outre pour la possibilité d'accéder aux informations secrètes en cas d'urgence.

Quatorze participants[10] rappellent que la situation des personnes incapables de discernement et des

[10] BL, CDS, GL, OW, UR, VAKA, NW, FR, BE, K3, VZK, ZG, ZAD, TG

enfants n'est pas réglementée et demandent qu'on se saisisse de la question. En effet, selon neuf[11] de ces participants, le droit d'exécution ne prévoit pas à ce stade si, et à quelles conditions, les droits de gestion du dossier d'un patient pourraient être exercés sans son consentement, voire même contre sa volonté, par des personnes qu'il a habilitées en application de l'art. 3, let. g. *K3*, *VZK*, *ZG* et *ZAD* souhaitent en outre que l'ordonnance règle aussi la gestion des dossiers de personnes décédées. Pour *K3* et *VZK* se pose en plus la question d'attribuer ou non un dossier aux sans-papiers.

Al. 1 : L'*Insel* critique le fait que l'instauration de trois niveaux de droits d'accès paraît inutilement compliquée. On peut partir du principe que le patient ne saisira même pas dans son dossier les données sensibles dont il voudra empêcher la consultation par des tiers, à quoi il faut ajouter que les institutions de santé ne feront qu'un usage limité, si tant est qu'elles en font un, d'un dossier électronique si celui-ci est incomplet ; elles préfèreront s'appuyer sur leurs systèmes primaires, d'où la demande de la suppression de la let. a de l'al. 1. *HÄ CH* et *ÄTG* signalent que leur proposition de fusionner les let. b et c de l'art. 1, al. 1 réduit à deux le nombre d'options dans l'art. 2, al. 1. Ils font remarquer que l'attribution de droits d'accès sous la forme prévue est un processus complexe et exigeant qui risque de dépasser les patients, et demandent par conséquent qu'il soit simplifié. *PharmaSuisse* et *ZH* recommandent qu'un prestataire qui n'aurait qu'un accès restreint à certaines données en soit obligatoirement informé, et qu'il lui soit communiqué notamment à quels contenus il n'a pas accès. *PharmaSuisse* ajoute qu'il faudrait prévoir la possibilité de retracer, en consultant des fichiers-journaux, les informations dont un prestataire a pu disposer à un moment donné. *Integic* demande une adaptation aux trois niveaux de confidentialité du système international EPSOS. Cela implique de reformuler comme suit les let. a à c de l'al. 1 : « a. "restreint" : autorise l'accès au niveau de confidentialité "données accessibles normalement" ; b. "normal" : autorise l'accès aux niveaux de confidentialité "données accessibles normalement" et "données d'accès restreint" ; c. "étendu" : autorise l'accès aux niveaux de confidentialité "données accessibles normalement", "données d'accès restreint" et "données d'accès très restreint" ». *PH CH* fait valoir que l'introduction de définitions pour les droits d'accès n'a pas de sens et demande que le texte de l'al. 1 soit modifié comme suit : « […] à des groupes de professionnels de la santé l'accès aux données utiles uniquement, aux données utiles et médicales ou aux données utiles, médicales et sensibles, à choix ». Les let. a à c doivent être supprimées, tout comme l'al. 3 qui peut être réintégré dans l'al. 2. *Tessaris* propose que tous les professionnels de la santé impliqués dans le traitement d'un patient puissent accéder à ses « données médicales », à la condition que le patient n'en ait pas interdit préalablement l'accès à tous les professionnels de la santé ou à une personne en particulier. De plus, un professionnel de la santé devrait pouvoir accéder à des données même « sensibles » ou « secrètes » sur accord préalable du patient. *KAeG SG* fait remarquer que la saisie de certaines données ne deviendrait plus appropriée dès lors que le patient pourrait y accéder. Il demande aussi comment accéder aux données en cas de perte de la carte, et si les données sont stockées dans une solution Cloud.

Onze participants[12] trouvent que la construction « groupes de professionnels de la santé » est compliquée et laborieuse. Neuf d'entre eux souhaitent[13] que l'on essaie de la simplifier, tandis que *ZH* et *ZAD* demandent sa suppression pure et simple. *ZH* propose le nouvel énoncé suivant pour l'al. 1 : « Le patient peut accorder à des prestataires ou à des professionnels de la santé les droits d'accès suivants : […] ». […] ». *TI* juge nécessaire de définir l'expression « groupe de professionnels de la santé » et de faire en sorte que les patients comprennent l'utilisation de cette fonction. Six autres cantons[14] demandent que cette notion de « groupe » soit précisée. D'après eux, le fait que l'on ne puisse pas accorder de droits d'accès à toute une institution pose des problèmes de faisabilité, notamment aux hôpitaux. Ils souhaitent que l'al. 1 soit complété comme suit : « Le patient peut accorder à des institutions, des professionnels […] » et proposent la modification suivante pour l'al. 4 : « […] un groupe ou une institution reçoit les droits d'accès accordés à ce groupe ou à l'institution. »

Les al. 1 et 4 doivent être complétés de manière à être valables pour les groupes comme pour les

[11] BL, CDS, GL, OW, UR, VAKA, NW, BE, TG
[12] BL, GL, LU, OW, UR, ZG, SZ, NW, CDS, ZH, ZAD
[13] BL, GL, LU, OW, UR, ZG, SZ, NW, CDS
[14] GE, VS, VD, JU, FR, NE

institutions de santé. *SMCF* estime que pour des raisons de praticabilité, il ne devrait pas exister de droits d'accès individuels au sein d'un groupe donné. Pour *AG*, les droits d'accès de groupe sont très importants pour des raisons de praticabilité. La recherche de la composition d'un groupe est conforme au droit de la protection des données, mais peut entraîner des surcoûts pour la communauté. Les *PKS* sont d'avis que les dispositions régissant les droits d'accès sont à la fois impraticables et inadaptées aux besoins thérapeutiques des patients et aux processus hospitaliers. Ils proposent que les configurations de base permettent l'accès intégral à toutes les données médicales et que les patients puissent limiter cet accès au besoin. La restriction actuelle de l'accès aux données, fussent-elles sensibles, et l'obligation de justification compliquent inutilement la collecte d'informations en cas d'urgence.

Al. 2 : *KDSBSON*, *DSBAG*, *privatim* et *FR* réitèrent ici leurs commentaires relatifs à l'art. 1, al. 2 concernant le principe de « privacy by default ».

La *FSAS*, *Physioswiss*, *SWOR*, l'*ASI* et *H+* préconisent de définir les droits d'accès avec la configuration « normale » par défaut. La *Poste*, quant à elle, s'en tient à un droit d'accès « restreint » à défaut d'attribution de droits plus étendus. *Tessaris* propose la suppression pure et simple de cet alinéa, vu que la restriction d'accès aux données du niveau de confidentialité « données sensibles » est déjà contenue dans sa proposition d'énoncé de l'art. 1, al. 2. La *FMH* réitère ici son commentaire relatif à l'art. 1, al. 2.

Al. 3 : *KDSBSON*, *DSBAG*, *privatim* et *ZG* mettent en garde contre l'octroi de droits d'accès pour une durée illimitée. Ils recommandent aussi d'examiner la possibilité d'avertir le patient avant l'expiration de ses droits d'accès. Ils proposent la modification suivante de l'art. 3, let. a : « Les droits d'accès sont accordés aux professionnels de la santé pour une durée maximale de deux ans ». *TG* se prononce également pour une limitation de la durée maximale des droits d'accès. *Tessaris* souhaite que l'alinéa soit supprimé, vu que le changement des niveaux de confidentialité, avec la modification ou la suppression des droits d'accès qu'il implique, découle déjà de sa proposition d'énoncé de l'art. 1, al. 3. L'art. 2, al. 3 peut être reformulé comme suit : « Le patient peut exclure temporairement ou en permanence un professionnel de la santé ou un groupe de professionnels de la santé nommément désigné de l'accès à son dossier électronique ».

Al. 4 : *privatim*, *KDSBSON* et *DSBAG* soulignent la nécessité impérative de préserver l'option d'un « opt-out » selon l'art. 3, let. f au cas où les autorisations d'accès de groupe seraient maintenues. *TG* pense que l'attribution automatique à un groupe et la reprise de ses droits d'accès pourraient poser des problèmes par rapport au secret professionnel et en donne un exemple. Une solution est exigée qui garantisse le secret professionnel dans tous les cas.

KSSG relève l'impossibilité de garder une vue d'ensemble de la présentation des professionnels de la santé et de leurs groupes au sein d'une grande organisation. De plus, les changements de personnel sont tellement fréquents que les patients seraient débordés par la pléthore d'informations qui leur seraient transmises. C'est pourquoi il convient de compléter l'art. 8 d'une lettre supplémentaire précisant que l'OFSP peut autoriser les communautés à ne divulguer aux patients qu'une partie des noms des professionnels de la santé par souci de clarté. Se pose aussi pour l'art. 2, al. 4 la question de l'octroi immédiat ou non des droits d'accès en application de l'obligation d'informer visée à l'art. 8, let. f. *KSSG* propose de compléter l'al. 4 comme suit : « […] reçoit, sans confirmation expresse par le patient, les droits d'accès accordés à ce groupe ; ces droits lui sont retirés lorsqu'il […] ». *VGIch* fait remarquer qu'un professionnel de la santé faisant partie d'un groupe qui détient un droit d'accès automatique a le temps de transférer des informations d'un patient dans le système primaire avant que le patient n'ait la possibilité d'exclure ce professionnel de l'accès à ses données. L'association propose la création de vrais groupes collectifs, à charge du patient de décider s'il y consent ou non. *ISSS* propose la rédaction d'un nouvel alinéa obligeant les communautés à présenter sur demande une liste de leur personnel aux patients afin qu'ils puissent choisir les (groupes de) professionnels de la santé auxquels ils attribuent des droits d'accès. *PH CH* et *IG eHealth* critiquent le fait que dans les configurations de base, les patients sont certes informés de toutes les modifications du groupe, mais non des accès en urgence. Il s'ensuit une pléthore d'informations aux patients et une transparence des mutations des professionnels de la santé susceptible de porter atteinte à leur personnalité. Ils proposent de laisser l'al. 4 inchangé,

mais de modifier les options dans l'art. 3. *Lovis* est d'avis qu'il ne devrait pas exister de « liste noire » visant à exclure certaines personnes d'un groupe donné.
K3 et *VZK* signalent que rien n'indique si un professionnel de la santé peut faire partie de plusieurs groupes simultanément et souhaitent un moyen d'identification qui permette de le savoir. En outre, il est important pour les hôpitaux que l'accès aux dossiers électroniques de patients puisse être attribué à tout l'hôpital, à un groupe au sein de l'établissement ou à des professionnels de la santé à titre individuel, et que l'autorisation d'accès soit normalement octroyée par défaut à tout l'établissement. Les deux participants observent également ici que ces droits d'accès doivent aussi être accordés au personnel auxiliaire. Ce point doit être précisé dans l'ordonnance, vu qu'il n'est encore mentionné que dans l'annexe 2 des CTO, ch. 1.3 de l'ODEP-DFI. Il faut également assurer aux services du personnel des hôpitaux les moyens de procéder simplement à des vérifications d'identité (art. 23 ODEP) et de remettre (art. 22 ODEP) ou de renouveler (art. 25 ODEP) des moyens d'identification appropriés.

Al. 5 : *BRH* trouve que la procédure d'accès en urgence est laborieuse, voire confuse et souhaite une description plus concrète des éléments de sécurité. Il estime en outre qu'il faut indiquer les temps requis pour franchir de telles barrières de sécurité dans une situation d'urgence. *VAKA*[15] se prononce pour que les données même sensibles soient disponibles par défaut dans l'éventualité d'une urgence. *Senesuisse* fait valoir que l'énoncé n'est pas assez clair pour réglementer les droits d'accès des professionnels de la santé concernés. Alors que l'al. 5 limite les possibilités d'accès uniquement aux données « utiles » et « médicales », l'art. 3, let. b dispose que la réglementation du droit d'accès est entièrement à la discrétion du patient, y compris pour les cas d'urgence. Une réglementation dûment adaptée pour les cas d'urgence médicale serait préférable. *ZG* demande qu'il soit précisé dans le rapport explicatif, à propos des accès en urgence médicale, que l'art. 24 LDEP ne s'applique que dans les situations où il n'y avait manifestement pas d'urgence.

VAKA veut imposer la nécessité de se reconnecter pour un accès en urgence. Toute autre justification lui paraît obsolète, raison pour laquelle la phrase « Vous devez d'abord justifier votre demande d'accès » doit être biffée de l'alinéa. *K3*, *VZK*, *ZH* et *ZAD* sont également d'avis que l'on peut se passer d'une justification pour un accès en urgence. *ASPS*, *Spitex* et *BINT* soulignent la nécessité de maintenir les obstacles d'une justification à un faible niveau pour assurer la rapidité d'accès et préconisent des consignes structurées, plus faciles à appliquer et à interpréter. Tous trois proposent de simplifier la procédure de justification ou de prévoir la possibilité d'une justification rétroactive pour les cas d'urgence. La *FMH* et *Physioswiss* sont d'accord pour considérer comme inutile la justification préalable d'un accès en urgence. La collecte rétrospective et systématique d'informations et la justification éventuelle des cas suspectés d'accès abusif doivent être des instruments suffisants. Six cantons[16] demandent en outre que la mention « au préalable » soit supprimée de l'al. 5. *ZG* souhaite voir précisé que l'on n'imposera pas de hautes exigences au contenu et au volume de la justification. Sinon, les professionnels de la santé risquent de renoncer à consulter le dossier électronique du patient en cas de doute. *HL7*, *IHE* et *Integic* voudraient une consigne quant à la forme et aux détails de la documentation à fournir pour justifier un accès en urgence afin de restreindre toute utilisation illicite. Ils sont en outre d'avis, à l'instar de la *SSIM*, que l'on pourrait envisager de remplacer la justification préalable par une brève confirmation du cas d'urgence (1 clic), à charge pour l'utilisateur de fournir une justification détaillée par la suite. La *Poste* estime qu'une justification est dénuée de sens et propose de la remplacer par un message d'information automatique au médecin de confiance et au patient. La volonté d'accéder en urgence avec notification doit être confirmée (cocher et cliquer sur « OK »). *AG* souligne que l'accès en urgence doit être d'une simplicité technique maximale. *TI* doute qu'il soit praticable d'exiger une justification écrite et l'éventuelle sécurisation d'un accès en urgence au moyen d'un mot de passe et d'un code. L'accès aux données doit par conséquent être simplifié, p. ex. au moyen d'un choix de réponses à confirmer par l'utilisateur. Alors que *LUKS* déclare également préférer une justification a posteriori et qu'*Insel* demande concrètement la suppression du mot « préalable », l'*OSP* appuie l'exigence de justifier préalablement une demande d'accès et de la sécuriser par une interaction manuelle dans les cas d'urgence médicale. Comme l'*OSP*, la *FRC* juge nécessaire de motiver et au préalable et brièvement

[15] Sans Bethesda
[16] GE, VS, VD, JU, FR, NE

l'accès dans les cas d'urgence.

SMCF propose concrètement comment formuler l'al. 5 : « En cas d'urgence médicale, […] Ils doivent pouvoir motiver cet accès a posteriori ». *Tessaris* propose d'en modifier le texte comme suit : « […] accéder aux niveaux de confidentialité "données médicales" et "données sensibles". Ils doivent consigner la justification d'un tel accès par une inscription dans le dossier électronique du patient ». *IG eHealth* et *PH CH* préféreraient le texte suivant pour l'al. 5 : « En cas d'urgence médicale, les professionnels de la santé peuvent accéder au niveau de confidentialité "données médicales". Ils doivent confirmer au préalable une telle demande d'accès par une déclaration d'intention. Cette déclaration doit mentionner que l'accès ne peut s'effectuer que dans une situation d'urgence médicale du patient. Le patient et son médecin de famille doivent être informés de cet accès en urgence. *Pharmasuisse* soumet également une proposition concrète d'énoncé : « […] accéder à tous les niveaux de confidentialité, à condition de ne pas faire l'objet d'une exclusion d'accès générale par le patient. […] ». *CURAVIVA* et *Insos* font remarquer que la relation entre l'al. 5 et l'art. 3, let. b in fine ODEP, et le rapport hiérarchique qui les lie, ne sont pas clairs. Ils proposent d'ajouter la phrase suivante à la fin de l'al. 5 : « L'art. 3, let. b in fine demeure réservé ». L'*AMDHS* recommande que l'al. 5 prévoie d'assurer aussi l'accès aux « données sensibles » dans les cas d'urgence, sauf si le patient a restreint l'accès aux « données médicales » ou aux « données utiles » comme le lui permet l'art. 3, let. c. *KAeG SG*, *BüAeV*, *GAeSO* et la *CCM* souhaitent l'ajout du texte suivant à l'al. 5 : « La communauté de référence fait en sorte que les informations d'accès parviennent au patient par le canal de transmission qu'il aura préalablement choisi. Si le patient n'a pas choisi de mode de transmission, l'information lui est communiquée par lettre recommandée ». *BüAeV*, *GAeSO* et la *CCM* demandent en outre une définition plus précise des cas d'urgence médicale et proposent donc d'ajouter à l'art. 5 un alinéa ayant la teneur suivante : « Un cas d'urgence médicale est un cas dans lequel le patient a besoin d'une assistance médicale urgente suite à un accident ou une maladie ».

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.

HIN réitère les remarques déjà formulées à propos de l'art. 1. Neuf participants[17] réitèrent en outre leur demande de voir adopter une réglementation découlant de l'art. 2 pour les personnes incapables de discernement et les enfants, une requête à laquelle se joint *SZ*, et qui est également appuyée par *BE* en ce qui concerne les personnes incapables de discernement. *ZG* et *ZAD* rappellent ce qu'ils ont relevé à propos de l'art. 2, à savoir la nécessité d'adopter une réglementation pour les personnes décédées. La *FMH* réitère sa position exprimée en introduction aux art. 1 et 2.

La *FRC* est expressément satisfaite de l'énoncé des let. d à h. Six cantons[18] souhaitent l'ajout d'une

[17] CDS, BL, GL, LU, OW, UR, NW, ZG, ZAD
[18] FR, NE, GE, VS, VD, JU

let. i formulée comme suit : « Introduire la notion de délégation temporaire d'un professionnel de la santé à un autre (en cas d'absence), sans qu'un patient n'ait à ajouter ce professionnel dans les droits d'accès. Ce mode serait activé par défaut. Proposer une option de désactivation par le patient pour cette fonction de délégation de professionnel de la santé à un autre ». *ASPS* et *Spitex* proposent ici la création d'une sorte de table des matières avec les noms de tous les documents enregistrés dans le dossier électronique du patient, afin que le patient puisse être informé le cas échéant de la nécessité d'autres documents importants pour le traitement correspondant. *KAeG SG*, *BüAeV*, *GAeSO* et la *CCM* observent que leur proposition d'ajouter un article réglementant la saisie de données propres implique que l'art. 3 doit être adapté comme suit : « [...] choisir le niveau de confidentialité attribué aux données qu'il a lui-même enregistrées dans son dossier et/ou définir un droit d'accès, voire l'exclure complètement ». En outre, leurs déclarations dans le rapport explicatif et l'adaptation de l'art. 2 nécessitent de modifier l'art. 3 comme suit : « […] interdire à certains professionnels de la santé de déléguer les droits d'accès à des auxiliaires ». Le ch. 6 de l'annexe « Critères techniques et organisationnels de certification » doit être étendu ou complété par analogie. Les *PKS* font remarquer que les options d'octroi et de retrait de droits d'accès représentent une charge considérable pour les communautés et que l'inscription de professionnels de la santé sur une liste noire ne correspond pas à la pratique actuelle en matière de soins de santé. *SMCF* observe que les avantages du dossier électronique du patient sont réduits à néant par la multiplicité et la complexité des options, et que les droits d'accès devraient donc être gérés si possible de manière globale pour l'entier du dossier.

Let. a : Pour des considérations relevant du principe de « privacy by default », *privatim*, *DSBAG*, *KDSBSON* et *FR* déconseillent d'inscrire des droits d'accès d'une durée illimitée dans la configuration de base. À l'instar de *ZG*, ils proposent l'énoncé suivant pour l'art. 3, let. a : « a. accorder des droits d'accès de durée illimitée à certains professionnels de la santé ». *ZG* recommande quant à lui que l'on examine l'option de limiter la durée de l'autorisation d'accès dans la configuration de base. De l'avis de *K3*, *VZK* et *VAKA*, une restriction des durées d'accès n'a guère de sens et serait trop complexe à gérer. Ou le droit d'accès existe, ou il n'existe pas. Tout comme *Integic*, ils demandent la suppression de la let. A. Au lieu d'une suppression pure et simple, *Integic* entrevoit toutefois la possibilité de définir des restrictions dans d'autres intervalles de temps. Les let. a et f sont en tout cas trop compliquées à appliquer en la forme, même pour les fabricants de systèmes. *VGIch* ne voit pas pourquoi l'option de fixer une durée pour les droits d'accès devrait être limitée à 6 mois. Comme *H+* et *Insel*, ils souhaitent que cette règle soit assouplie pour que le patient puisse fixer la limite de cette durée d'accès en toute autonomie. *IG eHealth*, *PH CH* et *La Poste* trouvent trop rigide l'instauration d'une durée fixe de six mois. Ils font remarquer que les patients pourraient vouloir donner à un professionnel de la santé le droit d'accès pour une seule consultation et recommandent de compléter la let. a comme suit : « […] en vertu de l'art. 2, al. 1, s'éteignent au bout de six mois au maximum ; ». Dix participants[19] déclarent que la fixation de ces délais doit être laissée aux fournisseurs de solutions pour le dossier électronique et proposent que la let. a soit reformulée comme suit : « […] en vertu de l'art. 2, al. 1, aient une durée de validité limitée ; ». *TI* fait valoir que la let. a n'indique pas clairement si d'autres durées de validité sont également admises et qu'il convient de le préciser. *Tessaris* parle de surdétermination à propos de la fixation de l'échéance à six mois et recommande que la durée des droits d'accès visés à l'art. 2 soit fixée par le patient lors de la consultation. *FR* souligne que le patient devrait être informé par une alarme de l'existence d'une échéance des droits d'accès et de ses conséquences et demande l'inscription dans l'ordonnance d'un article ou d'un alinéa supplémentaire à cet effet.

La *FRC* trouve très bien que le patient ait la possibilité d'annuler automatiquement les droits d'accès au bout de six mois.

Let. b : *CURAVIVA* et *Insos* réitèrent leur position vis-à-vis de l'art. 2, al. 5. *PharmaSuisse* recommande – sous réserve de l'acceptation de sa proposition d'énoncé de l'art. 2, al. 5 – la modification suivante de l'art. 3, let. b : « […] exclure de manière générale le droit d'accès à son dossier en cas d'urgence médicale ». Au cas où la proposition d'énoncé pour l'art. 2, al. 5 serait rejetée, l'art. 3, let. b doit être reformulé comme suit : « limiter au niveau de confidentialité […] en cas d'urgence médicale, après avoir reçu

[19] CDS, BL, GL, LU, OW, UR, AR, TG, BS, SZ

les informations nécessaires de la part d'un professionnel de la santé ». *Spitex* et *ASPS* préconisent que l'on demande au patient de confirmer activement son refus de voir afficher les données sensibles dans les cas d'urgence. La configuration par défaut doit par conséquent inclure le paramètre « données sensibles ». Une notification automatique de l'accès en urgence effectué serait en outre utile. *Tessaris* demande la suppression de l'art. 3, let. b en cas d'acceptation de sa proposition de reformulation de l'art. 5, al. 2. La *FRC* souligne qu'il peut être assez dangereux d'exclure complètement le droit d'accès pour les cas d'urgence médicale. Pour *AG*, une exclusion par le patient de l'accès en urgence serait problématique si celui-ci était incapable de discernement au moment de paramétrer la configuration. Il est important de faire dûment référence au droit de protection de l'adulte et de l'enfant dans les passages correspondants du rapport explicatif. *HÄ CH* et *ÄTG* ne voient pas de sens à la let. b et demandent sa suppression. D'après *STSAG*, il convient aussi de préciser dans cet article que le patient assume la responsabilité des éventuelles conséquences thérapeutiques de la non-disponibilité de certaines informations. L'autre option est de définir la configuration de base du dossier électronique du patient de manière à garantir un accès à toutes les informations en cas d'urgence.

Let. c : *Tessaris* demande la suppression pure et simple de l'art. 3, let. c, une mesure en droite ligne avec l'introduction proposée à l'art. 1. *HÄ CH* et *ÄTG* trouvent cette disposition risquée et souhaitent ne laisser aucune possibilité de choix. Se référant à leur commentaire de l'art. 1, ils demandent l'attribution par défaut aux données médicales.

Let. d : *H+*, *HÄ CH* et *ÄTG* sont d'avis que l'accès en urgence devrait pouvoir être accordé par un professionnel de la santé malgré le refus d'accès général par le patient. Dans un ordre d'idées similaire, *VGIch* demande que le patient puisse avoir la possibilité d'exclure des professionnels de la santé mais de leur autoriser quand même l'accès aux données en cas d'urgence. *BS* est du même avis et propose l'énoncé suivant : « […] de la santé. Dans des situations d'urgence médicale, il peut accorder le droit d'accès à des professionnels de la santé qui en sont exclus. » *KSSG* pense que la let. d est en contradiction avec des déclarations verbales selon lesquelles tous les professionnels de la santé ne sont pas tenus d'être présentés aux patients. S'il doit exister une possibilité effective de restreindre la présentation des professionnels de la santé à l'extérieur, la let. d doit être précisée comme suit : « d. refuser […] à certains professionnels de la santé visibles de l'extérieur […] ». *Tessaris* souhaite la suppression pure et simple de l'art. 3, let. d et renvoie à sa prise de position sur l'art. 2, al. 3.

Let. e : *VAKA* souhaite que la let. e, tout comme l'art. 2, soit applicable par défaut et n'admette que des exceptions effectives. Il propose des adaptations basées sur la valence des paramètres par défaut et des exceptions. Dans la suite logique de leur demande de supprimer la let. f de l'art. 8, six cantons[20] considèrent que la let. e de l'art. 3 doit également être supprimée. *IG eHealth* et *PH CH* mettent en garde contre le risque de susciter un déferlement inapproprié d'informations chez certains patients dans l'état actuel de la réglementation. Selon eux, la let. e doit donc être adaptée comme suit : « e. consulter en tout temps la composition actuelle d'un groupe de professionnels de la santé ». La *Poste* qualifie également de pléthorique l'abondance des notifications de mutations en cours et demande, comme *ZG*, que l'« opt-out » soit remplacé par l'« opt-in ». Pareillement, *Tessaris* recommande que les patients doivent demander à être informés des mutations (arrivées/départs) dans un groupe de professionnels de la santé. *Spitex* et *ASPS* sont également pour que l'on demande aux patients de confirmer activement leur volonté d'être informés de l'arrivée de nouveaux membres dans un groupe de professionnels de la santé. En conséquence, le mot « désactiver » doit être remplacé par « activer » à la let. e. Pour des raisons relevant de la protection des données, *K3* et *VZK* jugent que l'on ne peut pas prendre la responsabilité de laisser au patient la possibilité de se servir de son dossier électronique pour rechercher tous les professionnels de la santé d'une institution, y compris ceux qui n'ont pas accédé à son dossier. C'est pourquoi la let. e doit être supprimée.

Let. f : *VGIch* réitère ici son commentaire relatif à l'art. 2, al. 4 concernant les groupes de professionnels de la santé, tandis que *KDSBSON*, *DSBAG* et *privatim* réaffirment leur position sur l'art. 2, al. 4 concernant la possibilité d'« opt-out ». L'*ASI*, *FSAS* et *SWOR* jugent possible que cette disposition s'avère

[20] FR, NE, GE, VS, VD, JU

difficile à appliquer dans de grandes organisations, mais soulignent que ce droit doit être reconnu aux patients.

Six cantons[21] sont d'avis qu'un patient ne devrait avoir la possibilité ni de modifier les droits d'accès reçus par des professionnels de la santé lors de leur entrée dans un groupe, ni d'inscrire des professionnels de la santé nommément désignés sur une « liste noire ». *Insel* fait remarquer que l'exclusion individuelle de personnes est pratiquement impossible à mettre en œuvre dans un hôpital et dans les systèmes primaires. Ce n'est probablement pas non plus dans l'intérêt du patient au cas où un accès en urgence s'imposerait. *K3* et *VZK* contestent également la praticabilité de cette disposition dans un hôpital. À l'instar de *La Poste*, ils insistent sur le principe que les droits d'accès d'un groupe sont donnés à tous ses membres et que la seule autre option consiste à nommer individuellement un ou plusieurs professionnels de la santé. Toute autre solution est inapplicable dans les hôpitaux et peut créer des situations dangereuses. Il faut en outre faire en sorte que les professionnels de la santé voient à tout moment s'ils ont un accès total ou restreint à un dossier électronique du patient. Pour *USB*, donner au patient la possibilité d'exclure généralement de l'accès à son dossier les professionnels de la santé nouvellement entrés dans le groupe est une tâche trop complexe. Il doit suffire de pouvoir inscrire certaines de ces personnes sur la liste d'exclusion. *ZH*, *NW*, *ZG* et *ZAD* considèrent que la let. f est inapplicable chez les gros prestataires. Les droits d'accès d'un groupe doivent être garantis à tous ses membres, sous peine d'exposer les patients à des situations potentiellement dangereuses pour leur vie. *KSSG* plaide pour que les professionnels de la santé et les auxiliaires venus rejoindre un groupe héritent automatiquement de ses autorisations d'accès, tandis que *LUKS*, *Integic*, *HL7*, *IHE* et *medshare* reprochent à la let. f d'être trop compliquée à mettre en œuvre sur le plan technique et organisationnel. *Integic* ajoute que rien dans le texte n'indique si le patient est activement informé lorsqu'un professionnel de la santé a procédé à une transmission des droits d'accès. *IG eHealth*, *PH CH* et *La Poste* déclarent qu'il revient au patient de décider s'il accorde sa confiance à l'institution et à sa capacité d'auto-organisation ou à des individus. *SBC* plaide de manière générale pour une réduction de la complexité. *VAKA* se déclare pour que l'on autorise un héritage des droits d'accès et recommande que l'on renforce l'usage des exclusions primaires et des droits d'accès individuels plutôt que d'essayer de gérer les dynamiques des groupes.

Vingt-quatre participants[22] demandent la suppression pure et simple de l'art. 3, let. F. *La Poste* en propose également la suppression, mais pourrait envisager à sa place que l'on oblige les portails à proposer au patient d'autoriser un groupe ou de copier les noms de ses membres. Ainsi, le patient saura toujours clairement s'il a donné son autorisation à des individus ou à tout un groupe. *IG eHealth* et *PH CH* proposent de reformuler la let. f comme suit : « f. choisir qu'aucun droit d'accès ne soit accordé à des groupes ». *Tessaris* demande que l'ordonnance dispose que les professionnels de la santé qui entrent dans un groupe ne reçoivent le droit d'accès attribué à ce groupe qu'une fois que leur nom a été communiqué au patient. *OSP* demande si les représentants agissent sous leur propre identité et souhaite une formulation plus intelligible.

Let. g : *K3* et *VZK* observent que les règles auxquelles sont soumis les représentants sont appelées à changer très souvent et que l'ordonnance doit surtout définir à partir de quel âge un enfant peut ouvrir lui-même un dossier électronique du patient ou en assumer l'entière responsabilité. À ce propos, *VGIch* signale que le statut de l'enfant et les droits d'accès à son dossier ne sont pas clairement définis relativement au droit de garde. Pour *IG eHealth*, *PH CH*, *ZG* et *La Poste*, ces dispositions ne vont pas assez loin. Alors qu'*IG eHealth* et *PH CH* souhaitent que le texte clarifie comment procéder en cas de perte de la qualité pour agir, *ZG* et *La Poste* plaident pour qu'il précise les modalités d'usage des moyens d'identification, des procurations et des révocations.

TI souhaite que soit défini le terme de « représentant » ou, à défaut, que le texte fasse référence au

[21] FR, NE, GE, VS, VD, JU

[22] FR, NE, Insel, Integic, HL7, IHE, KSSG, K3, VZK, LUKS, SBC, ZH, NW, ZG, ZAD, USB, GE, VS, VD, JU, HÄ CH, ÄTG, medshare, STSAG

« représentant thérapeutique » du patient ou à la « personne habilitée à [le] représenter dans le domaine médical » conformément à l'art. 377 CC. *Senesuisse* qualifie la réglementation des droits des représentants de tentative inutile et ratée. Ces droits sont réglés de manière beaucoup plus claire et complète par l'art. 377, let. f CC. Il serait possible d'y faire référence et de lui apporter des compléments éventuels. *CURAVIVA* et *Insos* font remarquer que le représentant d'un patient incapable de discernement est habilité à prendre des décisions dans tous les domaines où le patient pourrait décider lui-même s'il était capable de discernement, pour les mesures médicales en particulier. Une fois dûment informé par le médecin et le personnel soignant, le représentant peut consentir à un traitement et notamment à l'ouverture d'un dossier électronique du patient, ou au contraire s'y refuser. Le représentant n'intervient cependant que si le patient incapable de discernement ne s'est pas déjà exprimé lui-même sur la décision à prendre dans les directives anticipées (art. 377 et 378 CC). Cette réglementation est claire et se suffit à elle-même. Elle complète harmonieusement celle du dossier électronique du patient. À cet égard, l'art. 3 let. g est superflu et de surcroît, incomplet, mais comme il n'entre pas en conflit avec la législation protégeant les personnes incapables de discernement, il peut être conservé en la forme. *HÄ CH* et ÄTG rappellent que l'*énoncé de la let.* g a été conçu pour des patients ; ils souhaitent que la représentation des professionnels de la santé, et notamment celle des médecins de famille avec leurs suppléants régionaux (pour les urgences) ou des cabinets de groupe, soit également réglementée.

Let. h : *KDSBSON*, *DSBAG*, *privatim*, *FR* et *AG* demandent s'il est exact et voulu que les droits d'accès ne puissent être transmis qu'à des professionnels de la santé de la même communauté de référence et non à ceux d'autres communautés (de référence ou non). Dans le cas contraire, le texte de l'ordonnance doit être corrigé. Avec *ZG*, ils proposent en outre l'énoncé suivant pour la let. h : « h. habiliter des professionnels de la santé à accorder des droits d'accès à d'autres professionnels de la santé en son nom. Un professionnel de la santé peut accorder tout au plus les droits d'accès qu'il possède. Il doit aviser le patient de tels octrois de droits d'accès. » *BE* propose d'ajouter la phrase : « Il doit aviser le patient de tels octrois de droits d'accès. » *IG eHealth*, *PH CH* et *La Poste* plaident pour que la transmission des droits d'accès aux délégations fasse partie de la configuration par défaut. *IG eHealth* et *PH CH* considèrent cependant que le patient devrait avoir l'option d'y mettre une limite et *La Poste* recommande de préciser jusqu'où peut aller la chaîne d'autorisation. *IG eHealth* et *PH CH* proposent l'énoncé concret suivant pour la let. h : « h. interdire la transmission des droits d'accès à d'autres professionnels de la santé de sa communauté de référence ou limiter cette transmission à un autre professionnel de la santé ou à un autre groupe au maximum. » *Tessaris* propose l'énoncé suivant pour la let. h : « […] à accorder en son nom des droits d'accès à d'autres professionnels de la santé dont l'identité lui est communiquée. » Pour *VGIch*, le but, la nécessité, les exemples et les modalités d'habilitation à transmettre les droits d'accès ne sont pas clairs. Ils demandent que la let. h soit supprimée ou clarifiée. *AG* trouve que l'habilitation d'un professionnel de la santé à transmettre ses droits d'accès à d'autres professionnels de la santé est une bonne idée, mais recèle un certain risque pour les patients, raison pour laquelle ils sollicitent des exemples. *HÄ CH* et ÄTG demandent une réglementation pour des traitements hors de la communauté de référence du patient.

3.1.2 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, 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.

D'après *Insel*, on comprend mal du point de vue des hôpitaux pourquoi on ne pourrait pas utiliser le numéro AVS pour l'identification des patients au lieu d'un numéro distinct généré par la Centrale de compensation AVS. Après tout, la Suisse s'inflige ainsi un facteur de coût qui se justifie mal si l'on se

réfère aux solutions de cybersanté confirmées en vigueur dans d'autres pays. *STSAG* souligne la nécessité de n'attribuer qu'un seul NIP à chaque patient ; celui-ci doit figurer dans le texte. *Bethesda* et *RPB* souhaitent que la question du moment d'attribution aux nouveau-nés de leur propre NIP de dossier électronique soit clairement réglementée. Ils préconisent de donner la possibilité d'ouvrir dès que possible un dossier électronique qui soit géré par la mère ou le père en qualité de représentant-e.

Al. 1 : Selon *DSBAG*, *privatim*, *ZG* et *SZ*, il est heureux du point de vue de la protection des données que le NIP ne permette pas d'identifier la personne concernée. Un avis partagé par la *CCM*, *BüAeV*, *GAeSO* et *KAeG SG*, qui s'interrogent à ce propos sur le bien-fondé et les raisons d'un enregistrement des NIP à la Centrale de compensation (CdC). Il faut d'ailleurs éviter que la CdC puisse identifier une personne à partir de son NIP. Sept participants[23] font valoir que l'adoption de standards internationaux tels que GS1-GSRN serait préférable à une solution suisse isolée. *ICTS*, *IG eHealth* et *PH CH* proposent l'énoncé suivant pour l'art. 4, al. 1 : « Le numéro d'identification du patient est un NIP conçu selon des normes internationales. Il peut être utilisé […]. » *Fondation refdata*, *GS1* et *SSIM* expliquent que la clé de contrôle GS1-GSRN se calcule sur l'algorithme Modulo-10, également proposé pour le calcul de la clé de contrôle dans le projet actuel. L'ISO « Spécification technique 18530 » adoptée par CEN en 2015 montre de quoi se compose une telle clé (GSRN) et comment elle peut être utilisée. Ils ajoutent un exemple de la structure d'une GSRN et se réfèrent au graphique qui l'illustre dans le document d'audition. *Economiesuisse* signale que la solution proposée ici empêche par ex. les frontaliers d'ouvrir un dossier électronique du patient, et qu'il convient d'y remédier.

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. 50c LAVS.

[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.

Insel réitère son commentaire relatif à l'art. 4. *VAKA*[24] propose l'obligation d'annoncer automatiquement toute mutation de données démographiques à la communauté de référence par voie électronique. Six cantons[25] demandent que pour des raisons de sécurité et de coût, le NIP puisse être utilisé au sein de la communauté (dans les systèmes primaires) pour pouvoir vérifier sans ambiguïté les identités des patients. *NE*, *GE*, *JU*, *VS* et *VD* demandent quels sont les délais et les coûts de création d'un NIP et d'ouverture subséquente d'un dossier électronique du patient. Idéalement, il devrait être possible d'obtenir un NIP en « mode transactionnel » et de créer un dossier électronique directement à partir du système primaire. Ils souhaitent que la demande de création d'un NIP soit fournie sous forme électronique et mise à disposition au cours du processus de création du dossier électronique du patient. En outre, le NIP doit être disponible immédiatement.

Al. 1 : *VAKA*, *K3* et *VZK* font remarquer que d'après ce texte, un statut d'assuré en Suisse est probablement nécessaire pour l'ouverture d'un dossier électronique du patient. Si c'est le cas, les personnes sans AVS13 (par ex. les touristes, les diplomates, les frontaliers, etc.) ne peuvent probablement pas ouvrir de dossier. *K3* et *VZK* demandent que cette question soit examinée, tandis que *VAKA* et *AG* plaident pour que tous les groupes de personnes, dans la mesure du possible, soient pris en considération pour l'attribution d'un NIP. De même, *La Poste* et *H+* demandent qu'il soit possible de créer des

[23] GS1, Stiftung refdata, SSIM, ICTS, IG eHealth, PH CH, economiesuisse
[24] Sans RPB
[25] FR, NE, GE, JU, VS, VD

NIP même pour des personnes sans AVS13. *H+* demande en outre que les communautés de référence puissent utiliser la plate-forme de transmission Sedex pour l'envoi à la CdC des demandes d'attribution de NIP. C'est la seule manière d'assurer la communication par un canal électronique efficace et déjà standardisé pour ce processus. *OFAC* demande, de manière générale, ce qui doit advenir des patients qui veulent ouvrir un dossier électronique mais ne possèdent pas de numéro AVS13. *IG eHealth* et *PH CH* proposent de compléter l'art. 5, al. 1 comme suit : « [...] de référence. La CdC veille à ce que même les personnes non obligatoirement assurées en vertu de l'art. 1 LAVS puissent être inscrites au registre central des assurés sans numéro AVS13 et que les communautés de référence puissent demander un NIP pour ces personnes ». *K3* et *VZK* demandent que le processus visé à l'al. 1 soit gardé le plus simple possible. *ASPS* et *Spitex* proposent d'attribuer un NIP à toutes les personnes ayant un numéro AVS, car cela simplifierait l'enregistrement. Les prestataires qui créent un nouveau dossier électronique de patient ou demandent un NIP par l'intermédiaire de la communauté de référence ne doivent pas encourir de frais supplémentaires.

Al. 2 : *Santésuisse* plaide pour qu'en plus des communautés de référence, le fournisseur d'identité puisse lui aussi transmettre à la CdC les données mentionnées à l'al. 2. *BRH* est d'avis que le numéro AVS, qui fait partie du NIP, compromet la protection des données ; il demande une stricte séparation entre l'identité du patient et celle de l'assuré. *PharmaSuisse* rappelle que conformément à l'art. 4, al. 1, le NIP ne doit donner aucune possibilité de tirer des conclusions sur la personne concernée. Or, une communauté de référence pourrait établir un tel lien avec le numéro AVS lors de la demande d'attribution du NIP. La question qui se pose dès lors est de savoir si la réglementation prévoit une clause de confidentialité appropriée.

Al. 3 : *K3* et *VZK* pensent qu'il n'est pas certain que la communauté de référence ne doive pas disposer d'autres données sur l'utilisateur d'un dossier électronique pour répondre à des demandes de renseignements. Ils proposent que la CdC ait l'obligation d'annoncer automatiquement toute mutation de coordonnées, de nom, etc. à la communauté de référence. Six participants[26] souhaitent que l'on précise de quelles données il s'agit. *medshare* demande en outre une définition générale de la notion de « données ». Ce terme revient régulièrement dans tous les textes du projet d'ordonnance, mais donne parfois lieu à des différences d'interprétation. *Tessaris* part du principe que l'al. 3 couvre entre autres les cas de personnes séjournant en Suisse par ex. en tant que touristes, qui ne possèdent pas de numéro d'assuré selon l'art. 50, al. C LAVS. *KSSG* fait remarquer que le service fournissant les renseignements complémentaires doit être décrit et que les demandes manuelles sont trop fastidieuses.

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.	

ASPS et *Spitex* réitèrent leur position relative à l'art. 5. *HL7*, *IHE* et *Integic* souhaitent que l'on précise les données requises pour la demande et proposent les données visées à l'art. 5, al. 2. *K3* et *VZK* soulignent que les prestataires et les professionnels de la santé doivent aussi être admis à faire cette demande, sinon certaines données risquent de ne pas pouvoir être retrouvées en cas d'urgence en raison de l'impossibilité d'accéder au dossier. *La Poste* relève que le NIP peut aussi être utilisé pour la communication entre les prestataires et le patient, et que ce numéro devrait donc être valable à vie. Il convient d'examiner si le NIP se prête à d'autres usages pour lesquels il faudrait aménager les bases juridiques dans l'ODEP.

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.	

[26] HL7, IHE, VAKA, La Poste, ZG, medshare

KSSG renvoie à sa prise de position sur l'art. 5 et rappelle la nécessité d'une description détaillée de ce service. *VAKA* rejoint ici la prise de position de *Bethesda* et de *RPB* relative à l'art. 4. *Lovis* fait valoir que le NIP doit être maintenu et que son unicité doit être garantie par l'émetteur. Pareillement, *TI* et la *FMH* demandent que l'art. 7 soit modifié par une disposition voulant que le NIP d'un patient soit conservé lors de la fermeture de son dossier électronique et lui soit réattribué à la réouverture de son dossier le cas échéant. *AG* signale à propos des art. 5 et 7 que le fait de devoir demander la suppression du NIP d'un patient lors de la révocation de son dossier électronique impose un surcroît de travail non négligeable à la communauté de référence. *medshare* déclare considérer ici que le dossier électronique d'un patient lui appartient pour la vie dès son ouverture. Pour cette raison, personne, hormis lui-même, n'a le droit de supprimer des données. Un NIP ne peut par conséquent être supprimé que sur demande du patient à la CdC. Dans un tel cas, le numéro doit également être effacé dans tous les MID. Six cantons[27] font valoir que le NIP peut servir à la communication entre communautés. Il est possible qu'un patient qui a déménagé soit inscrit auprès de deux communautés de référence. De plus, un NIP ne doit jamais être annulé, sous peine d'entraîner la perte des correspondances d'identité dans le MID de la communauté de référence et les MID des autres communautés. De la même manière qu'une personne conserve toujours le même numéro AVS13, le NIP d'un patient doit perdurer après la suppression de son dossier électronique. Cette pérennité est la condition sine qua non de l'interopérabilité. Un NIP donné doit en outre correspondre à un seul numéro AVS. Ils proposent de modifier comme suit l'art. 7, al. 1 : « […] son numéro d'identification est conservé ». Ils souhaitent l'énoncé suivant pour l'art. 2 : « En cas de création ultérieure d'un nouveau dossier électronique du patient, le numéro d'identification initial doit être repris ».

Al. 1 : *HL7*, *IHE*, *BINT* et *Integic* font valoir que les NIP des DEP devraient être supprimés aussi dans tous les MID et recommandent par conséquent la suppression de cet article. Si le concept est maintenu, les MID, Reg. & Rep. doivent être rectifiés. *BINT* et *Integic* demandent en outre que les communautés de référence avisent toutes les communautés certifiées et la CdC de la suppression d'un dossier électronique de patient.

Al. 2 : *BINT* et *Integic* plaident pour que les communautés et communautés de référence puissent, dans un certain délai, rechercher des NIP annulés en consultant la CdC par une procédure électronique. *La Poste* propose de mentionner expressément que l'al. 2 s'applique même s'il s'agit du même patient. *ASPS* et *Spitex* réitèrent la proposition que l'« ancien » NIP soit réactivé à la réouverture du dossier électronique du patient. *BFH* recommande d'introduire un al. 3 qui spécifie comment les numéros doivent être gérés si un nouveau dossier électronique du patient est ouvert après une annulation.

3.1.3 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;

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.

[27] FR, GE, VS, VD, JU, NE

VGIch réitère ici son commentaire relatif à l'art. 2, al. 4 et à l'art. 3, let. f concernant les groupes. Seize[28] participants déplorent le travail administratif considérable imposé par les dispositions de l'article 8. *VAKA* demande qu'il soit révisé en vue de réduire ce travail. *Physioswiss*, l'*ASI*, *SWOR* et *FSAS* appellent à une réglementation rapide des processus et à leur implémentation sous une forme praticable. Des ressources supplémentaires doivent être fournies à cette fin. *PharmaSuisse* fait remarquer que les patients devraient autoriser l'équipe de la pharmacie à accéder au dossier électronique en tant que groupe, sous peine de compliquer à l'extrême des activités d'équipe somme toute banales. *TI* souligne qu'il est important que les patients puissent donner l'accès à leurs données à un groupe de professionnels de la santé collaborant entre eux et renvoie aux expériences pratiques du projet « reTIsan ».

Pour *IG eHealth* et *PH CH* se pose la question de savoir comment garantir que le patient pourra connaître l'identité des auxiliaires, y compris ceux de toutes les différentes communautés/communautés de référence, et voir à qui il donnera accès à ses données. Ils proposent concrètement de reformuler l'art. 8 comme suit : « […] les professionnels de la santé, les auxiliaires et les groupes de professionnels de la santé qui leur sont affiliés. […] » […] ». S'appuyant sur les précisions à la page 15 du rapport explicatif relatif à l'ODEP et sur le message relatif à l'art. 3 LDEP, *HIN* en conclut qu'un professionnel de la santé peut déléguer le traitement d'un dossier électronique à ses auxiliaires, sauf si le patient l'a expressément interdit. Ils recommandent qu'au moment de donner son accord à la saisie de ses données dans son dossier électronique, le patient doive habiliter les professionnels de la santé auxquels il a autorisé l'accès à s'adjoindre des auxiliaires s'ils le jugent utile. *HIN* renvoie aux points qu'il a soulevés en complément aux art. 2 et 3 et souhaite, si ceux-ci n'étaient pas pris en considération, une définition plus claire des professions/formations désignées par le terme de « professionnel de la santé ». *HIN* ajoute des propositions d'énoncés pour des lettres supplémentaires à l'al. 8 : « g. veiller à ce que les patients sachent en tout temps quels auxiliaires de professionnels de la santé leur sont attribués ; », et « h. aviser le patient de la première fois qu'un auxiliaire de professionnel de la santé lui est attribué ». *KSSG* considère que l'art. 8 doit être complété pour remplir en substance les exigences suivantes : « L'OFSP désigne les groupes professionnels réputés faire partie des professionnels de la santé. Le canton désigne les registres fédéraux ou cantonaux auprès desquels l'autorisation d'accès d'un professionnel de la santé doit être vérifiée. Tous les groupes professionnels non explicitement désignés comme des professionnels de la santé sont réputés être des auxiliaires au sens des Critères techniques et organisationnels de certification, point 1.3 ». Il convient en outre d'ajouter la lettre suivante : « Par souci de clarté pour les patients, l'OFSP peut autoriser sur demande les communautés à ne rendre publics qu'une partie des noms des professionnels de la santé ».

STSAG attire l'attention sur la quasi-impossibilité pratique d'une authentification à deux facteurs. Il faut examiner l'introduction d'une infrastructure similaire à la passerelle d'accès HIN qui soit acceptée comme équivalente à l'accès authentifié. *HÄ CH* et *ÄTG* demandent une simplification de la gestion des professionnels de la santé. Ils proposent une réorganisation de cette gestion en deux modes. Un mode professionnel, pour tous ceux qui veulent étudier à fond le système et tout diriger et paramétrer eux-mêmes, et un mode « easy » où tous les paramètres se règlent « d'un clic de souris » sur des valeurs par défaut réputées raisonnables et plutôt libérales (sur lesquelles il reste éventuellement à s'entendre).

NW, *ZG*, *ZH* et *ZAD* sont d'avis qu'il ne faut pas faire appel à des dispositions indirectes, mais au contraire fixer des règles directes pour ce que les communautés ont à faire. *ZG*, *ZH* et *ZAD* proposent l'énoncé suivant pour l'art. 8, remarques comprises : « Les communautés gèrent les institutions de santé, les professionnels de la santé et les groupes de professionnels de la santé qui leur sont affiliés, conformément aux principes suivants :
a. La communauté règle les modalités d'entrée et de sortie des institutions de santé, des professionnels de la santé et des groupes de professionnels de la santé [Que doivent régler les communautés au juste ? Faut-il absolument qu'elles règlent les modalités d'entrée et de sortie ? Cette disposition est-elle vraiment nécessaire ?] ;
b. La communauté identifie les professionnels de la santé [moyens d'identification ? Que doit vérifier exactement la communauté ? Quand procède-t-elle à l'identification ?].

[28] ASPS, Spitex, Insel, VAKA, RPB, Physioswiss, PKS, UDC, ASI, SWOR, FSAS, La Poste, STSAG, HÄ CH, ÄTG

c. La communauté assure la mise à jour des données dans le service de recherche des institutions de santé et des professionnels de la santé visés à l'art. 40.
d. La communauté n'autorise l'accès au dossier électronique du patient qu'aux personnes s'authentifiant avec un moyen d'identification émis par un éditeur certifié selon l'art. 30.
e. La communauté informe les patients lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé. »

Let. b et c : *ASPS* et *Spitex* font remarquer qu'il n'existe à ce jour aucun registre complet d'infirmiers/ères en Suisse. La loi sur les professions de la santé prévoit bien la création d'un registre national, mais comme ce dernier ne sera probablement pas en place début 2017, il est important de disposer d'une solution transitoire. L'ODEP doit prévoir un registre complet ou définir un processus de transition qui permette aussi de certifier du personnel infirmier dans tous les cas. En outre, l'inscription à un registre national doit être gratuite et celui-ci doit être tenu par un organisme indépendant. À ce propos, l'*ASI*, *FSAS*, *SWOR* et *H+* notent également que l'identification univoque des professionnels de la santé, en particulier dans le secteur des soins infirmiers, confrontera les institutions de santé et les communautés à des défis de taille, raison pour laquelle un registre professionnel national complet est un outil incontournable pour la fiabilité des identifications. *HL7*, *IHE*, *Integic* et *medshare* proposent la précision suivante dans la let. b : « authentifier et identifier de manière univoque les professionnels de la santé. » Ils souhaitent en outre que l'on fixe une périodicité pour la let. c. *AG* demande que l'article soit plus clair sur les modalités d'identification des auxiliaires et précise quels auxiliaires auront une autorisation d'accès.

Let. d : *VGIch* et *Insel* observent qu'en tant qu'éditeur de moyens d'identification, un hôpital devrait, en vertu de cet article, se faire certifier ou utiliser des signatures qualifiées pour les systèmes primaires qui y sont raccordés. *Insel* demande la suppression pure et simple de la let. d et *VGIch* fait remarquer que le choix de procédures appropriées d'Identity Management du personnel hospitalier appartient exclusivement aux hôpitaux. De l'avis de *KSSG*, il convient de préciser au point 1.4 des Critères techniques et organisationnels de certification que l'identité des professionnels de la santé et des auxiliaires peut être sécurisée électroniquement et dotée d'une forte authentification pour les demandes d'accès au dossier électronique du patient.

HÄ CH et *ÄTG* proposent de maintenir l'accès au système primaire sur un seul niveau, comme cela se fait en général jusqu'à présent, et de ne faire appel aux caractéristiques de sécurité certifiées à deux niveaux que lorsque le système primaire est connecté au dossier électronique du patient pour y consulter ou y enregistrer des données. On peut aussi imaginer des cabinets où la connexion au dossier électronique du patient ne se ferait que depuis certains postes informatiques, sur lesquels les caractéristiques de sécurité correspondantes seraient installées.

Let. e : Six cantons[29] pensent que le patient ne devrait pas pouvoir accéder en temps réel à la composition des groupes, mais devrait pouvoir connaître en tout temps (via les journaux des accès) les noms des professionnels de la santé qui ont accédé à ses données, ainsi que de leur groupe. La let. e de l'art. 8 doit être supprimée. *TI* se prononce également contre un accès en temps réel et pour la suppression de la let. e. La suppression de la let. e est également souhaitée par *STSAG*, *ZG*, *K3* et *VZK*. Par souci de pragmatisme, *BFH* propose en première priorité de réduire la composition d'un groupe au médecin-chef « et à son équipe », comme c'est déjà le cas. En deuxième priorité, ou si la décision est prise de conserver tout de même la let. e, il faut entre autres faire comprendre clairement au patient que même les professionnels de la santé auxquels le droit d'accès a été refusé peuvent consulter les données via leur système clinique (primaire). *KSSG* critique le manque de traçabilité pour les patients du fait de l'exclusion des auxiliaires. Il en résulte une contradiction avec le point 1.3.2.2. des Critères techniques et organisationnels. Les auxiliaires doivent également être répertoriés dans le HPD et synchronisés avec les services centraux si cela s'avère nécessaire, mais ce n'est pas ce que souhaite *KSSG*. Il demande que les autorisations d'accès soient contrôlées au niveau du groupe ou de l'organisation et que des professionnels de la santé puissent explicitement en être exclus à titre individuel. L'*ASI*, *FSAS*

[29] FR, GE, VS, VD, JU, NE

et *SWOR* se montrent critiques par rapport à l'afflux d'informations qui s'ensuivrait si les patients étaient avisés de tous les changements du personnel soignant. Cette transparence est aussi potentiellement problématique pour les professionnels de la santé. *VGIch* souhaite que l'on nomme les critères auxquels se mesure la proportionnalité d'un groupe. *HÄ CH* et *ÄTG* trouvent la gestion des professionnels de la santé (let. e et f) trop complexe. Ils craignent que les patients ne soient dépassés, à quoi s'ajoute le risque que le médecin appelé à intervenir se voie quand même refuser l'autorisation d'accès.

Let. f : Seize participants[30] font remarquer qu'une information active sur les mutations des professionnels de la santé dans les groupes générerait une pléthore inutile d'informations, surtout dans les grandes institutions. Seize participants[31], là encore, demandent par conséquent la suppression de la let. f. I*nsel*, *K3, VZK* et *LUKS* invoquent comme autre raison le conflit avec la protection des données du personnel hospitalier. *KSSG*, la *SSIM*, la *FMH* et *LUKS* demandent que l'obligation d'information active soit supprimée. *Insel* juge suffisante une solution où le patient peut consulter ces informations au besoin. *SCH* propose que la let. f soit complétée comme suit : « offrir aux patients, sous la forme d'une option opt-in, la possibilité d'être informés lorsque des professionnels de la santé intègrent […] » *Economiesuisse*, *ZG*, *NW*, *ZH* et *ZAD* sont également partisans de limiter les possibilités d'information à une option opt-in. *HL7*, *IHE* et *Integic* déclarent que les entrées et sorties de professionnels de la santé ne doivent être communiquées au patient que si elles concernent des groupes auxquels il accorde actuellement les droits d'accès. Ils sont d'avis que la possibilité de muter de telles communications devrait renforcer considérablement l'acceptation de la solution retenue. *Integic* recommande en outre de concrétiser la conservation des journaux d'accès après une sortie. Les *PKS* et l'*UDC* estiment suffisant que les patients puissent avoir en tout temps un suivi des accès effectifs à leur dossier électronique. Tout l'hôpital devrait y avoir les droits d'accès en tant que groupe. *VGIch* fait savoir que le processus « Entrée de professionnels de la santé » doit être déclenché pour tous les professionnels de la santé qui entrent dans une institution de santé. Le rapport explicatif prévoit la possibilité de déléguer le processus d'entrée aux institutions de santé. Cette disposition doit être interprétée comme une habilitation des institutions de santé à désigner elles-mêmes les personnes qui y entrent activement. Les Critères techniques et organisationnels doivent être modifiés en conséquence.

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. es prescriptions relatives aux données historisées.

[30] AG, ASPS, Spitex, FR, GE, VS, VD, JU, NE, Insel, KSSG, FMH, SCH, economiesuisse, LUKS, La Poste, TI
[31] FR, GE, VS, VD, JU, NE, Insel, K3, VZK, LU, SCH, TI, STSAG, NW, ZH, ZAD

[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.

HÄ CH et *ÄTG* demandent si le non-accès à un dossier pourrait justifier une action en justice (par ex. pour omission) et sollicitent un avis de droit afin de tirer au clair cette question actuellement entourée d'un flou juridique, pour les patients comme pour les professionnels de la santé. Les *PKS* et l'*UDC* reprochent aux dispositions concernant l'enregistrement des données d'être lourdes à appliquer parce qu'elles ne correspondent pas aux processus actuellement en usage dans les hôpitaux. En particulier, l'enregistrement des données dans des lieux de stockage séparés génère un surcoût considérable pour les communautés sans apporter de valeur ajoutée pour les patients.

Al. 1 : *IG eHealth* et *PH CH* dénoncent l'imprécision des termes et définitions utilisés dans l'art. 9. Ils demandent en outre que l'al. 1 soit complété d'une lettre à la teneur suivante : « que les données enregistrées dans le dossier électronique du patient ont un cycle de vie indépendant de celui des données primaires saisies par les professionnels de la santé ». *ISSS* demande que l'al. 1 soit complété d'une let. d en référence à la let. c. En effet, le texte ne spécifie aucune exigence ni de bonne tenue des données ni de preuve de leur intégrité, une lacune à combler par des dispositions à l'image des exemples concrets trouvés dans d'autres lois (par ex. l'ordonnance concernant la tenue et la conservation des livres de comptes (Olico), art. 3). En l'occurrence, il s'agit de sauvegarder les données du dossier électronique du patient de telle manière qu'il soit possible de vérifier leur intégrité, c.-à-d. de déceler si elles ont été modifiées ultérieurement (p. ex. par un utilisateur ou suite à un dysfonctionnement technique ou une utilisation abusive/cyberattaque).

Al. 1, let. a : La *CDS* et 18 cantons[32] sont d'avis que la destruction systématique des données médicales au bout de dix ans n'est ni dans l'intérêt des patients, ni sensée dans l'optique d'un suivi des cas traités médicalement. La *CDS* et 8 cantons[33] préconisent de donner au patient la possibilité de fixer une limite supérieure à dix ans pour la durée de conservation de ses données. *ZH* et *ZAD* souhaitent que les dispositions relatives à la durée de conservation des données soient revues et corrigées. Le délai par défaut de conservation des données doit être significativement prolongé (par ex. à vie). Huit participants[34] signalent la nécessité de clarifier à partir de quand le délai de dix ans commence à courir. Outre la question du début du délai, *ZG*, *KDSBSON*, *DSBAG* et *privatim* observent qu'il convient aussi d'ajouter à la let. a l'obligation d'aviser le patient avant la destruction de ses données. D'après *HÄ CH* et *ÄTG*, le médecin traitant (médecin de famille) doit également être avisé en temps utile d'une destruction prévue des données de son patient. D'après six cantons[35], cette réglementation ne respecte pas l'art. 40, al. 1 de la loi fédérale sur les produits thérapeutiques (LPTh), qui prescrit l'archivage pendant 30 ans des données relatives à l'utilisation de sang ou de produits sanguins.

Onze participants[36] demandent la suppression de la let. A. *VAKA* rappelle qu'il faut également supprimer les explications qui s'y rapportent ainsi que les autres mentions d'un délai fixe d'expiration des documents. *Economiesuisse* déclare à ce sujet que toutes les données concernant la santé et la sécurité du patient doivent être saisies sans exception dans son dossier électronique. *Insel* fait remarquer que le délai maximum de dix ans est inopportun et diverge en outre des délais de conservation cantonaux. *BRH* se réfère également aux dispositions cantonales et demande que le délai de conservation soit

[32] AI, BL, GL, OW, UR, LU, SZ, BS, SH, ZH, ZG, TG, FR, GE, VS, VD, JU, NE
[33] BL, GL, OW, UR, LU, SZ, SH, TG
[34] AG, AR, TG, ZG, La Poste, KDSBSON, DSBAG, privatim
[35] FR, GE, VS, VD, JU, NE
[36] economiesuisse, Bleuer, Insel, K3, VZK, SBC, BS, NW, VAKA, SUVA, medshare

porté à dix ans après dernière consultation, par analogie avec la législation bernoise. *K3* et *VZK* observent que cette réglementation contrevient aussi à celle du canton de Zurich. *AG* fait savoir que le délai de dix ans pour les données d'importance thérapeutique dans le dossier électronique du patient (système secondaire) est compatible avec les dispositions régissant la conservation des dossiers médicaux dans le système primaire, la loi argovienne sur la santé prévoyant également un délai de conservation de dix ans pour ces dossiers. *La Poste* demande enfin que le patient puisse décider lui-même de la destruction de ses données sans devoir se conformer aux délais de conservation cantonaux. *NW* fait valoir que même sur le plan de la protection des données, la tenue séparée des données n'apporte aucun avantage, vu que les données particulièrement sensibles sont de toute façon déjà enregistrées dans le système KIS par les gros prestataires. La tenue séparée des données doit être remplacée par des mesures techniques de sécurité. *K3* et *VZK* jugent inopportun que les données soient supprimées du dossier électronique du patient au bout de dix ans, vu que ces dossiers électroniques de patients doivent idéalement rester en service toute une vie. *H+*, l'*ASI*, la *FSAS* et *SWOR* sont du même avis et pensent que nos concitoyens devraient disposer de leur dossier toute leur vie pour qu'il puisse être réactivé sur demande. À la place de cette suppression d'office, ils proposent que les données soient détruites sur préavis à la condition qu'il n'y ait pas eu d'accès au dossier électronique du patient pendant dix ans, ou suite à une suppression du dossier ou au décès du patient. La réglementation doit correspondre à celle prévue à l'art. 20 pour l'ensemble du dossier électronique du patient. *STSAG* plaide pour que les patients décident seuls de la suppression et de la conservation de leurs données ou que ces dernières soient automatiquement supprimées après dix ans d'inactivité. *Santésuisse* attire l'attention sur le fait que la limitation de durée risque d'entraîner une perte de données aux conséquences médicales potentiellement négatives. *KSOW* se réfère à l'obligation de supprimer les données saisies par les professionnels de la santé après dix ans et demande si d'autres données sont également concernées. Il souligne que des données de santé dotées d'une échéance plus longue (par ex. des maladies chroniques) ne peuvent pas être purement et simplement supprimées après dix ans. Le délai de conservation des données en question doit être fixé de cas en cas.

Six cantons[37] proposent l'énoncé suivant pour la let. a : « […] sont conservées jusqu'à la suppression du dossier électronique du patient, même si ceux-ci sont supprimés dans le système primaire après le délai légal de conservation des données spécifiés dans les lois cantonales ». *HÄ CH* et *ÄTG* se prononcent pour que le délai de dix ans soit augmenté à quinze ans au minimum, voire plus. *IG eHealth* et *PH CH* proposent l'énoncé suivant pour la let. a : « que le patient soit avisé si des données saisies par un professionnel de la santé dans le dossier électronique du patient n'ont pas été consultées depuis dix ans ». *PharmaSuisse* recommande de traiter toutes les données du dossier électronique du patient sur un pied d'égalité et donc de compléter la lettre a comme suit : « […] détruites au bout de dix ans, sauf si cette possibilité a été exclue par le patient ». Par voie de conséquence, la possibilité suivante doit être incluse comme option dans l'art. 3 : « i. refuser la destruction automatique, au bout de dix ans, des données saisies dans le dossier électronique du patient telle que prévue à l'art. 9, al. 1, let. a ». *SCH* propose la modification suivante de la let. a : « […] peuvent être détruites au bout de dix ans ». *Moeri* demande, quant à lui, le remplacement de la destruction prévue au bout de dix ans par une suppression implicite en application de l'art. 20 al. 1. Ce délai ne doit valoir que pour le système primaire, une solution qui a également les faveurs de *BE*. *HL7*, *IHE*, *BINT*, *Bleuer* et *SG* déclarent que la décision de supprimer ou non les données doit appartenir au patient. Le paradigme de la souveraineté finale sur les données n'autorise pas leur destruction automatique par les exploitants au bout de dix ans. De l'avis de *SG*, les communautés doivent garantir que les données saisies dans le dossier électronique du patient sont supprimées au bout d'un délai librement choisi par le patient, qui peut décider que les données seront stockées indéfiniment/à vie. *La Poste* propose la possibilité (pour le patient/le médecin de famille) de supprimer manuellement les documents devenus caducs. Un stockage permanent assorti de l'option de configurer les délais de conservation peut également être envisagé à la place. *Physioswiss* souligne que des données médicales importantes doivent rester à disposition jusqu'à ce que le patient en autorise la destruction. Le patient peut se voir proposer de choisir un délai de conservation pour ses données au moment d'ouvrir son dossier électronique. La conservation des données doit par ailleurs être garantie au-delà de l'existence d'une communauté, une préoccupation partagée par la *FMH*. *LUKS* demande

[37] FR, GE, VS, VD, JU, NE

que les documents déposés dans le dossier électronique du patient y restent à son décès, sauf opposition du patient. *Tessaris* déclare que les données saisies par des professionnels de la santé dans le dossier électronique du patient doivent être détruites, ou rendues en permanence inaccessibles, au terme de la durée fixée par le professionnel de la santé traitant d'entente avec le patient. La *FMH* estime que la disposition énoncée à la let. a est contraire à l'esprit et au but du dossier électronique du patient et propose d'instaurer l'obligation de contacter le patient avant toute suppression de données. Une telle suppression ne peut avoir lieu que si le patient l'autorise ou s'il supprime le dossier. Pareillement, *VGIch* demande que l'obligation de conserver les données ne prenne fin qu'à la suppression du dossier sur demande du patient ou à son décès. *TI* considère que la let. a doit être modifiée de telle sorte que les données sont conservées jusqu'à la suppression du dossier électronique du patient. La *SSIM* déclare que le principe d'une destruction des données au bout de dix ans n'a aucun sens et propose que les données ne soient supprimées que sur demande du patient au bout d'un délai de conservation minimum (variable selon le canton et le type de données).

Al. 1, let. b : *Tessaris* demande que la let. b soit adaptée à sa proposition de modification de la let. a. Les données doivent être mises à disposition même au-delà de la durée fixée par le professionnel de la santé traitant. *SCH* propose que la notion de « destruction » soit remplacée par la définition suivante : « […] Les données doivent être supprimées de manière irréversible par des procédés conformes aux progrès techniques. » *PharmaSuisse* recommande l'ajout à l'al. 1 d'une lettre dont le texte est le suivant : « le patient est informé au moins trois mois à l'avance d'une destruction de données du dossier électronique du patient en application de la let. a ». D'après la *FMH*, il faudrait faire en sorte que les données des patients puissent être rétablies au lieu d'être purement et simplement supprimées. Ainsi, elles seraient à nouveau disponibles si le patient revenait sur une décision de révocation de son consentement. En outre, la suppression ne peut concerner que les données enregistrées auprès de la communauté ainsi que les liens éventuels. *medshare* souhaite une reformulation de la let. b pour y inclure une disposition à définir régissant l'héritage numérique. Les données ne seraient alors effectivement supprimées qu'après le décès du patient, et ce seulement si aucun héritier n'exprime, dans un délai à définir, le souhait de maintenir le dossier. Sept cantons[38] demandent la suppression de la let. b.

Al. 1, let. c : *HL7*, *IHE* et la *SSIM* souhaitent que le texte précise ce que sont des lieux de stockage prévus exclusivement à cet effet. Si l'on entend par là une séparation physique, celle-ci doit être définie. La question de principe qui se pose est de savoir si une ordonnance doit se situer au niveau serveur ou au niveau technologie de stockage. La séparation physique d'un dossier virtuel en des infrastructures virtuelles est une contradiction en soi. *IG eHealth* et *SCH* sont incertains quant au sens qu'il faut donner au terme « exclusivement », vu qu'il peut être interprété comme une duplication du lieu de stockage, ce qui ne conduirait pas au but recherché. Ils proposent que le mot « exclusivement » soit supprimé de la let. c : *VGIch* demande quant à lui que l'on définisse les « lieux de stockage prévus […] à cet effet » et ce qu'on entend par « cas exceptionnels reposant sur des raisons techniques » (voir rapport explicatif). Un avantage substantiel des référentiels de données validés à l'IHE disparaîtrait dans les hôpitaux qui autoriseraient un enregistrement direct de documents locaux. Une communauté de référence doit être expressément autorisée à tenir un référentiel de données secondaire central contenant les copies du système primaire. Il convient aussi d'établir une liste exhaustive de cas exceptionnels pour raisons techniques et d'autoriser, à titre de solution de remplacement, l'enregistrement direct de documents locaux dans les référentiels de données des prestataires. *medshare* souhaite également que l'on précise les « lieux de stockage » prévus exclusivement à cet effet.

VAKA prévient que cette restriction éliminera les possibilités d'exploiter des processus fonctionnels utiles et occasionnera des surcoûts énormes dus aux redondances. Elle est aussi contraire au principe de gestion décentralisée des données sur lequel repose le modèle de base. Dans ce contexte, toutes les communautés et leurs modèles d'activité seront privés d'importants aspects et bénéfices de l'utilisation dirigée de ces processus. *VAKA* demande la suppression pure et simple de la let. c, y compris

[38] FR, GE, VS, VD, JU, NE, TI

les dispositions qui s'y rapportent dans les Critères techniques et organisationnels. Huit autres participants[39] se joignent à VAKA pour demander la suppression de la let. c. *ZG*, *NW*, *ZH*, *SZ* et *ZAD* observent que même sur le plan de la protection des données, la tenue séparée des données n'apporte aucun avantage, vu que les données particulièrement sensibles sont de toute façon déjà enregistrées dans le système primaire des prestataires. La tenue séparée des données doit être remplacée par des mesures techniques de sécurité qui doivent être compatibles avec un système primaire afin que celui-ci puisse aussi être utilisé comme lieu de stockage pour le dossier électronique du patient. *LUKS* fait remarquer que la let. c rend le système inutilement plus cher. Le dossier électronique du patient a toujours été défini comme un dossier virtuel avec des référentiels de données décentralisés. Des exigences doivent être définies pour ces référentiels. *KSSG* demande une reformulation qui permette une séparation logique des documents du dossier électronique du patient d'une part, et des autres documents d'autre part. *K3* et *VZK* font valoir que les hôpitaux tiennent déjà des dossiers médicaux électroniques. Restocker les mêmes données dans un autre lieu de stockage crée des doublons inutiles. Il est suffisant d'enregistrer les clés d'accès aux données dans des lieux de stockage distincts, tandis que la lecture des données elles-mêmes s'effectue depuis leurs dossiers internes à l'hôpital. *Privatim* cite un entretien téléphonique avec l'OFSP dont il ressort qu'aux termes de cette disposition, les données des systèmes primaires ne peuvent être enregistrées que dans les référentiels de données se trouvant dans les communautés, de sorte qu'il est exclu d'enregistrer des données du système primaire directement dans le dossier électronique du patient. Cette disposition manque de clarté. Et comme il s'agit d'un point essentiel, il devrait être formulé plus clairement pour pouvoir être compris directement à la lecture du texte édicté, sans référence au rapport explicatif. *HIN* et *BINT* jugent exagérée la mise à disposition d'unités de stockage réservées aux seuls dossiers électroniques des patients. Il suffit d'une séparation logique et toujours transparente des données. La let. c doit être adaptée en conséquence : « […] électroniques sont enregistrées dans des lieux de stockage prévus à cet effet de telle manière qu'elles puissent à tout moment être séparées des autres données (séparation logique) ». Des adaptations des passages correspondants du rapport explicatif sont également nécessaires. Pareillement, *USB* pense que la possibilité d'une séparation logique des données secondaires du DEP, mentionnée dans le rapport explicatif, doit aussi être explicitée dans l'ordonnance, d'où sa proposition de modifier comme suit la let. c : « […] électroniques sont enregistrées dans des lieux de stockage physiquement ou logiquement séparés ».

Al. 2 : *IG eHealth*, *PH CH* et *La Poste* critiquent l'énoncé allemand : « Sie haben auf Verlangen […] » (« A la demande du patient, elles doivent : ») et demandent qui est désigné par ce « sie ». *IG eHealth* et *PH CH* préconisent la formulation : « Die Gemeinschaften haben auf Verlangen […] », correspond déjà au texte français (« A la demande du patient, les communautés doivent: ») *AI* rappelle à ce propos que l'enregistrement des données et les processus administratifs qui lui sont liés doivent être adaptés aux dispositions légales sur la protection des données. *BE* et *STSAG* sont d'avis que la destruction sélective de données du patient dans son dossier électronique doit être effectuée entièrement par le patient et ne peut pas être exigée des professionnels de la santé. Le patient dispose des instruments pour le faire, il peut attribuer aux nouvelles données le niveau de confidentialité « données secrètes », puis leur réattribuer d'autres niveaux de confidentialité ou les supprimer. Ils proposent que l'al. 2 soit reformulé comme suit : « Les communautés doivent permettre au patient de limiter la disponibilité des données visée à l'al. 1 à dix ou à vingt ans ». Selon la *CDS* et huit cantons[40], il s'agit de parvenir à rallier les prestataires au dossier électronique du patient sans prendre le risque de les dissuader de son usage en leur imposant des règles compliquées. Les modalités de remplissage et de gestion des dossiers par les professionnels de la santé doivent être fixées de manière à être compatibles avec les processus thérapeutiques.

Al. 2, let. a : Six cantons[41] souhaitent la suppression de la let. a, car cette dernière concerne les professionnels de la santé et leur système primaire et non la communauté. *Insel* considère que la let. a doit être supprimée et la responsabilité transférée aux patients. *KSSG* et *VGIch* doutent fortement que l'on dispose des ressources nécessaires pour demander aux patients si un document doit ou non être publié.

[39] K3, VZK, LUKS, FMH, ZG, NW, ZH, ZAD
[40] BL, GL, LZ, OW, UR, NW, SH, SZ
[41] FR, GE, VS, VD, JU, NE

KSSG souligne que les patients peuvent eux-mêmes classer « secrets » certains documents et d'après *VGIch*, les systèmes primaires permettent d'effectuer ces manipulations sans grande adaptation technique de leurs fonctions logicielles. Les deux participants demandent la suppression de la let. a. *La Poste* demande de quelles données il est question et selon quels critères ces données sont définies. La réglementation est pléthorique au point d'être inapplicable. Une autre possibilité serait que le patient classe « secrètes » toutes les données enregistrées dans son dossier électronique par les professionnels de la santé. À l'instar de *La Poste*, *medshare* demande que la notion de « données » soit précisée, une remarque qui vaut du reste pour les autres mentions du terme dans les textes du projet d'ordonnance. *IG eHealth* et *PH CH* proposent que la let. a soit modifiée comme suit : « enregistrer tous les nouveaux documents, à partir d'un moment déterminé par le patient, dans son dossier électronique en leur attribuant le niveau de confidentialité "données secrètes" ou "données sensibles" ».

Al. 2, let. b : Dix-huit participants[42] réitèrent pour l'al. 2, let. b leurs commentaires relatifs à l'al. 1, let. a. *IG eHealth* et *PH CH* relèvent la nécessité de supprimer la let. b suite à leur proposition concernant la let. a. *KSSG* demande également la suppression de la let. b. Le patient doit pouvoir enregistrer ses documents dans l'espace mémoire mis à sa disposition par le dossier électronique s'il souhaite prolonger le délai de conservation. *La Poste* demande si cette obligation est faite à la communauté (le texte allemand ne le précise pas, contrairement au français) ou au professionnel de la santé, et dans ce dernier cas, comment les choses sont censées se passer. S'il ne s'agissait pas de la communauté, des précisions seraient nécessaires. *NW* propose que le patient se voie offrir la possibilité de garder ses données jusqu'à révocation. *Moeri* qualifie la let. b d'obsolète. *SUVA* critique notamment le mécanisme prévu par les let. a et b, qui nécessite une intervention active de la part du patient, et demande que ces deux lettres soient supprimées.

Al. 2, let. c : *K3*, *VZK*, *VGIch* et *Insel* réitèrent la position qu'ils ont prise à propos de la let. a et demandent donc la suppression de la let. c. Pour *VAKA*, rien ne permet de conclure à l'Usecase. Le maintien du niveau de confidentialité « données secrètes » produit le même effet sans gros effort, si bien que la let. c peut être supprimée. *IG eHealth* et *PH CH* demandent quelle est la différence entre « supprimer » et « détruire ». *SCH* relève lui aussi que la signification de « détruire » n'est pas claire. *IEGH* et *PH CH* proposent de modifier l'énoncé comme suit : « […] supprimer de son dossier électronique des données déterminées le concernant ». *SCH* propose l'énoncé suivant : « […] supprimer de manière irréversible de son dossier électronique des données déterminées le concernant ». *SMCF* fait savoir qu'une telle suppression ne devrait pas être possible, seule une désactivation est envisageable.

Al. 3 : *LUKS* et la *SSIM* font valoir que le DFI et l'OFSP ont des compétences très étendues en la matière. Alors que *LUKS* demande la fin de la délégation au DFI et à l'OFSP et la reprise des principales exigences dans l'ordonnance, la *SSIM* se dit partisane de créer une possibilité de contrôle ou de recours qui soit indépendante de l'administration. L'*ASI*, *FSAS*, *SWOR* et *Physioswiss* saluent les conditions cadres essentielles fixées à l'al. 3. Les bases prises en considération correspondent à des normes internationales qui assurent une régulation fiable de l'échange électronique de données. L'*ASI*, *FSAS* et *SWOR* soulignent en outre la nécessité de mettre en place un centre de compétences en sémantique. C'est le seul moyen d'implémenter un usage judicieux des terminologies de référence (SNOMED CT). L'*ASI* et *SWOR* renvoient ici à leur prise de position sur l'ODEP-DFI, al. 3 : Métadonnées. *La Poste* souhaite l'introduction en premier lieu du terme de « profils d'intégration » et demande un glossaire contenant les principales définitions. *LUKS* et la *FMH* font remarquer que la tenue d'un historique a des implications pour la responsabilité civile des professionnels de la santé. Elle doit impérativement servir à établir quelles données ont été consultées par un professionnel de la santé au moment de son accès, et il faut en tenir compte dans la poursuite des investigations. *VGIch* fait valoir que les données de l'historique doivent également inclure les accès des administrateurs ou des personnes travaillant pour les services d'assistance.

La *FMH* est d'avis qu'il faut renoncer à régler les détails techniques au niveau de l'ordonnance et renvoie à sa prise de position dans les remarques générales, d'où sa demande de supprimer les let. b à d de

[42] Insel, AI, AR, BL, CDS, GL, OW, UR, LU, SZ, SH, SG, TG, ZG, ZH, ZAD, FMH, Physioswiss

l'al. 3.

Al. 4 : Six cantons[43] signalent une erreur de traduction en français. Le DFI pourrait renoncer à traduire un document source dans une langue nationale si celui-ci est en anglais, mais pas à le traduire dans les autres langues nationales officielles s'il est déjà rédigé dans l'une des langues officielles. L'al. 4 doit être reformulé ainsi : « […] à les faire traduire dans les langues officielles ». La *FMH* demande que les prescriptions soient obligatoirement disponibles dans les trois langues nationales ou en anglais. *SBC* demande la suppression de l'al. 4.

Al. 5 : *LUKS* et la *SSIM* réitèrent leur position relative à l'art. 9, al. 3. Pareillement, la *FMH* déclare que la compétence de délégation de l'OFSP doit être abrogée au profit d'une réglementation par une ordonnance du Conseil fédéral. À défaut, il convient d'aménager une possibilité de contrôle ou une voie de recours indépendante de l'administration. *KDSBSON*, *DSBAG*, *privatim* ainsi que *ZG* et *BE* observent qu'une prescription à caractère potestatif ne mène nulle part. Il faudrait réévaluer les progrès techniques à intervalles périodiques (à déterminer) et procéder aux réajustements appropriés lors de changements susceptibles de produire une situation critique. Ils proposent que l'al. 5 soit modifié comme suit : […] (OFSP) vérifie régulièrement que les prescriptions de l'al. 3 sont compatibles avec l'état de la technique et procède à des adaptations en cas de divergences susceptibles de conduire à une situation critique. *K3*, *VZK* et *ZH* préféreraient que seul le DFI puisse modifier les dispositions de l'ordonnance ou de ses annexes, aussi *K3* et *VZK* proposent-ils de modifier l'al. 5 comme suit : « Le DFI peut adapter les prescriptions […] ». *HIN* fait remarquer que les profils d'intégration et les formats d'échange à l'introduction ne sont pas complets. Il faudrait introduire un processus de changement et de suivi des versions dans lequel les adaptations sont harmonisées avec les participants et les exploitants de manière à garantir à tout moment l'interopérabilité et l'échangeabilité des données. HIN recommande que l'al. 5 soit adapté comme suit : « Ce faisant, il importe en particulier d'assurer une harmonisation des adaptations avec les exploitants, un suivi des versions et leur rétrocompatibilité de manière à garantir à tout moment l'échangeabilité des données ».

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.	

VAKA signale que plusieurs portails d'accès (destinés aux patients) sont mentionnés. Il demande une déclaration plus précise ou une fusion des portails, ou au moins l'avertissement qu'il peut s'agir de deux GUI/masques de login différents sur un même portail. *VAKA* demande en outre, tout comme *AG*, un emploi unifié des termes « données » et « documents » dans toutes les ordonnances. *AG* ajoute que la transparence sur le portail d'accès lui paraît très importante et qu'il salue la possibilité de télécharger des documents vers le système primaire pour s'acquitter de l'obligation de documentation. *La Poste* aimerait que le texte dise clairement si un portail d'accès pour professionnels de la santé est obligatoire et s'il faut un portail d'accès dédié aux professionnels de la santé et aux patients. *BFH* propose de référer d'emblée l'utilisateur aux Critères techniques et organisationnels en annexe pour lui faciliter la recherche des exigences. *HÄ CH* et *ÄTG* sont en faveur d'un portail d'accès pour professionnels de la santé qui mette toujours la clarté au premier plan, dans sa présentation comme dans la configuration des filtres. Un travail rationnel dans le quotidien n'est possible qu'à ces conditions. L'actualité et la qualité des données doivent primer la quantité. De l'avis d'*IG eHealth* et de *PH CH*, déléguer entièrement au DFI la définition des portails d'accès pour professionnels de la santé constitue ici une solution très complète. Des exigences minimales doivent être définies pour le portail d'accès. Dans leur commentaire sur l'art. 10, ils font en outre une proposition d'énoncé détaillée pour cet article. *K3* et *VZK* font valoir qu'un professionnel de la santé qui ne possède qu'un accès restreint doit s'en apercevoir immédiatement et renvoient à leur proposition d'amendement à l'art. 3, let. f.

SCH et *economiesuisse* constatent que les recommandations d'eHealth Suisse et le message relatif à la LDEP prévoyaient également l'accès aux données des patients par un portail externe. Or, la certification d'un portail d'accès externe ne figure plus dans les textes d'ordonnance actuels. La loi n'offre

[43] FR, GE, VS, VD, JU, NE

donc plus d'accès « light » au DEP par ex. aux communautés qui ne souhaitent pas faire fonction de communauté de référence. *Economiesuisse* déplore cette situation, *SCH* souligne qu'elle n'est pas profitable au développement de la cybersanté en Suisse et constitue un frein à l'innovation pour les « use cases » dans les domaines de la santé mobile (mHealth), de la responsabilisation du patient (empowerment) et pour le système de santé en général. La *SSIM* et *SBC* rappellent que des portails externes peuvent aussi être créés sous forme d'applications mobiles, qui offrent par ailleurs d'autres services innovants. Ils trouveraient regrettable que mHealth et eHealth évoluent en parallèle sans aucune concertation. Comme *SCH*, ils ajoutent que les portails externes apporteront une contribution essentielle à la responsabilisation du patient et que les nouveaux services de prestataires externes peuvent être une source d'innovation. *SBC* donne d'ailleurs un exemple de cas concret dans sa prise de position sur cette question. *HL7*, *IHE*, *SBC*, la *SSIM* et *economiesuisse* sont également d'avis que l'espace de confiance de la LDEP ne devrait pas être un système fermé réservé aux seuls prestataires de la communauté, car les portails externes certifiés qui sont innovants créent une valeur ajoutée pour les patients, les fournisseurs de services en ligne et au bout du compte aussi pour notre système de santé, notre économie et la Suisse en tant que pôle d'innovation. Six participants[44] font une proposition identique sous la forme d'un nouvel article 10bis intitulé « Portails d'accès externes ». Comme pour la nouvelle version proposée par *IG eHealth* et *PH CH* pour l'art. 10, nous invitons à lire les avis consultables en ligne pour l'énoncé exact au vu du gros volume qu'il représente.

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.

Six participants[45] estiment plus utile de donner une formulation générale abstraite aux objectifs prescrits au ch. 11 devant être remplis au niveau de la protection et de la sécurité des données. Il faut laisser aux communautés, aux communautés de référence et aux prestataires le soin de décider comment réaliser ces objectifs. En conséquence, l'art. 11 doit être entièrement remanié. *La Poste* propose la publication d'une liste des rôles attendus d'une communauté. On pourrait aussi envisager d'inclure un chapitre à ce sujet dans le rapport explicatif. *VAKA* et *AG* saluent l'idée d'un système de gestion de protection et de sécurité des données, le jugeant conforme au droit, mais observent qu'il occasionnera une charge pour les communautés. Ils souhaitent que le rapport explicatif suggère des moyens d'empêcher ce surcroît de charges, par ex. l'engagement par plusieurs communautés d'un mandataire indépendant en qualité de responsable de la protection des données. *AG* dénonce aussi le flou des formules utilisées pour décrire la procédure de cryptage. Celle-ci doit déjà être définie dans l'ODEP et pas seulement dans les Critères techniques et organisationnels. *SMCF* déclare qu'au vu de ces exigences, il paraît légitime de limiter le nombre de communautés en Suisse à une dizaine au lieu de 20 à 40. D'après *VGIch*, la compétence des communautés d'assurer la protection et la sécurité des données doit s'arrêter au point de transmission des prestations, c'est-à-dire à l'interface de recherche et de paramétrage des

[44] HL7, IHE, SBC, SSIM, economiesuisse, SCH
[45] ZH, NW, ZG, ZAD, K3, VZK

documents de l'institution affiliée. Ce point doit être réglementé par un alinéa supplémentaire dans l'art. 11. *VGIch* fait également remarquer que les objectifs fixés et réalisés dans le cadre des Critères techniques et organisationnels ne doivent pas influer sur les systèmes primaires, ou alors à un niveau ne dépassant pas les principes généraux de sécurité des données.

Al. 1 : La *FMH* rappelle l'obligation d'appliquer les dispositions de la loi sur la protection des données et met en garde contre toute réglementation excessive. *SQS* propose l'énoncé suivant pour l'al. 1 : « Les communautés doivent être certifiées conformément à l'art. 11 de la loi fédérale du 19 juin 1992 sur la protection des données. Elles doivent se doter d'un système de gestion de la protection et de la sécurité des données qui remplit les exigences de l'art. 4 al. 2 de l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD) et des directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (directives sur la certification de l'organisation et de la procédure) émises par le PFPDT le 19 mars 2014. Ce système comprend […] ». Leur commentaire contient aussi une autre proposition d'énoncé qui fait référence aux normes internationalement reconnues ISO 9001 et ISO/IEC. *OFAC* relève qu'en tant qu'organes cantonaux, les communautés seront soumises au droit de leur canton en matière de protection des données. Or, certaines notions importantes de la protection des données, telles que le SGPD et la procédure de certification, n'existent pas dans la plupart des législations cantonales. Il faut également noter que les disparités entre les législations cantonales sont très importantes. Les directives du PFPDT sur les exigences minimales qu'un système de gestion de la protection et de la sécurité des données doit remplir doivent s'appliquer à tous les types d'organisations. *Economiesuisse*, *SBC*, *HL7* et *IHE* demandent que les communautés puissent déléguer leur système de gestion de la protection et de la sécurité des données pour éviter que leurs coûts prennent inutilement l'ascenseur. Concrètement, ils demandent que l'al. 1 soit complété comme suit : « […] se doter ou déléguer l'exploitation d'un système de gestion […] éléments suivants : ».

Al. 1, let. a : *LUKS* demande la suppression de la let. a. Le profil exigé, les tâches et l'utilité du responsable de la protection des données sont mal définis. La *CDS* et six cantons[46] partagent cet avis et demandent avec six autres participants[47] que l'idée de nommer des responsables particuliers de la protection et de la sécurité des données soit abandonnée. *AI* conseille de ne pas mettre de mandataire indépendant sur cette tâche tant que le préposé à la protection des données a les capacités de s'en charger.

Al. 1, let. b et c : *ISSS* propose d'apporter la précision suivante à l'énoncé de la let. b : « b. un système de détection proactive et de gestion des incidents du domaine de la sécurité contre les attaques et contre les pannes », et de modifier comme suit la let. c : « c. un registre des lieux de stockage des documents, des autorisations et des procédures de sauvegarde et de stockage sécurisé des données ».

Al. 1, let. d : *KDSBSON* et *DSBAG* observent que durant l'élaboration de la législation relative au dossier électronique du patient, il n'a jamais été question que les systèmes primaires soient directement liés au dossier. Il était plutôt prévu de le lier aux systèmes secondaires, comme l'a aussi remarqué *FR*. Ils demandent que l'on examine s'il est vraiment souhaitable de lier le dossier aux systèmes primaires, une mesure qui pose des problèmes de droit de la protection des données et qu'il conviendrait donc de rejeter. Si cet objectif est néanmoins poursuivi, les systèmes primaires doivent remplir les critères de protection des données et de sécurité de l'information exigés par la législation sur le dossier électronique du patient. *privatim* renvoie à ses déclarations à ce sujet dans les remarques générales. *SQS* fait remarquer que le système de gestion de protection des données selon l'OCPD, le système de management ISO 9001 et le système de management de la sécurité des informations ISO/IEC 27001 comprennent chacun de ces systèmes secondaires et pas seulement les systèmes primaires liés aux communautés. On peut par conséquent renoncer à exiger que les systèmes primaires soient expressément nommés si l'une de ces normes de certification est choisie pour certifier une communauté ou une communauté de référence. *SQS* recommande par conséquent la suppression de la let. d. D'après *BE*,

[46] BL, GL, LU, OW, UR, SZ
[47] ZAD, NW, ZH, ZG, K3, VZK

l'énoncé suggère que les systèmes primaires sont liés « directement » au dossier électronique du patient alors qu'en fait, ils ne lui sont liés qu'indirectement par le lieu de stockage des documents (copie synchronisée). La formulation suivante convient donc mieux pour la let. d : « d. un registre des systèmes primaires reproduits ». La *FMH* demande ce que signifie la let. d et si cette exigence est réaliste et raisonnable. D'après elle, la let. d doit être supprimée ou remplacée par un répertoire des fichiers secondaires. Six cantons[48] trouvent comme elle que le texte de la let. d n'est pas clair. Les données que doit contenir le registre doivent être précisées, par ex. dans le rapport explicatif. Il n'est pas possible de mettre à disposition une liste des ordinateurs et logiciels utilisés par des milliers de professionnels de la santé. La let. e doit donc être supprimée. *NE* ajoute qu'il faudrait au moins compléter l'ordonnance ou le rapport explicatif par des précisions sur les données que doit contenir le registre des systèmes primaires. *ISSS* propose que l'énoncé de la let. d soit précisé comme suit : « […] systèmes primaires qui ont, ou peuvent obtenir, un accès direct ou indirect aux données/à la communication ». *Lovis* souhaite que l'on précise si le répertoire des systèmes primaires liés contient des organisations ou des systèmes.

Al. 1, let. e et f : *CURAVIVA*, *Insos* et *TG* trouvent cette norme de (sous-)délégation trop vague. Elle devrait indiquer le contenu, ou du moins les éléments de base, des normes de protection et de sécurité des données à observer par les institutions de santé affiliées, les professionnels de la santé qui y travaillent, le personnel et les tiers. Il y va de la lisibilité de la loi, de son application correcte par les acteurs concernés et en fin de compte, de la sécurité du droit. *senesuisse* juge insuffisantes les dispositions des let. e et f. Il faut définir plus clairement à l'attention des communautés les exigences qu'elles doivent fixer aux institutions de santé, aux professionnels de la santé, au personnel et aux tiers. Il faut soit compléter le texte de l'ordonnance, soit préformuler une aide à l'exécution au contenu approprié.

Al. 2 : *HL7* et *IHE* se disent en faveur d'un délai entre la survenue et le signalement de tels incidents, tout comme *medshare* qui demande que l'on définisse une périodicité. *La Poste* demande quelles sont les exigences imposées en matière de notification et recommande que cette disposition soit adaptée à la nouvelle directive de l'UE sur la protection des données. Pour l'*OSP,* il ne ressort pas clairement du texte allemand si cette obligation de signaler a un caractère contraignant et si l'on a défini une catégorie d'incidents réputés importants pour la sécurité. Elle demande une formulation claire et compréhensible. La *FRC* demande également que l'on clarifie les modalités et surtout que l'on précise le délai imparti pour signaler des incidents dans le système. La réaction doit être aussi immédiate que possible.

SQS fait valoir que les organismes de certification ont pour compétence exclusive de certifier les communautés et les communautés de référence conformément aux prescriptions et de leur faire passer chaque année un audit selon la procédure de certification. Ils n'ont aucun rôle à jouer dans les activités opérationnelles durant les périodes entre les audits. Les incidents doivent par conséquent être signalés uniquement à l'OFSP et non aux organismes de certification. En vertu de l'art. 36 al. 1 let. c et de l'art. 37 al. 3 let. a de cette ordonnance, l'OFSP peut faire intervenir les organismes de certification si, suite au signalement d'incidents significatifs affectant la sécurité, un contrôle par l'organisme de certification est nécessaire pour empêcher des violations imminentes de la législation sur la protection et la sécurité des données. *OFAC* relève que les services du PFPDT sont rattachés à la Confédération afin de garantir leur indépendance. C'est normalement à la Confédération qu'il revient d'apprécier la gravité d'un incident et de décider des mesures à faire prendre par les parties intéressées. Il en est de même pour le DFI et l'OFSP.

Al. 3 : D'après la *SSIM,* il faut que les exigences de protection et de sécurité des données soient conformes à la loi sur la protection des données et n'aillent pas au-delà. *LUKS* déclare lui aussi qu'il faut se garder d'une surréglementation, que la loi sur la protection des données s'applique ici comme ailleurs. Une disposition supplémentaire est inutile, l'al. 3 doit donc être revu. *ISSS* et *Tessaris* proposent que l'al. 3 soit complété comme suit : « […] à la protection et à la sécurité des données et les adapte à l'évolution du niveau de menace ». Comme dans son commentaire relatif à l'al. 1, *SQS* fait remarquer que les exigences pour le choix d'une certification selon l'OCPD sont définies dans les « Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir » émises

[48] GE, VS, VD, JU; FR, NE

le 19 mars 2014 par le PFPDT, et que seules les exigences supplémentaires doivent donc être retenues. *OFAC* estime que les exigences relatives à la protection des données doivent être fixées par un département fédéral et non par les services du PFPDT. Une fois les exigences fixées se pose la tâche de contrôler leur observation. Les services du PFPDT sont rattachés à la Chancellerie fédérale, ce qui garantit la neutralité des contrôles et des surveillances exercés. Une surveillance exercée par l'OFSP ne sera pas neutre, en particulier à l'égard des services de recherche centralisés dont l'OFSP restera juridiquement responsable.

Al. 4 : *KDSBSON*, *DSBAG*, *privatim* ainsi que *BE* et *FR* considèrent que le droit sur la protection des données rend impérative une telle disposition vu que les données de santé sont des données personnelles particulièrement dignes d'être protégées, compte tenu aussi du risque de favoriser la création de profils de personnalité dans le cadre du dossier électronique du patient. Il convient aussi d'examiner si le siège des entreprises et le lieu de travail de tous les collaborateurs impliqués ne devraient pas être obligatoirement situés en Suisse. Dans le même esprit, *TG* observe qu'il faut éviter tout traitement de données à l'étranger et que l'alinéa doit être complété en conséquence. *ISSS* soumet une proposition concrète d'énoncé : « Les lignes de données et les dispositifs de connexion, de transmission, de stockage et de traitement des données doivent être situés en Suisse et régis par le droit suisse. » HIN comprend et soutient l'intention de l'al. 4 et ajoute que les personnes juridiques devraient être explicitement mentionnées, ce qui l'amène à proposer l'énoncé suivant : « Les prestations de stockage de données doivent être fournies par des personnes juridiques situées en Suisse et régies par le droit suisse. Les dispositifs de stockage de données doivent […] ».

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.	

CURAVIVA, *Insos* et *AG* saluent la mise en place de services d'assistance pour professionnels de la santé. L'*ASI*, *SWOR* et *Physioswiss* considèrent un service compétent d'aide aux professionnels de la santé comme un facteur décisif de succès dans la réalisation du dossier électronique du patient. *senesuisse* salue également la création de tels services d'assistance, mais observe que leur financement doit être assuré sur une longue durée et que les aides financières prévues sont insuffisantes pour le garantir. *HÄ CH* et *ÄTG* font valoir que des services hotline peuvent très vite gaspiller beaucoup d'argent et de temps. Il faut prévoir suffisamment de capacités, surtout dans la phase initiale. De plus, les frais d'exploitation devraient être idéalement proches de zéro ou, à tout le moins, plafonnés. Ces frais supplémentaires doivent être pris en compte et couverts dans le tarif. *HÄ CH* et *ÄTG* soulignent que les adaptations de systèmes primaires, les interfaces, la certification, les hotlines, etc. ne doivent pas être des cas d'étude de rentabilité (« business cases »). *BINT* demande que l'art. 12 soit suivi d'un nouvel article rédigé comme suit : « Les communautés garantissent un accès intercommunautaire permanent et gratuit à leurs données sur autorisation du patient ». *KSSG* reproche à ce service d'assistance son profil très flou. Certaines de ses caractéristiques sont bien mises en évidence dans les Critères techniques et organisationnels, d'autres – essentiellement organisationnelles – restent entièrement à définir. *BS* fait remarquer que les communautés doivent rester libres de tenir un ou plusieurs services d'assistance pour les professionnels de la santé ou les patients. Il faut donc parler de l'obligation de « désigner au moins un service d'assistance », à préciser dans les art. 12 et 19.

L'*OSP* invite à s'interroger s'il ressort clairement du texte de l'ordonnance que les prescriptions figurant dans le rapport explicatif, comme celle de devoir « être assujettis à une obligation analogue au secret médical », sont effectivement contraignantes.

Section 2 : Communautés de référence

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.

La *CCM*, *KAeG SG*, *BüAeV* et *GAeSO* déplorent que la question du financement de l'information en relation avec les questions des patients ne soit pas réglée. Il y a lieu de supposer que les communautés de référence répercuteront ces frais sur les professionnels de la santé qui leur sont affiliés, par ex. par les cotisations des membres. Selon le principe de causalité, les coûts liés à l'information des patients devraient en fait être partagés par ces derniers. Tous quatre demandent l'ajout de la lettre supplémentaire suivante à l'al. 1 : « e. Bases de calcul et utilisation des cotisations à verser. » *K3*, *VZK* et *VAKA* constatent que les informations à communiquer aux patients sont décrites très longuement, avec un luxe de détails, aussi bien dans l'art. 14 que dans les Critères techniques et organisationnels. Ce n'est guère le but d'une information. Ils demandent qu'elle soit revue ou remplacée par une spécification simplifiée, plus pragmatique. *K3* et *VZK* ajoutent que la recommandation de mesures de protection et de sécurité des données n'apporte rien aux patients. Ils préfèrent que ces prescriptions soient implémentées sous forme de paramètres par défaut du système. *FRC* fait remarquer ici que le patient devra aussi être informé si son médecin, son pharmacien, etc. participent ou non au dossier électronique et quelles pourront en être les conséquences pour lui. *Santésuisse* pense que c'est au fournisseur de moyens d'identification (IDP) ou au service d'inscription de se charger d'informer le patient. Il est raisonnable à son avis que le patient soit informé des conséquences du dossier électronique au moment d'ouvrir son dossier ou de soumettre sa demande. Cela lui évite de devoir aller trouver sa communauté de référence exprès pour cela. L'*OSP* demande l'ajout de trois alinéas supplémentaires à l'art. 14 : « Al. 3 : Elle s'assure que les informations visées à l'al. 1 ont été données et a l'obligation d'en faire la preuve. Al. 4 : Elle informe régulièrement les patients par écrit des traitements de données effectués. Al. 5 : Elle veille à ce que les modifications des droits d'accès des professionnels de la santé selon l'art. 9, al. 3 et l'art. 10, al. 2, let. b, ch. 1 LDEP soient consignées dans un historique ».

Al. 1 : Pour l'*ASI*, *FSAS* et *SWOR*, la compétence d'une communauté de référence d'informer suffisamment les patients doit être vue d'un œil critique. La communauté de référence doit veiller à ce que la compétence professionnelle pour ces informations aux patients puisse être assurée. *KSSG* et l'*UDC* souhaitent que l'on définisse plus précisément comment l'information doit avoir lieu. *KSSG* montre en outre à l'aide d'un exemple chiffré qu'une information directe par les collaborateurs peut devenir très coûteuse, et demande que la forme que prendra l'information du patient soit décrite dans les dispositions d'exécution ou dans les critères techniques et organisationnels. D'après six cantons[49], il importe également d'informer le patient des conséquences d'une révocation : les données seraient perdues et le patient ne pourrait plus récupérer son anamnèse médicale en cas de nouveau consentement. Ils proposent l'ajout d'une lettre à l'al. 1 : « e. la possibilité de révoquer le dossier et les conséquences d'une révocation ». La *FRC* propose quant à elle de compléter la let. c comme suit : « […] consentement, ou d'un non consentement, et la possibilité […] ». L'*OSP* regrette que le passage disant qu'une « révocation du patient ne devait lui causer aucun préjudice » ait été supprimé de la section 2, art. 3.3 LDEP. Elle propose que l'al. 1, let. c soit complété comme suit : « […] consentement, la possibilité de le révoquer et les conséquences possibles d'une révocation ». *CURAVIVA*, *Insos et TG* attirent l'attention sur l'obligation d'informer les représentants de patients incapables de discernement et proposent que l'al. 1 soit reformulé comme suit : « […] est tenue d'informer le patient et, le cas échéant, son représentant en particulier sur […] ». *CURAVIVA* et *Insos* insistent sur l'importance d'informer également les patients incapables de discernement. *HL7*, *IHE* et *Integic* font une proposition d'énoncé similaire : « […] est tenue d'informer le patient ou son représentant en particulier sur […] ». *senesuisse* reproche également à ces dispositions de ne faire aucune mention des patients devenus incapables de discernement. Et comme ces cas sont fréquemment rencontrés dans la pratique, les dispositions doivent être dûment

[49] GE, VS, VD, JU; FR, NE

complétées sur la base de l'art. 377, let. f CC. De l'avis de *privatim, KDSBSON, DSBAG, BE* et *ZG*, cette disposition doit prévoir une obligation de la communauté de référence d'informer les patients des risques possibles de l'utilisation du dossier électronique sur le plan du droit de la sécurité des informations. Ils souhaitent que l'al. 1 soit complété des lettres suivantes : « e. les risques de l'utilisation du dossier électronique du patient en regard du droit de la sécurité des informations ». *Tessaris* soumet la proposition concrète suivante pour l'énoncé de l'al. 1 : « Les communautés de référence donnent au public, aux professionnels de la santé et aux patients des informations générales sur les points suivants concernant l'ouverture, l'exploitation et la suppression du dossier électronique du patient ». Il propose en outre de compléter la let. d comme suit : « l'importance de fixer les niveaux de confidentialité ainsi que l'attribution […] ». La *FMH* souligne également la nécessité d'informer des conséquences d'une restriction d'accès.

Al. 2 : *CURAVIVA*, *Insos* et *TG* proposent aussi un additif à l'al. 2 concernant l'information des représentants de personnes incapables de discernement : « […] recommander au patient et, le cas échéant, à son représentant des mesures de protection et de sécurité des données ». *HL7*, *IHE*, *Integic*, *LUKS* et *medshare* souhaitent que les recommandations soient précisées et demandent selon quels critères elles doivent être délivrées. La *FMH* demande la suppression de l'al. 2. Sept participants[50] font remarquer que les mesures de protection et de sécurité des données devraient être non pas recommandées au patient, mais prédéfinies à l'aide de paramétrages techniques appropriés (par ex. accès protégé par mot de passe, cryptage obligatoire, etc.) selon le principe de la « privacy by default ». Se limiter à une simple recommandation reviendrait à rejeter sa responsabilité sur le patient, ce qui serait manifestement inadéquat compte tenu de la nature des données traitées. *Tessaris* propose le texte suivant pour l'al. 2 de l'ordonnance : « Les communautés de référence rendent les professionnels de la santé et, de manière générale, les patients attentifs aux exigences de protection des données et aux risques encourus par les données stockées dans le dossier électronique du patient. » *VGIch* observe que l'information (al. 1)/la recommandation (al. 2) équivaut à un conseil juridique qui tombe dans le domaine d'activités soumises à des réserves d'autorisation, requiert une formation appropriée et engage la responsabilité des consultants. Une distinction claire doit être établie entre les informations et les recommandations et les Critères techniques et organisationnels doivent être formulés plus clairement.

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.

L'*ASI*, *FSAS* et *SWOR* demandent quel est ici le rôle exact de la communauté de référence et si celle-ci fait activement de la « publicité » auprès des patients. *KSOW* et *ZG* demandent si le consentement, et donc la signature, peuvent aussi être donnés par voie électronique. *Economiesuisse* trouve judicieuse la possibilité de signature électronique et La Poste propose également que la signature électronique soit reconnue valable pour attester un consentement. *SCH* considère que dans le contexte d'une extension généralisée du numérique, on ne peut qu'accepter le principe de la signature électronique qualifiée selon l'art. 14 CO, mais d'autres moyens doivent également être admis pour l'identification univoque des personnes. Cette précision doit aussi être clairement formulée dans le texte de l'ordonnance. *SCH* propose l'ajout de la phrase suivante à l'art. 15 : « […] signature du patient. Le recours à d'autres aides destinées à l'établissement univoque de l'identité du patient est également admis ». *IG eHealth* et *PH CH* souhaitent également l'assurance que le consentement pourra être donné au moyen d'une signature électronique et proposent le texte suivant pour l'art. 15 : « […] doit porter la signature du patient conformément à l'art. 14, al. 2bis de la LF complétant le CC suisse (Livre cinquième : Droit des obligations) ». La *CCM*, *KAeG SG*, *BüAeV* et *GAeSO* saluent l'exigence que le consentement soit muni de la signature personnelle du patient ou d'une signature électronique assimilée à sa signature autographe. *Tessaris* propose que les professionnels de la santé ou la communauté soient tenus d'obtenir du patient son consentement à la tenue du dossier électronique, au début ou au plus tard à la fin du traitement. Ce consentement doit être rédigé par écrit et signé par le patient ou être consigné dans un procès-verbal créé et signé devant témoins par le professionnel de la santé traitant. *VAKA* trouve que

[50] privatim, DSBAG, KDSBSON, BE, AG, ZG, ZAD

la définition de la notion de « signature » manque de clarté. Il ne pense pas qu'à la signature manuscrite sur papier, mais aussi à la possibilité de signer sur une tablette électronique. Il faut s'assurer de pouvoir apposer le plus simplement possible une signature juridiquement valable, ce que demandent également *Medgate*, *K3* et *VZK*. *K3* et *VZK* ajoutent que le consentement doit pouvoir être donné à domicile, dans un Swisscom-shop ou dans un bureau de poste. *AG* fait remarquer que la forme écrite et la signature autographe s'imposent pour pouvoir disposer d'éléments de preuve. La signature électronique répond aux exigences du CO, même si elle n'est pas encore très utilisée dans la pratique. Les *PKS* et la *SSIM* déplorent que la procédure d'ouverture empêche une utilisation ad hoc chez un prestataire, puisque la communauté de référence doit avoir reçu au préalable un consentement signé. Il faut donner la possibilité d'ouvrir un dossier électronique du patient directement chez le prestataire et la signature doit être possible sur place sans nécessiter d'infrastructure supplémentaire. Se référant à son commentaire relatif à l'art. 14, *santésuisse* trouve raisonnable ici aussi que le consentement soit recueilli par l'IDP ou son service d'inscription au moment où l'inscription a lieu.

Tessaris est d'avis que les personnes capables de discernement peuvent exercer leurs droits sur le dossier électronique du patient soit elles-mêmes, soit par l'entremise d'un représentant qu'elles ont désigné, tandis que pour les personnes incapables de discernement, seuls leurs représentants légaux doivent pouvoir agir en leur nom. *La Poste* demande que l'on précise comment la capacité de discernement/responsabilité des patients est vérifiée et ce qui se passe quand cette condition n'est plus réalisée. *senesuisse* est ici du même avis que pour l'art. 14.

La *CCM*, *KAeG SG*, *BüAeV* et *GAeSO* sont d'avis qu'au moment de donner son consentement et sauf disposition contraire de sa part, le patient est réputé avoir autorisé les professionnels de la santé à saisir toutes les données relatives à sa santé dans le dossier électronique du patient, cette mesure étant bienvenue. On peut cependant craindre que cette disposition n'incite les professionnels de la santé à saisir toutes les données dans le dossier électronique du patient pour éviter qu'on leur reproche plus tard d'avoir omis d'y inclure des informations « importantes ». Pour prévenir un déluge de données, il convient de donner aux professionnels de la santé un maximum de latitude dans le choix des données jugées d'importance thérapeutique, données qui sont du reste insuffisamment décrites dans le message du CF. Ils demandent l'ajout d'un article formulé comme suit : « L'importance thérapeutique des données et la décision de les saisir ou non dans le dossier électronique du patient sont laissées à l'appréciation des professionnels de la santé ». Tout comme *ZAD*, ils déplorent en outre que la question de savoir s'il faut autoriser les professionnels de la santé à modifier ou à effacer les données qu'ils ont saisies dans le dossier électronique du patient ne soit toujours pas réglée. *ZAD* demande que ce point fasse l'objet d'une disposition générale, tandis que les autres considèrent que la question de l'autorisation devra sans doute être réglée par une adaptation directe de la LDEP. *ZH* rappelle la nécessité de définir les données qui devront être rendues accessibles dans le dossier électronique du patient. Il s'agit également de déterminer si un médecin se rend punissable en omettant de transférer des données ou en les transférant de manière incomplète.

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.

AG prévient que les tâches administratives mentionnées, bien que probablement nécessaires, constitueront – comme le changement de communauté de référence par les patients – une charge trop lourde pour les communautés de référence. *medshare* propose l'énoncé suivant pour préciser l'al. 1, let. a : « […] régler les modalités d'ouverture et de suppression du dossier électronique par les patients ». Il souhaite l'énoncé suivant pour la let. b : « authentifier et identifier les patients ». *Tessaris* propose que

l'al. 1, let. b soit complété comme suit : « identifier les patients ou les faire identifier par le professionnel de la santé qui fait la demande en leur nom ». *VAKA*, *K3* et *VZK* font remarquer qu'il ne ressort pas clairement de l'article s'il suffit d'utiliser le mTAN et demandent qu'il soit clairement mentionné (dans l'article suivant et les Critères techniques et organisationnels) que la procédure mTAN et son autorisation sont suffisantes. Le patient qui souhaiterait une procédure plus sûre pour lui peut toujours l'obtenir. *La Poste* demande comment l'art. 16 doit être interprété pour les personnes qui ne résident pas en Suisse et souhaite que ce point soit clarifié. *IG eHealth* et *PH CH* font valoir à propos de l'al. 1, let. d que la législation actuelle ne permet d'attribuer un NIP qu'aux personnes obligatoirement assurées au sens de l'art. 1 LAVS. D'autres personnes, par ex. des frontaliers, ne peuvent pas avoir de dossier électronique du patient et sont ainsi exclues du système, bien qu'elles aient droit à des prestations sociales en vertu des accords bilatéraux. *IG eHealth* et *PH CH* renvoient ici à leur proposition de modification de l'art. 5, al. 1. La formulation de l'art. 1, let. e leur paraît en outre trop évasive, raison pour laquelle ils proposent l'énoncé suivant : « en cas de changement de communauté de référence par le patient, rendre accessibles toutes les données, règles d'accès et historiques des accès nécessaires de la nouvelle communauté de référence afin que les accès au dossier électronique du patient puissent continuer de s'effectuer dans une mesure comparable. Le DFI fixe le volume et les formats des données à transférer. » *Moeri* relève qu'il faut prévoir des procédures régissant le changement de communauté de référence pour les patients et leurs données. *ZH*, *ZG*, *NW* et *ZAD* souhaitent une formulation plus directe de ces dispositions. Les engagements doivent être conclus directement avec les communautés de référence. La possibilité de changer de communauté de référence doit être expressément prévue. Il faut laisser la communauté de référence décider par quelle procédure elle entend se conformer aux prescriptions. Ils demandent une révision complète de cette disposition et incluent dans leur prise de position des propositions concrètes de formulation, trop longues pour être exposées ici.

Art. 17	Portail d'accès pour les patients
Le DFI fixe les exigences applicables au portail d'accès destiné aux patients.	

CURAVIVA, *Insos* et *TG* reprochent à cette norme de (sous-)délégation de ne pas remplir les exigences minimales de précision et de densité normative. Ne serait-ce que par souci de transparence et de lisibilité, l'art. 17 devrait indiquer au moins les éléments fondamentaux des exigences que doit remplir le portail d'accès pour patients. La *FRC* rapporte qu'il devient difficile de donner aux patients des informations relatives à l'utilisation du portail d'accès. Elle propose que les organisations de patients, de défense de l'intégrité et autres organisations ayant qualité pour porter plainte, ainsi que les associations de consommateurs, soient invitées à collaborer aux fonctions d'information et payées/rémunérées dans le cadre de contrats de prestations. Dans ce contexte, on devrait également les encourager à coopérer mutuellement pour cette tâche. *SMCF* fait remarquer qu'il est difficile de juger ces modalités d'accès pour les patients au vu de ces dispositions. Ces modalités joueront cependant un rôle essentiel pour l'emploi du dossier électronique et la charge de travail des professionnels de la santé dans ce cadre.

LUKS propose d'intégrer une disposition réglant la certification de portails d'accès patient « externes », c'est-à-dire n'appartenant à aucune communauté de référence. Il faut renoncer aux restrictions objectivement inutiles et rendre possibles des solutions/modèles de gestion innovants. Onze participants[51] craignent que les dispositions de l'OFSP restreignent démesurément les modèles possibles de financement de l'exploitation du dossier électronique du patient. Le droit d'exécution et en particulier les critères techniques et organisationnels doivent être conçus de manière à permettre le développement de solutions innovantes et de nouveaux modèles de gestion. Comme *LUKS*, ils préconisent l'abandon de toute restriction objectivement inutile.

FSAS, *Physioswiss*, l'*ASI* et *SWOR* font valoir qu'un portail d'accès attrayant et sans obstacle sera d'une grande aide pour les patients et constitue ainsi un facteur de succès. *AG* dit saluer l'accès clairement délimité au portail et l'absence de barrière. *VGIch* fait valoir qu'il faut régler les grandes lignes de l'exigence (par ex. l'accès sans barrière) dès le stade de l'ordonnance, sans attendre des décisions

[51] CDS, BL, GL, OW, UR, LU, NW, ZH, SZ, ZG, ZAD

exécutives du DFI. On contrevient ici au principe de légalité. La *FMH* avance que tous les portails d'accès, qu'ils fassent partie de l'offre d'une communauté de référence ou d'une communauté ordinaire, doivent être certifiés en vertu de l'art. 11 LDEP. Elle est d'avis qu'il faut au moins adopter une disposition réglant la certificabilité des portails d'accès des communautés (autres que de référence).

La Poste voit ici une forte « concentration de pouvoir » aux mains du DFI. Elle considère que les use cases doivent déjà figurer nommément dans les textes d'ordonnance, que cela n'empêche pas des use cases futurs, et demande par conséquent qu'ils soient définis et complétés. *senesuisse* a l'impression que les normes de délégation au DFI ont été calculées trop juste. Il est clair qu'au moins les principes de base doivent être inscrits dans l'ordonnance et publiés prochainement. Pour *IG eHealth* et *PH CH*, le choix de déléguer entièrement au DFI la définition des portails d'accès pour patients est une très mauvaise option. Les exigences minimales pour le portail d'accès doivent être définies afin de garantir le fonctionnement homogène et l'interopérabilité du dossier électronique du patient. D'où leur proposition d'un art. 17 foncièrement nouveau, trop long pour être cité ici.

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.	

CURAVIVA, *Insos*, *TG*, *senesuisse* et *SMCF* réitèrent leur prise de position déjà exprimée à propos de l'art. 17. *VAKA* rappelle la dépendance par rapport au ch. 10.2 des Critères techniques et organisationnels et relève que le rapport coût-bénéfice, et en particulier l'extension en dehors d'un téléchargement, ne sont pas réalisés avec un archivage entièrement hors ligne. D'autres articles prévoient déjà un téléchargement des documents. Une importation hors du seul document du patient n'est ni possible, ni souhaitable. *AG* dit saluer l'archivage clairement délimité des données du patient. L'exportation de données du patient lui paraît admissible et utile.

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.	

senesuisse, *BS*, CU*RAVIVA* et *Insos* réitèrent l'avis déjà exprimé à propos de l'art. 12, mais à propos des patients au lieu des professionnels de la santé. *SMCF* réitère ici le commentaire émis à propos des art. 17 et 18. L'*ASI*, *FSAS*, *SWOR* et *Physioswiss* considèrent l'aide aux patients dans l'utilisation du dossier électronique du patient comme un facteur décisif de succès dans la réalisation de ce projet. L'*ASI*, *FSAS* et *SWOR* proposent en outre l'instauration d'un examen pour obtenir le soutien des autorités nationales. *AG* juge nécessaire la mise en place d'un service-desk pour patients, mais pense que des tâches de conseil, de traitement des plaintes et de médiation occasionneraient un surcroît de charges non négligeable. D'après la *FRC*, il est essentiel que les communautés de référence désignent un service d'assistance aux patients afin de les aider dans l'utilisation de leur dossier électronique. Là aussi, il lui semble très important que le patient dispose de plusieurs services et supports d'information. Ces sources d'information supplémentaires devraient être externes à la communauté pour éviter les conflits d'intérêts et garantir une meilleure indépendance, tout en parvenant à très bien coordonner la circulation de l'information.

KSSG demande quelles sont les exigences au niveau des temps de réaction. La mise en place d'un service-desk nécessite le concours d'environ 2-3 collaborateurs dans une communauté de référence pour limiter les temps d'attente. Si les temps de réaction font partie des critères de certification, l'article doit être cité dans les Critères techniques et organisationnels. *VGIch* déclare que la tenue du journal des accès sera soumise aux mêmes dispositions que pour les professionnels de la santé. Or, on constate ici des lacunes dans l'ordonnance ou des imprécisions dans le rapport explicatif, et il faut s'assurer d'obtenir un tout cohérent. Tous les utilisateurs doivent consigner leurs accès dans un journal. *H+* fait valoir qu'il est indispensable pour la mise en œuvre pratique dans les hôpitaux que les patients disposent, pour l'utilisation du dossier électronique, d'un service d'assistance confié à des spécialistes. Il n'est pas réaliste de vouloir laisser cette tâche à tous les professionnels de la santé. La spécialisation des

tâches implique en outre un effort de formation continu. Les moyens d'analyser et de quantifier ce surcroît de charge doivent être examinés dans le cadre de la « fourniture de données pour évaluation ».

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.

Invoquant la dépendance au ch. 12.14.1 des Critères techniques et organisationnels, *VAKA* relève qu'une révocation/un départ sans autre formalité contrevient à l'obligation de conserver les données pendant 10 ans. En fait de révocation « sans formalité », il convient de nuancer (citation) : « pas tout à fait… ». Six cantons[52] déclarent qu'on ne devrait pas effacer des dossiers électroniques de patients au nom du principe de rentabilité. Il ne faut pas économiser au mauvais endroit au regard de ce que va coûter tout le reste. Ils ajoutent que ces délais de conservation des données et du dossier électronique nous éloignent de la nécessité de disposer d'un dossier médical. Le dossier électronique du patient appartient à celui-ci pour la vie et contient ses données médicales qui pourraient devenir indispensables pour des prises en charge futures. *HIN* observe que la suppression d'un dossier auquel personne n'a accédé pendant dix ans est apparemment une mauvaise idée si l'on considère les informations médicales qu'il contient sur le patient ou le fait que les facteurs de risque tendent à être identifiables toujours plus tôt. La *CCM*, *KAeG SG*, *BüAeV* et *GAeSO* constatent que si l'on s'en tient à l'art. 20, les données visées à l'art. 9, al. 1, let. b doivent être supprimées, mais les données historisées doivent être conservées pendant dix ans. Selon le ch. 2.10.2 des Critères techniques et organisationnels, les données historisées ne contiennent pas de données médicales. Ces participants voudraient savoir comment on peut, à partir des données historisées, déterminer rétrospectivement qui a consulté quelles données et quand, et demandent si les données à supprimer en cas de révocation ne devraient pas être conservées dans un espace d'archive séparé, non accessible aux professionnels de la santé. *K3* et *VZK* proposent que la suppression du dossier électronique du patient ne se fasse pas immédiatement, mais seulement au terme d'un certain délai. Cela permet aux personnes autorisées de sécuriser des données au besoin, par ex. pour des analyses génétiques. *privatim* demande qu'il soit stipulé expressément ici que toutes les parties travaillant avec des dossiers électroniques de patients ne peuvent traiter les données personnelles liées aux DEP que pour exécuter les tâches qui leur sont dévolues par la LDEP ou la législation qui en découle. Bien que cette disposition ressorte implicitement de l'art. 4, al. 3 de la loi sur la protection des données (LPD), la nature des données personnelles liées au dossier électronique du patient justifie de l'inclure expressément. Concrètement, *privatim* propose l'énoncé suivant : 1. « 1. Toutes les personnes ou institutions chargées de la constitution, de l'exploitation et de l'utilisation de dossiers électroniques de patients ne peuvent traiter les données personnelles liées aux DEP qu'aux fins exclusives des tâches qui leur sont dévolues par la LDEP et ses dispositions d'exécution ou qui reposent sur une autre base légale dûment définie. 2. La retransmission de données personnelles à des fins publicitaires est interdite dans tous les cas ». D'après *AG*, les dispositions concernant la révocation, la suppression et le délai de conservation de dix ans sont plausibles et ce délai de dix ans est conforme à la législation en matière de preuve. L'important est que le patient reçoive un préavis trois mois avant la suppression, conformément aux prescriptions. *Lovis* est d'avis qu'un dossier électronique du patient ne devrait jamais être supprimé.

[52] GE, VS, VD, JU, FR, NE

Al. 1 : D'après *IG eHealth*, *PH CH* et *economiesuisse*, le texte relatif à la suppression d'un dossier électronique du patient, tel qu'il est formulé actuellement, peut conduire à un effacement automatique et irrévocable des données médicales du patient sans que celui-ci en soit informé. Et comme les données des systèmes primaires devraient également être supprimées selon certaines législations cantonales, il peut en résulter une perte involontaire de données. Ils proposent d'ajouter la nouvelle lettre suivante au début de l'alinéa : « a. non-réponse à un avis écrit de suppression du dossier au patient, à ses représentants et à son médecin de confiance (médecin de famille) à l'expiration d'un délai de 90 jours ». La let. c doit en outre être rédigée comme suit : « c. décès du patient, survenu à une date saisie par un professionnel de la santé ou un auxiliaire et certifié par une autorité, un membre de la famille du patient ou un représentant de sa communauté de référence. » Les let. a à c deviendraient les let. b à d. *STSAG* propose de modifier l'énoncé « La communauté de référence supprime […] ». Il se peut que la communauté de référence n'ait même pas connaissance du décès, l'obligation d'annoncer un décès n'étant pas réglementée. Il se prononce pour que seul le patient (sauf en cas de décès) puisse effacer des documents et supprimer son dossier. Une option alternative serait de permettre la suppression de tous les documents enregistrés dans le dossier électronique du patient depuis plus de 10 ans (ils restent dans le système primaire et peuvent au besoin être repris du système de stockage au prix d'un effort administratif minimal). Pour *SUVA*, une suppression ne se justifie que si le patient révoque son consentement à la tenue de son dossier.

Al. 1, let. a : *Tessaris* pense que l'on devrait en principe imposer les mêmes exigences pour la révocation que pour le consentement à la tenue du dossier électronique. La déclaration de révocation devrait du reste suffire à remplir les exigences de l'al. 2, let. a, ch. 2. *Tessaris* propose l'énoncé suivant pour la let. a : « […] à la tenue de son dossier électronique par une déclaration portant sa signature ou remise, historisée et signée par le professionnel de la santé traitant ».

Al. 1, let. b : *LUKS* objecte que la suppression d'un dossier électronique du patient auquel personne n'a accédé pendant dix ans ne s'inscrit pas dans la perspective d'un dossier à vie et est contraire au but du dossier électronique du patient. D'après la *FMH*, une telle mesure ne sert ni l'intérêt du patient, ni les objectifs de la législation. Pour la *SSIM*, une suppression générale à l'issue d'une période de non-accès est dénuée de sens et Insel considère le délai de dix ans comme inadapté. *Insel* ajoute que l'on peut donner la possibilité de supprimer des données à tout moment (art. 20, al. 1, let. a) et que par souci de compréhension, les conséquences de cette suppression, à savoir l'effacement de toutes les données, soient expressément mentionnées à l'al. 1, let. a, ch. 3. Il faut porter le délai à 20 ans ou, mieux encore, renoncer à tout délai dans les réglages par défaut.

HÄ CH et *ÄTG* observent que cette disposition ne vaut que sur déclaration de consentement préalable du patient que le médecin traitant aura informé en temps utile, et renvoient à leur commentaire de l'art. 9, al. 1. La même remarque s'applique à l'al. 2, let. b. *ASPS* et *Spitex* considèrent qu'avec cette limite de durée, l'ouverture d'un dossier électronique du patient a peu de sens pour des personnes en bonne santé. Celles qui jouiraient d'une bonne santé pendant dix ans après avoir été victimes d'un événement aigu perdraient leur inscription. Il faut s'abstenir de toute limite de durée et supprimer les deux alinéas. *KSOW* fait remarquer qu'il peut s'écouler dix ans entre l'inscription et un premier cas. Il est donc exclu de supprimer automatiquement les données. De plus, le patient doit avoir donné son consentement. L'*ASI*, *FSAS* et *SWOR* se disent en faveur d'un renouvellement automatique du dossier électronique sauf instruction contraire de la part du patient. *Bleuer* observe que sans instruction du patient, les données seront probablement conservées au moins dix ans après son décès établi. De l'avis de *SMCF*, seule une désactivation du dossier devrait être possible, mais pas sa suppression automatique. En outre, les délais usuels devraient être appliqués avant toute destruction de données médicales. Treize participants[53] au total se disent en faveur de la suppression de la let. b, *Moeri* qualifie quant à lui la let. b d'obsolète.

[53] LUKS, SSIM, FMH, ASPS, Spitex, GE, VS, JU, VD, NE, FR, Bleuer, SUVA

Al. 1, let. c : Sept participants[54] observent que l'on n'a pas déterminé comment la communauté de référence doit être informée du décès du patient. Il faudra éventuellement examiner si ce but peut être atteint par une obligation faite à la CdC d'annoncer les décès. Ils demandent que l'on étudie la question et que la let. c comme l'art. 9, al. 1, let. b soient ensuite adaptés en fonction du résultat. En outre, *privatim*, *DSBAG*, *AG* et *BE* souhaitent que l'on examine dans quelle mesure il est utile d'observer une période transitoire de plusieurs années après le décès d'un patient. Plusieurs raisons peuvent conduire les proches d'un patient à devoir obtenir l'accès à son dossier électronique. La *SSIM* fait elle aussi remarquer qu'il pourrait se révéler nécessaire de réaccéder au dossier électronique d'un patient décédé et demande qu'un délai approprié soit prévu à la let. c. *LUKS* a la même requête et propose par ex. un délai de trois mois. Il s'agit aussi de définir la possibilité de remettre des documents à la famille du patient après son décès. *KSSG* relève que le décès d'un patient n'est pas activement communiqué aux prestataires. L'alinéa doit préciser quand commence l'obligation de supprimer le dossier et la let. c doit donc être complétée comme suit : « la communauté de référence est informée du décès du patient ». Pour *La Poste*, les modalités de constat de décès par les communautés de référence doivent être clarifiées. *ZH* et *ZAD* demandent eux aussi que l'on clarifie comment les communautés de référence seront avisées du décès d'un patient et soulignent qu'il est interdit, après le décès d'un patient, de rendre son dossier électronique accessible à des personnes – membres de sa famille inclus – qu'il n'aura pas expressément désignées comme ses représentants. *K3* et *VZK* ajoutent que les institutions de santé et les professionnels de la santé ne sont pas toujours informés du décès d'un patient. Il serait utile que la CdC envoie un communiqué aux communautés de référence lorsqu'elle a connaissance d'un décès. La *FMH* déplore que l'on ne puisse pas supprimer le dossier électronique d'un patient tout de suite après son décès. Selon le droit en vigueur, des erreurs thérapeutiques peuvent être portées devant la justice jusqu'à dix ans après le traitement. Une solution juridiquement cohérente est nécessaire pour répondre aux questions de responsabilité civile/de conservation de données que pose la suppression. *SUVA* demande la suppression pure et simple de la let. c. Six cantons[55] demandent si un dossier électronique du patient peut avoir un intérêt médico-légal. Ils recommandent que le dossier électronique du patient reste masqué et inaccessible pendant un certain temps (par ex. dix ans) puis soit supprimé complètement ensuite.

Al. 2 : *Integic*, *HL7* et *IHE* souhaitent que l'al. 2 soit complété comme suit : « […] doit supprimer avec effet immédiat tous les droits d'accès au dossier […] ». *KSSG* demande ici sous quelle forme les communautés de référence sont censées informer les communautés de la suppression du dossier électronique d'un patient. Aucun profil d'intégration IHE n'a encore été décrit pour ce processus, un retard qu'il faut rattraper.

Al. 2, let. a : *CURAVIVA*, *Insos* et TG dénoncent l'imprécision de la notion de délai approprié et proposent de modifier l'énoncé du ch. 1 comme suit : « informer […] ainsi que la CdC dans un délai d'un mois. *HL7* et *IHE* proposent les nouveaux chiffres suivants pour la let. a : « 3. procéder à la destruction des données visées à l'art. 9, let. b 10 jours au plus tôt et 60 jours au plus tard après la suppression du dossier » et « 4. sur demande, suspendre l'ordre de destruction des données pendant 60 jours. Sont considérés comme requérants le patient, une hoirie pouvant se légitimer par une attestation de qualité d'héritier ou un exécuteur testamentaire se légitimant par un certificat d'exécuteur testamentaire. » *Medshare* propose les mêmes nouveaux chiffres, à la différence près qu'ils demandent un délai de « 30 jours au plus tôt » au ch. 3. De l'avis de *Physioswiss*, le processus de suppression d'un dossier électronique du patient ne doit pas aboutir à ce que toutes les communautés soient informées. Il convient de biffer cette réglementation et de choisir éventuellement un autre processus. La *FMH* demande elle aussi que cette disposition soit biffée, précisant que certaines communautés pourraient être informées de l'existence même du dossier électronique du patient par l'annonce de sa suppression. On ne devrait rien pouvoir effacer dans les archives locales, ni supprimer le NIP. La nécessité d'informer la communauté et la CdC en devient caduque. *La Poste* observe qu'il n'est pas clair comment la suppression du dossier électronique du patient dans toutes les communautés est censée fonctionner. Seule la communauté de référence a la charge de supprimer ledit dossier. D'après *VGIch*, l'idée et le but de l'obligation

[54] privatim, DSBAG, KDSBSON, BE, SZ, ZG, AG
[55] GE, VS, VD, JU, FR, NE

d'informer toutes les communautés restent obscurs. La CdC pourrait par exemple être chargée d'informer – éventuellement sur un mode automatique – les autres communautés si nécessaire. Une révocation devrait en outre toujours être valable avec effet immédiat. Il s'agit également de définir comment interpréter la notion de délai approprié visée à l'art. 20. Cette notion est répétée dans les Critères techniques et organisationnels. Or, leur rôle est de décrire les critères techniques et organisationnels de certification et non d'interpréter l'ordonnance. *VGIch* conseille de fixer un délai (par ex. d'un mois) dans l'ODEP. *La Poste* dit préférer l'énoncé suivant pour la let. a, ch. 2 : « conserver la preuve de la révocation …] ».Six cantons[56] déclarent qu'en cas de suppression d'un dossier électronique du patient, le NIP doit être conservé, comme mentionné dans l'art. 9. Aucun besoin donc d'informer la CdC. Ils proposent dès lors le libellé suivant pour la let. a, ch. 1 : « […] les communautés dans un délai approprié ». La *FMH* renvoie à son commentaire à propos de l'art. 9 et demande ce qu'on entend par « suppression ». Elle ajoute que la manière dont il convient de gérer les aspects médico-légaux en cas de suppression suite à la révocation du consentement du patient n'est pas claire.

Al. 2, let. b : *ÄTG*, *ASPS* et *Spitex* réitèrent ici la position qu'ils ont prise à propos de l'al. 1, let. b. La *FMH* y voit une impossibilité pratique. Si un dossier n'a pas été utilisé pendant dix ans, la probabilité de ne pas pouvoir joindre le patient n'est pas négligeable, si bien qu'il convient de biffer la let. b, ce que demande aussi la *SUVA*. Six cantons[57] demandent également la suppression de la let. b. Ils jugent vraisemblable qu'après dix ans d'inutilisation du DEP, les coordonnées du patient (adresse, numéro de téléphone, etc.) ne soient plus valables. D'après *Moeri*, la let. b est obsolète. *SBC* demande, quant à lui, que le patient soit averti pas moins de six mois à l'avance de la suppression de son dossier.

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.

Medshare observe qu'il manque un titre à cet article. Sept participants[58] font valoir que cette disposition doit être précisée sur le plan du droit de la protection des données. L'OFSP ne doit pouvoir traiter les données que sous forme anonymisée. La liste figurant dans l'annexe 6 de l'ODEP-DFI montre bien que des données anonymisées suffisent amplement à l'évaluation des informations envisagées. Ils préconisent de maintenir l'al. 1 et de faire de l'actuel al. 2 un nouvel al. 3. Ils proposent un nouvel al. 2 dont l'énoncé est le suivant : « L'OFSP ne peut traiter les données que sous forme anonymisée. Les communautés et les communautés de référence sont tenues d'anonymiser ou de faire anonymiser les données avant de les fournir à l'OFSP ». *ZH* et *ZAD* sont eux aussi d'avis que les données ne doivent pouvoir être transmises à l'OFSP que sous forme anonymisée, et relèvent que l'évaluation prévue à l'art. 18 n'exige pas qu'elles ne le soient pas. Ils proposent que l'al. 1 soit complété comme suit : « Les communautés et communautés de référence mettent régulièrement des données anonymisées à la disposition […] ». *Medgate* demande comment vérifier de manière fiable si des indicateurs permettent d'identifier un professionnel de la santé ou un patient. Les données doivent toujours être fournies sous forme anonymisée uniquement. *LUKS* et la *FMH* demandent que la transmission des données soit limitée à un minimum absolu et ajoutent que le financement des charges occasionnées doit être assuré. De l'avis de la *FMH*, le dossier électronique du patient ne doit pas devenir une fin en soi, mais doit servir les objectifs définis dans la LDEP (art. 1, al. 3) et satisfaire aux critères EAE. En plus d'adapter l'ordonnance à ces objectifs, il s'agit aussi d'élaborer un concept d'évaluation approprié basé sur des critères et indicateurs transparents. Ce n'est qu'ensuite qu'il sera possible et admis de déterminer les données à évaluer. Les indicateurs figurant à l'annexe 6 de l'ODEP-DFI sont inadéquats pour évaluer si les buts fixés dans la LDEP ont été atteints. *Physioswiss* insiste pour que les critères soient transparents. *IG eHealth* et *PH CH* sont d'avis que l'al. 2 doit être complété comme suit : « […] les données à fournir, ainsi que les échéances pour la remise de ces données, d'entente avec les milieux concernés ».

[56] GE, VS, VD, JU, FR, NE
[57] GE, VS, VD, JU, FR, NE
[58] privatim, DSBAG, KDSBSON, FR, BE, ZG, AG

Medshare souhaite également que l'on fixe la périodicité et les échéances, *HL7* et *IHE* écrivent que la périodicité doit être définie au plus tard dans l'annexe avec les données à fournir. *VGIch* écrit que les clauses d'évaluation qui s'adressent à des autorités fédérales contiennent au moins des indications sur les éléments suivants : autorité chargée de faire rapport, destinataire des résultats du contrôle, date du contrôle, produit fini, critères de vérification et objet du contrôle. Le terme « régulièrement » a pour effet que l'on donne trop peu de poids à cette disposition. L'*UDC* constate que la formulation laisse en suspens la question de l'intervalle de temps auquel les communautés doivent fournir les données nécessaires à l'évaluation. La fréquence et le volume des données à fournir doivent être déterminés de manière à ne pas occasionner de charge disproportionnée pour les communautés. La *SSIM* critique le fait que cette forme peu stricte de fourniture de données constitue une voie détournée vers un contrôle indirect des prestataires et une collecte excessive de données. La fourniture de données doit être réduite à un strict minimum pour préserver l'anonymat de la statistique d'utilisation. L'al. 2 ne doit pas servir abusivement de blanc-seing au DFI. *STSAG* qualifie l'art. 21 de blanc-seing à l'administration et demande qu'il soit rejeté sous cette forme. Il convient donc de s'assurer que les exigences formulées dans l'ODEP-DFI ne peuvent pas être étendues de manière arbitraire. *VAKA*, *K3* et *VZK* font remarquer que la constitution d'une communauté de référence est déjà compliquée et coûteuse du fait des hautes exigences à remplir pour sa certification. L'art. 21 accroît la pression financière sur les communautés de référence sans qu'elles n'en retirent aucun bénéfice. *VAKA* ajoute qu'elle ne conteste pas l'évaluation de la LDEP, mais ne peut approuver ni la profondeur des données ni le type de sortie. Elle demande par conséquent la suppression pure et simple de cet article. *K3* et *VZK* souhaitent une pratique restrictive de la fourniture des données. *SWOR*, l'*ASI* et *FSAS* donnent une importance particulière à l'évaluation prévue. Ils estiment qu'elle fournira des repères importants en vue d'apprécier le déroulement du dossier électronique du patient et d'indiquer les actions requises.

3.1.4 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);
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.

Dix participants[59] qualifient de très élevées les exigences posées aux moyens d'identification (MID). Le droit d'exécution doit autoriser les MID utilisés aujourd'hui dans les hôpitaux pour autant qu'ils répondent à certains critères. Un professionnel de la santé travaillant dans un hôpital ne devrait pas être obligé de gérer plusieurs logins et systèmes d'accès. Les exigences posées au MID pour les professionnels de la santé travaillant dans les hôpitaux doivent être réexaminées. *La Poste* souhaite que partout où le personnel hospitalier utilise des MID valides selon le droit cantonal en vigueur, ces MID soient également utilisés pour le dossier électronique du patient. *VAKA* rappelle également les solutions MID existantes et demande que l'on détermine où, et en fonction de quels critères, ces dernières pourraient aussi être utilisées pour l'accès aux données régies par la LDEP. Dans une optique similaire, *LU* rapporte que le personnel devrait être équipé de nouveaux MID coûteux pour l'accès au dossier électronique du patient, d'où la nécessité de revoir le texte de l'article. Pour *medgate*, les exigences posées aux systèmes de confirmation d'identité et aux MID sont souvent trop élevées et de ce fait, inadaptées à la pratique ; il faut des procédures simplifiées, et la *SSIM* écrit que le recours à des MID existants déjà très répandus est souhaitable. Les *PKS* font remarquer que les dispositions régissant les MID ne correspondent pas aux procédures pratiquées par le service du personnel des hôpitaux pour les prises de service et les départs des professionnels de la santé. Dans la vie professionnelle quotidienne, il est préférable de se fier à la procédure d'authentification existante et aux MID qui sont déjà d'usage courant. *IG eHealth*, *PH CH* et *economiesuisse* demandent que l'art. 22 soit complété d'une disposition transitoire ou adapté comme suit : « Dans tous les établissements hospitaliers où les professionnels de la santé utilisent un MID valide selon le droit cantonal pour accéder aux données du patient, ce même MID

[59] NW, LU, La Poste, SZ, ZG, ZH, ZAD, IG eHealth, PH CH, economiesuisse

peut être utilisé pour accéder au dossier électronique du patient ». *HÄ CH* et *ÄTG* plaident pour une solution pragmatique et surtout utilisable dans la vie quotidienne, aussi bien au niveau du temps investi que des coûts. Il importe d'édicter des droits d'accès et une réglementation simples pour le personnel médical afin que l'on ne doive pas déléguer des tâches de secrétariat à un médecin juste pour des raisons de droit d'accès. Selon *K3* et *VZK*, le système du dossier électronique du patient doit pouvoir « se fier » à l'hôpital. Il importe dans le quotidien des hôpitaux qu'ils ne soient pas obligés de passer à de nouvelles procédures d'authentification pour accéder au dossier électronique du patient, mais qu'ils puissent se contenter de « compléter » la procédure déjà utilisée en interne. Il faudrait pour cela que la procédure interne remplisse certaines exigences (notamment pour la longueur du mot de passe) et ne doive être complétée que d'un troisième facteur pour l'accès au dossier. L'*UDC* va dans le même sens et fait valoir qu'il est superflu de se limiter à quelques MID bien définis. En effet, pour l'accès au dossier électronique du patient, les établissements hospitaliers pourraient fort bien recourir aux moyens d'authentification qu'ils utilisent déjà. *VAKA* et *AG* font remarquer qu'aucun entretien personnel ne devrait être requis lors de l'inscription du MID, vu que cette complication aurait un effet dissuasif sur de nombreux patients et professionnels de la santé.

Art. 22, let. a : *BRH* fait valoir que le contrôle de la norme ISO par le truchement de l'OFSP n'est pas garanti et qu'il serait donc judicieux d'avoir des indications transparentes au sujet de ladite norme. Il convient donc d'assurer un accès simplifié et de décrire les processus de contrôle ainsi que les autorités qui contrôlent ladite norme. *CURAVIVA*, *Insos* et *senesuisse* critiquent le renvoi à une norme ISO/IEC qu'ils jugent inapproprié dans la mesure où il viole le principe de légalité, et *TG* s'interroge lui aussi sur la conformité au droit de ce renvoi à une norme ISO/IEC. Ces participants ajoutent que ce renvoi constitue une infraction au principe de la transparence et de l'accès au public des textes légaux, d'autant plus que le contenu de cette norme n'est que difficilement accessible. De l'avis de *TG*, il importe que le niveau de confiance 3 corresponde aux autres critères de qualité expressément prévus par la LDEP. Ce principe vaut aussi tant pour l'accréditation que pour la protection des MID et pour la procédure d'authentification. *La Poste* est également d'avis que l'on ne devrait pas prescrire de norme spécifique au niveau de l'ordonnance, mais plutôt se limiter à fixer des conditions stables au niveau de l'ordonnance en déléguant à un office fédéral techniquement qualifié la compétence d'en superviser les exigences en détail. Il convient donc de supprimer la let. a et de rendre possible une harmonisation du texte avec la loi fédérale sur la signature électronique (SCSE). Pour ce qui est des MID électroniques, *ISSS* est d'avis que leurs éditeurs devraient pouvoir garantir leur mise à disposition dans les délais, en nombre suffisant et dans la qualité exigée. C'est possible si l'on se sert des MID actuellement reconnus et certifiés au lieu d'exiger de nouveaux MID fondés sur un autre standard. *ISSS* indique aussi dans sa prise de position les moyens qui existent en Suisse comme en Europe pour obtenir une authentification sûre. Des moyens qui ne sont pas, ou pas toujours, basés sur la norme ISO/IEC 29115. *ISSS* souhaite que l'on applique des MID électroniques déjà définis et rappelle que le standard eCH doit être déterminant pour la définition d'autres MID. Dans ces conditions, la let. a doit être reformulée comme suit : « a. satisfaire à l'une des normes ou prescriptions suivantes : - niveau de qualité 3 de la norme eCH-0170 ; certificat qualifié au sens de la SCSE ; - Certificat d'authentification d'ID selon la norme eCH-0113 ; - eIDAS ». La *SQS* demande elle aussi le remplacement de la norme ISO/IEC 29115 par la signature électronique selon la SCSE.

Art. 22, let. c : *La Poste* demande une formulation plus précise dont il ressorte que le mTAN est un MID possible. L'*OSP* salue l'obligation d'utiliser une procédure d'authentification conforme aux progrès techniques comportant au moins deux facteurs d'authentification. La sécurité de l'accès aux données sensibles doit correspondre au moins à celle des banques. *HIN* salue le principe d'adapter le niveau de sécurité à la situation et l'exigence stricte d'un deuxième facteur d'authentification. Par analogie au niveau des MID couramment appliqués aux professionnels de la santé exerçant en milieu ambulatoire et en pratique libérale, les exigences de sécurité doivent aussi s'appliquer en milieu hospitalier. *HIN* dit disposer en tant qu'IPD de solutions adéquates et de l'expérience nécessaire pour l'utilisation dans de grands établissements hospitaliers. La *SSMI* plaide quant à elle pour qu'on abandonne l'idée de deux niveaux d'authentification.

Art. 22, let. d : Six participants[60] font valoir qu'une période de validité maximale de dix ans paraît très longue au vu de la rapidité des progrès techniques. Malheureusement, le rapport explicatif ne livre pas de réflexions contextuelles à ce sujet. Ils demandent que ce délai maximum de dix ans soit réexaminé. *DSBAG* propose concrètement qu'il soit fixé à deux ans, *BE* propose cinq ans. *VAKA* et *La Poste* demandent la suppression de cette exigence. Si par contre le principe d'un délai était estimé indispensable, *La Poste* considère qu'il doit être réglé dans l'art. 25 et harmonisé avec les autres lois.

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 ou un titre de séjour conforme aux art. 41 à 41b de la loi fédérale du 16 décembre 2005 sur les étrangers 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.

[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.

Les *PKS* et la *SSIM* déplorent qu'à l'image de l'art. 22, on ait mis la barre trop haut pour le contrôle d'identité. Il faut pouvoir recourir à des méthodes bien établies qui ont fait leurs preuves. *La Poste* critique la contradiction manifeste entre les exigences très élevées posées aux MID dans ce projet et les très faibles exigences auxquels est soumise la vérification d'identité. Aussi demande-t-elle que l'on applique les mêmes exigences que celles fixés dans le projet de révision de l'ordonnance sur la signature électronique (OSCSE) pour l'établissement de certificats réglementés. *STSAG* est d'avis que le problème de la vérification d'identité doit pouvoir être résolu de manière plus pragmatique. Il devrait suffire que l'institution procède elle-même à cette vérification (dans le cadre du rapport de travail avec l'employé), que le rôle de ce dernier soit défini (par ex. dans le système KIS) et que l'accès lui soit donné au moyen d'une validation technique (par ex. HIN access gateway). L'identification/authentification dans le système primaire, couplée à une infrastructure d'accès sécurisée, pourrait être utilisée pour une authentification par deux facteurs qui permettrait d'accéder au dossier électronique d'un patient sans avoir à subir d'autres contrôles d'identité.

Al. 1 : *Medgate* réitère son commentaire relatif à l'art. 22. Six cantons[61] proposent de modifier comme suit l'art. 23, al. 1 : « L'éditeur ou la communauté est tenu de vérifier l'identité de la personne qui demande un moyen d'authentification ». *ISSS* écrit que la définition des exigences posées à la vérification de l'identité du requérant fait partie intégrante de la norme/réglementation respective (eCH-0170, eCH-0113, SCSE, eIDAS) et propose l'énoncé suivant pour l'al. 1 : « […] de vérifier l'identité de la personne qui demande un moyen d'identification, conformément à la norme d'émission de ce dernier. […] ». *Spitex* et *ASPS* font valoir que de nombreux clients Spitex ne disposent plus de carte d'identité ou de permis de conduire valable lorsqu'ils sont très âgés. Pour ces personnes, faire renouveler leurs papiers d'identité s'avère souvent très compliqué, de sorte qu'il y aurait lieu de prévoir une autre possibilité d'identification. *Tessaris* fait remarquer à propos de la vérification d'identité que par analogie à l'art. 5, al. 2, l'on devrait pouvoir admettre d'autres moyens de preuve d'identité pour les personnes qui séjournent en Suisse et n'ont aucun numéro d'assuré.

Al. 2 : *VAKA* écrit qu'il s'agit ici d'une vérification dont on ne connaît ni la procédure ni la situation en matière de données. L'OFSP doit définir clairement comment une telle vérification devrait se dérouler. *Spitex* et *ASPS* font remarquer que tant que tous les professionnels de la santé ne figureront pas dans un registre, l'identification en vertu des dispositions de l'art. 2, let. b LDEP sera très onéreuse. L'ordonnance doit prévoir ou régir des registres ad hoc pour les professions de la santé. La *FMH* demande qu'il n'y ait pas un seul attribut « professionnels de la santé », mais que l'on distingue les différents groupes

[60] DSBAG, privatim, KDSBSON, FR, ZG, BE
[61] FR, NE, VS, VD, JU, GE

professionnels. De même, *HIN* déclare que l'attribut « professionnel de la santé » devrait être complété du type de profession médicale, et ce en étroite collaboration avec les associations professionnelles respectives.

Al. 3 : *K3* et *VZK* sont d'avis que l'al. 3 de cet article doit être interprété dans le sens où un hôpital ou un établissement médico-social doit pouvoir identifier un collaborateur et vérifier en plus s'il s'agissait d'un professionnel de la santé. Toute autre solution n'est pas praticable et serait bien trop coûteuse. L'*ASI* et *SWOR* saluent l'attribution d'un numéro GLN aux professionnels de la santé. Ils voient l'ébauche d'une solution possible dans la tenue d'un registre professionnel pour les professionnels de la santé. La *FMH* rejette la possibilité de déléguer à n'importe quelle tierce personne la compétence de vérifier la qualification d'un professionnel de la santé, vu que cela pose un risque qui ne saurait être toléré. Seuls des services qualifiés dont les exigences restent à définir doivent porter cette responsabilité.

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).

[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.

La Poste observe au sujet de l'al. 1 que le NAVS13 n'est pas mentionné dans la liste des attributs. L'IDP ne devrait mettre cet attribut à disposition que pour le dossier électronique du patient et dans aucun autre but. Sans ces données, il n'y a pas de simplification possible de la procédure d'inscription pour les patients. Faute d'élever ces exigences, il faudrait conserver ces procédures d'inscription complexes et on en profiterait peu. Cela signifie que les MID génèrent beaucoup de frais sans fournir de valeur ajoutée. La *Poste* demande que l'on autorise au moins une possibilité de saisie des données. On doit aussi pouvoir y recourir pour une vérification d'identité hors du cadre du dossier électronique du patient, à la condition cependant qu'elle ne soit utilisée qu'en relation avec le dossier. *La Poste* ajoute à propos de l'al. 1, let. 3 qu'il conviendrait de saisir non seulement le numéro de la pièce d'identité fournie, mais aussi le type de document présenté, et propose de prévoir la saisie d'un code pour les preuves d'identité dans la définition des métadonnées. La *FMH* préconise à propos de la let. e que le numéro de la preuve d'identité soit remplacé par le GLN. Elle propose aussi la suppression de l'al. 2. *Tessaris* réitère le commentaire émis à propos de l'art. 23, al. 1 en relation avec la let. e. Six cantons[62] font remarquer que le MID doit certes être consulté, mais que le numéro n'a pas besoin d'être enregistré. Ce serait du temps perdu et il n'y a aucune raison d'enregistrer ces données. Ils demandent la suppression de la let. e. De l'avis de *Tessaris* et par analogie avec les observations formulées au sujet de l'art. 14, al. 2, l'obligation d'informer prévue à l'al. 4 engage dans une certaine mesure la responsabilité de l'éditeur du MID. Il y a également lieu d'attirer l'attention sur la règle de responsabilité visée à l'art. 59a CO pour les titulaires d'une clé de signature cryptographique.

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.

De l'avis de six cantons[63], il y a confusion entre les notions d'identification et d'authentification. L'art. 25 doit être adapté comme suit : « Renouvellement de la durée de validité du moyen d'authentification. 1.

[62] GE, FR, VS, VD, JU, NE
[63] GE, FR, VS, VD, JU, NE

Le moyen d'authentification peut être renouvelé avant l'expiration de sa durée de validité. 2. Lors du renouvellement du moyen d'authentification, l'éditeur ou la communauté vérifie à nouveau l'identité du demandeur conformément à l'art. 23 ». *HÄ CH* et *ÄTG* sont d'avis que pour des raisons rationnelles visant à réduire les charges au minimum, la durée de validité devrait être aussi longue que possible (pas inférieure à trois ans, ou alors deux ans au minimum).

Al. 2 : *VAKA* fait valoir qu'une personne déjà identifiée à l'aide d'une pièce d'identité en application de l'art. 23, al. 1 ne devrait pas avoir besoin de représenter une pièce d'identité lors d'un renouvellement. D'où sa demande de suppression pure et simple de la nouvelle vérification d'identité, un souhait partagé par *LUKS*, la *FMH* et la *SSIM*. De l'avis de huit participants[64], une nouvelle vérification de l'identité de la personne est superflue si un MID est encore valable. *IG eHealth* et *PH CH* proposent que l'al. 2 soit modifié comme suit : « Lorsqu'un moyen d'identification a expiré, l'éditeur est tenu de vérifier l'identité du demandeur en vue du renouvellement 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.

Six cantons[65] font remarquer que pour un blocage, le titulaire doit s'adresser à la communauté. Il ne peut le faire lui-même. Ils demandent le titre suivant pour l'art. 26 : « Blocage du moyen d'authentification », ainsi que l'énoncé suivant : « Le titulaire du moyen d'authentification peut demander de bloquer celui-ci à tout moment ». D'après *HÄ CH* et *ÄTG*, une spécification plus précise est nécessaire, l'utilisateur a besoin de sécurité. Les dépenses qu'impliquent un tel renouvellement et un changement de prestataire doivent être limitées. *SCH* juge l'art. 26 trop restrictif. Cette question doit être réglée dans les dispositions relatives aux MID. Le cas échéant, le MID pourra encore être utilisé pour d'autres applications. L'art. 26 doit être biffé et la disposition transcrite à toutes fins utiles dans l'annexe 5. *Tessaris* fait remarquer que rien n'est prévu concernant la forme de la révocation et qu'un coup de téléphone, un SMS ou un courriel devraient suffire. Par ailleurs, comme le texte de l'ordonnance prévoit un blocage « définitif », on ne sait pas comment le titulaire doit procéder en cas de perte ou de vol d'un MID. D'après *HIN*, il faut exiger que l'on vérifie à chaque accès au dossier électronique du patient s'il y a eu révocation (déclaration de nullité) du MID. Il ne suffit pas de régler uniquement le blocage du NIP. L'art. 26 doit être complété comme suit : « L'éditeur tient une liste des MID bloqués ou déclarés nuls (tableau des révocations). La communauté examine à chaque accès si la personne en question a été correctement authentifiée et que son moyen d'identification n'a pas été révoqué ». *La Poste* reproche à cette description d'être incomplète. L'éditeur peut bloquer lui-même le MID lorsqu'il est informé de manière crédible que les données ne sont plus valables. Il y a un risque de susciter des attentes infondées. L'éditeur doit également pouvoir bloquer le MID lorsque lui-même ou le titulaire nourrit au moins une suspicion d'abus, d'où la nécessité d'établir une liste des raisons conduisant au blocage. Si l'éditeur du MID doit s'assurer que la personne demandant le blocage est bien autorisée à le faire, il faut le mentionner explicitement. Par ailleurs, il serait souhaitable après tout blocage d'un MID que le titulaire en soit informé afin qu'il ait la possibilité de distinguer des blocages qui n'ont pas lieu d'être.

3.1.5 Chapitre 5 : Accréditation

Art. 27 Anforderungen
[1] L'accréditation est régie par l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation (OAccD) et elle est conforme à la norme ISO/IEC 27006:2015, 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;

64 LUKS, FMH, SSIM, HL7, IHE, Integic, IG eHealth, PH CH
65 GE, FR, VS, VD, JU, NE

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.

LUKS considère que les exigences posées aux organismes de certification sont trop élevées et demande qu'elles soient abaissées à un minimum praticable. Un souhait partagé par les *PKS*, la *SSIM* et la *FMH*, qui déclarent que ces hautes exigences occasionneraient des surcoûts pour l'accréditation sans pour autant améliorer significativement la sécurité de la structure globale. *STSAG* est d'avis que les exigences posées aux communautés devraient être définies et vérifiées par le truchement des communautés de référence et non par celui d'un organisme d'accréditation. De fait, il conviendrait de prévoir une accréditation pour les communautés de référence, tandis que pour les communautés, une certification suffirait.

BRH, *CURAVIVA*, *Insos* et *TG* réitèrent leur prise de position faite à l'égard de l'art. 22, let. a, tandis que *senesuisse* se réfère à sa prise de position à propos de l'art. 22, let. b. *SQS* rappelle à cet effet que la protection et la sécurité des données revêtent une importance cruciale pour le dossier électronique du patient. Aux termes du rapport explicatif sur la LDEP, la conformité doit être assurée par une procédure de certification telle qu'elle est notamment prévue à l'art 11 de la loi sur la protection des données (LPD). C'est justement dans ce domaine qu'il importe que les principes et procédures reconnus sur le plan international s'appliquent pour une mise en œuvre efficace. La certification selon l'OCPD répond précisément à cette exigence, car elle reprend dans ses grandes lignes la norme ISO/IEC 27001 reconnue sur le plan international quant aux aspects de la sécurité des informations et des données selon le ch. 3 des directives sur la certification de l'organisation et de la procédure. Les exigences de la protection des données et du système de gestion de la protection des données font d'ailleurs partie de ce certificat spécifique. L'accréditation des organismes de certification ainsi que les exigences auxquelles leur personnel doit répondre sont régies par l'OCPD. Par ailleurs, la certification selon l'OCPD dans le cadre des certifications légales des services de réception des données des assurances-maladie sociales a fait ses preuves au cours de ces dernières années. *SQS* demande que l'art. 27, al. 1 soit modifié comme suit : « […] et par l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD), sauf si […] ».

S'agissant de l'al. 3, *SQS* demande que l'application de la norme ISO/IEC 27006:2015 soit ajoutée à celle de l'Ordonnance sur l'accréditation et la désignation (OAccD). L'article comporte aussi des redondances et doit être allégé des exigences superflues. La mention de la norme ISO/IEC 27006 n'est justifiée que si l'on doit pratiquer une certification selon la norme ISO/IEC 27001. SQS demande la suppression pure et simple de l'art. 27, al. 3, let. a et b. Quant à l'al. 4, *SQS* relève que les critères de qualification sont aussi fixés par l'accréditation. Les critères techniques et organisationnels réglés à l'annexe 7 et les exigences qui en découlent pour les communautés de référence et les communautés ne contiennent aucune disposition qui dérogerait aux exigences de la norme ISO/IEC 27001:2013 ou d'une certification selon l'art. 11 LPD et qui requerrait des connaissances spécifiques d'informatique médicale propres à garantir une vérification dans les règles de l'art dans le cadre d'une certification. L'al. 4 doit donc être purement et simplement supprimé lui aussi.

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.

De l'avis de la *FMH*, il ne faut pas que les procédures d'accréditation soient trop longues et trop lourdes à assumer financièrement, surtout si l'on souhaite voir des sociétés de médecins indépendants se constituer en communautés.

3.1.6 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.
[4] Les milieux intéressés sont consultés au sujet des modalités visées à l'al. 2 et des adaptations visées à l'al. 3.

VAKA réitère ici son commentaire relatif à l'art. 18. *IG eHealth*, *PH CH* et *La Poste* trouvent rigide le système décrit par la LDEP. De nombreux critères techniques sont dictés par le DFI. Toutefois, le présent texte de l'ordonnance ne décrit nulle part comment mener les processus d'adaptation ni comment il convient de les garantir. Tandis que *IG eHealth* et *PH CH* proposent de compléter ce texte par une nouvelle section intitulée « Adaptations systémiques », *La Poste* propose quant à elle un tout nouvel article qu'elle intitule « Clauses d'adaptation ». *La Poste* ajoute qu'il faut définir un organisme chargé d'effectuer les adaptations. Par ailleurs, il convient de décrire dans un processus comment procéder aux modifications et dans quels délais elles doivent être introduites, acceptées et mises en œuvre. Il convient de faire participer les communautés et l'industrie à cette opération. La *FMH* trouve les critères de certification trop exigeants.

Al. 3 : *CURAVIVA* et *Insos* objectent qu'une délégation de compétences au contenu si vague est incompatible avec les exigences du principe de légalité. De même, *TG* déclare que la délégation à l'OFSP de l'adaptation des critères de certification est de trop large portée et trop mal définie. Selon *ZH* et *ZAD*, il est problématique que le DFI règle les critères de certification, mais que l'OFSP puisse les adapter en fonction des progrès techniques en vertu de l'al. 3. Il serait plus juste que cette adaptation soit également effectuée par le DFI. Selon l'art. 12, al. 2, LDEP une délégation à l'OFSP est tout à fait admissible. Une délégation au DFI devrait aussi être admissible en vertu du principe « a maiore ad minus ». Tandis qu'*AG* salue la délégation à l'OFSP de la compétence d'adapter les critères en fonction des progrès techniques, la *FMH* demande que cette délégation soit remplacée par une description générale et fonctionnelle de ces critères par voie d'une ordonnance du Conseil fédéral. Par ailleurs, ces critères doivent être restreints à un minimum indispensable à la création d'un espace de confiance.

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 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.

BRH réitère ici les commentaires qu'il a faits à propos des art. 22, let. a et 27, al. 1, *La Poste* répète sa prise de position relative à l'art. 22, let. c. *HIN* fait valoir que le rôle de l'éditeur du moyen d'identification est trop mal défini. Dans un contexte IHE, on parle d'IDP, d'ATP et de STS pour désigner les rôles intervenant dans l'authentification et les droits d'accès. L'énoncé actuel de l'article n'indique pas clairement si les trois rôles sont ou non joués par l'éditeur. Le jeton digital XUA nécessaire à chaque transaction contient des données apportées par les trois rôles, à savoir : les informations relatives à l'authentification (IDP), l'attribut du professionnel de la santé (ATP) et les indications pour le jeton (IDs, rôle, etc.) qui parviennent du STS. Si ces trois rôles étaient séparés et que l'éditeur du MID était considéré uniquement comme l'IDP, il en résulterait une faille de sécurité car le STS et l'ATP ne seraient alors ni certifiés ni vérifiés, alors que les données qu'ils apportent sont susceptibles d'affecter la sécurité. *HIN* propose de compléter comme suit la mention du rôle de l'éditeur de MID dans l'art. 30 : « [Les éditeurs de moyens d'identification doivent] mettre à disposition tous les acteurs (IDP, ATP et STS) nécessaires

pour rendre possible une authentification valable ».

Al. 1 : *La Poste* qualifie l'al. 1 de disposition judicieuse et souhaitable. *NW* observe ici que l'organisme de certification vérifie chaque année pour toutes les communautés si elles remplissent encore les critères de certification. C'est une dépense inutile puisqu'en vertu de l'art. 34, ces certificats sont censés être valables 3 ans. Ces vérifications pendant les trois ans de validité des certificats ne doivent pas se faire systématiquement chaque année, mais seulement par sondage. *ISSS* propose d'apporter la précision suivante à la let. b : « […] qualifications requises ainsi que les certifications reconnues ». La let. c doit en outre être adaptée comme suit en complément à l'art. 11, al. 1 : « […] exploités de manière sûre en Suisse ».

Al. 2 : *senesuisse* réitère ici son commentaire à propos de l'art. 22, let. b et de l'art 27, al. 1, tandis que *La Poste* et *CURAVIVA* renvoient à leurs prises de position relatives aux art. 22, let. a et 27, al. 1. *La Poste* ajoute que cet alinéa est confus, vu que les MID servent à l'authentification. L'ordonnance gagnerait en lisibilité si tous les critères exigés du MID étaient réglés au même endroit. *La Poste* recommande de déplacer cet alinéa après l'art. 22 si le texte de l'ordonnance le permet. La *FMH* critique le fait que les dispositions visant à protéger le MID soient déjà définies par la norme ISO/IEC 29115:2013(E) dans l'art. 22, let. a. Une protection plus étendue n'est pas nécessaire, si bien que l'al. 2 doit être biffé.

Al. 3 à 5 : De l'avis de *La Poste*, on ignore à la lecture de l'al. 3 si les critères de certification visés sont ceux définis pour l'éditeur ou pour l'organisme de certification. Les critères mentionnés dans l'annexe 7 au chapitre 2 (art. 7 de l'ODEP-DFI) pourraient être mentionnés directement ici, ce qui rendrait superflus les al. 3 à 5. La *FMH* observe que le DFI pourrait régler des détails concernant la certification, mais seulement sur la base de la norme ISO en vertu de l'art. 22, let. a. Le législateur ne doit pas poser de critères allant au-delà de cette norme. L'art. 3 doit avoir la teneur suivante : « […] critères de certification selon l'art. 22, let. a ». *CURAVIVA* et *TG* réitèrent pour l'al. 4 leur prise de position relative à l'art. 29, al. 3.

Section 2 : 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.

La Poste est d'avis que l'OAccD mentionnée à l'art. 27, al. 1 devrait être suffisante et que dès lors, l'art. 31 doit être supprimé. Alors qu'*AG* considère comme judicieuses les étapes esquissées pour la certification, la *FMH* répète que les critères de certification sont trop stricts et qu'il faut se garder de surréglementer la procédure de certification. La FMH souhaite concrètement la suppression de l'art. 31. *SQS* fait remarquer que la section 2 de l'ODEP traitant de la procédure de certification ne mentionne pas les délais qui devraient s'appliquer à la suspension ainsi qu'au retrait définitif de la certification Dans le cas où les communautés de référence et les communautés sont certifiées en vertu d'une norme existante, les délais sont réglés dans le cadre de cette norme. Deux variantes peuvent s'appliquer, chacune dépendant de la norme de certification choisie ou de l'application d'une procédure propre pour la certification dans le domaine du dossier électronique du patient régi par l'ODEP. La suspension ou le retrait d'une certification par l'organisme de certification en cas d'irrégularités constatées ou d'écarts substantiels aurait un impact direct sur l'admission des hôpitaux et autres institutions et, partant, sur l'exécution de la LAMal. Par conséquent, la réglementation des délais de procédure en cas d'un retrait ou d'une suspension de certification doit s'effectuer dans le respect des conditions posées dans le droit procédural. Cela plaide en faveur d'un règlement spécifique de la question des délais dans l'ODEP. Les deux procédures de suspension et de retrait de certifications, l'une en vertu du droit public appliquant

les conditions d'admission régies par la LAMal, l'autre appliquant les règles de certification selon les normes ISO, ne concordent nullement au niveau des délais ni des voies de droit. Partant de ce constat, une réglementation des délais dans le cadre des critères de certification telle qu'énoncée dans la section 2 de l'ODEP revêt une importance cruciale et doit aussi respecter le principe de la proportionnalité.
La variante a implique l'ajout d'un alinéa supplémentaire à l'art. 31 : « La procédure de certification de communautés de référence et de communautés est régie par l'ordonnance du 28 septembre 2007 sur l'accréditation et la désignation (OAccD), sauf si la présente ordonnance en dispose autrement. » Quant à la variante b, elle implique d'ajouter, dans la section 2 intitulée « Procédure de certification » du chapitre 6 ODEP, des dispositions réglant les délais de suppression des divergences substantielles ainsi que les modalités de suspension et de retrait d'une certification. *OFAC* rappelle qu'elle a depuis 2009 l'expérience simultanée des processus de certification ISO 27001 et OCPD. La superposition des normes ISO 29115, des exigences spécifiques aux eID des prestataires de soins, ainsi que la conformité du profil de protection de l'eID représentent un volume normatif et de certification (exprimé en jours d'audits) qui doit être réparti dans le temps sur une durée à fixer. Il convient d'édicter des dispositions transitoires dans ce domaine.

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.

CURAVIVA, *Insos* et *TG* réitèrent pour cet article leur prise de position relative à l'art. 20, al. 2, let. a. *La Poste* trouve judicieux l'al. 32.

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.

La *CDS*, *ZAD* et onze cantons[66] observent que l'organisme de certification vérifie chaque année pour toutes les communautés si elles remplissent encore les critères de certification. C'est une dépense inutile puisqu'en vertu de l'art. 34, ces certificats sont censés être valables 3 ans. Ces vérifications pendant les trois ans de validité des certificats ne doivent pas se faire systématiquement chaque année, mais seulement par sondage. *K3* et *VZK* font la même proposition. *ZG* ajoute que des vérifications devraient être entreprises aussi en cas de suspicion ou d'indices particuliers. Dans le même esprit, *AI* propose l'énoncé suivant pour l'al. 1 : « L'organisme de certification est tenu de vérifier par sondage ou en cas de suspicion d'irrégularité si les critères de certification sont toujours remplis », et *Insel* plaide pour l'adoption du texte suivant : « En cas de suspicion fondée que les critères de certification ne sont plus remplis, l'OFSP peut ordonner que l'organisme de certification procède à un examen ». La *FMH* estime que les vérifications annuelles prévues représentent une charge trop lourde et propose dès lors un délai d'au moins trois ans. *La Poste* estime qu'un contrôle tous les deux ans devrait suffire. Une cadence annuelle paraît judicieuse pour la certification des MID. *BFH* demande pourquoi on ne prolongerait pas d'une année la durée de validité du certificat après vérification. Il n'est pas non plus judicieux de procéder à une vérification durant la troisième année de validité du certificat en cours, vu que ce dernier va expirer et qu'il faut de toute manière procéder à une recertification. *AG* est d'avis que la vérification annuelle et la recertification au bout de trois ans doivent être mieux distinguées dans le rapport explicatif. Il convient également de préciser et de mieux délimiter les notions de « surveillance », de « certification » et de « recertification ». *LUKS* et la *SSIM* jugent disproportionnée une vérification annuelle quand le certificat n'est valable que trois ans et demandent donc la suppression de l'al. 1. *DSBAG* et *privatim* réaffirment de leur côté que pour des raisons de protection des données, une vérification annuelle est très souhaitable.

[66] BL, GL, LU, OW, UR, SH, SZ, ZG, TG, ZH, FR

HIN fait valoir qu'au vu de leur grand nombre, la vérification des critères de certification (points de mesure) n'est possible qu'au prix d'investissements conséquents. Par conséquent, il est proposé de les répartir en critères impératifs et obligatifs/potestatifs. L'al. 2 doit être adapté comme suit : « L'OFSP établit une liste de tous les critères et les classe en critères impératifs et obligatifs. Les écarts substantiels concernent les critères impératifs ». *SQS* relève que le registre des communautés de référence et communautés certifiées est tenu par l'OFSP. L'art. 36 dispose que l'OFSP peut prendre des mesures en cas de mise en danger grave de la protection ou de la sécurité des données du dossier électronique du patient. Un alinéa supplémentaire doit être ajouté à l'art. 33 : « L'OFSP peut demander en tout temps à l'organisme de certification ou à la communauté et à la communauté de référence de lui fournir les documents nécessaires à la certification ou à la recertification ».

Art. 34	Durée de validité
Le certificat est établi pour une durée de trois ans.	

BFH et *AG* réitèrent leur prise de position à l'égard de l'art. 23, al. 1 et la *FMH* reprend ici son commentaire de l'art. 28. *VAKA* s'étonne de la méfiance que suscitent les futures communautés et communautés de référence. Il convient de répéter avec insistance que le fait de devoir se préparer à une procédure de certification tous les trois ans est définitivement insupportable. *K3* et *VZK* qualifient également de très lourde l'obligation de recertifier tous les trois ans. *La Poste* estime qu'une durée de validité de 5 ans serait adéquate en ce qui concerne les communautés. Un rythme de trois ans serait judicieux pour les MID. Six cantons[67] souhaitent que l'art. 34 soit reformulé comme suit : « […] une durée de cinq ans ». Dix participants[68] au total demandent que le certificat soit établi pour cinq 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.	

VAKA et *La Poste* demandent que l'on veuille bien leur préciser la notion de « substantiel ». *VAKA* demande en outre qu'on lui fournisse des exemples. *HIN* et *BINT* font remarquer que le seuil définissant la notion de « substantiel » doit être placé assez haut pour éviter que l'organisme de vérification soit submergé par des annonces, et renvoient au commentaire de *HIN* à propos de l'art. 33. *AG* fait valoir que les adaptations aux infrastructures TI pourraient provoquer rapidement des vérifications ou recertifications compliquées et onéreuses. Il convient d'appliquer ici le principe de proportionnalité.

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.

K3 et *VZK* font valoir que l'exclusion d'une communauté de référence ou d'une communauté a des conséquences imprévisibles qui rendent impossible ou interdisent une telle option. Rendre possible l'exclusion même passagère d'une communauté de l'accès à un dossier électronique du patient serait méconnaître totalement l'importance que l'on compte donner au dossier électronique. Il convient de trouver d'autres solutions et moyens pour imposer les critères du dossier électronique du patient à un service d'exploitation. Il est impensable de mettre un système hors service. On pourrait imaginer par exemple qu'une société supplétive reprenne les tâches et les données. La *FMH* écrit que la disponibilité des données des patients est justement un facteur crucial pour l'acceptation d'un dossier électronique

[67] GE, FR, VS, VD, JU, NE
[68] VAKA, K3, VZK, La Poste, GE, FR, VS, VD, JU, NE

du patient. Ils proposent également une sorte « d'institution supplétive » pour le cas où une communauté serait mise hors service. *NW* considère que la clause de sauvegarde pose problème. Une exclusion aurait pour conséquence que les hôpitaux, par exemple, n'auraient pas accès aux données indispensables en cas d'urgence. Cela compromettrait la sécurité du patient, raison pour laquelle cet article doit être remanié. *SG* demande que l'on précise quelles prétentions les patients pourraient faire valoir auprès de qui dans l'éventualité où l'OFSP refuserait temporairement à une communauté l'accès au dossier électronique d'un patient, la privant ainsi de la possibilité de consulter les données du patient qui s'y trouvent. Six cantons[69] estiment que l'OFSP n'a pas le pouvoir de refuser à une communauté l'accès au dossier électronique du patient, pour la bonne raison que c'est la communauté qui le gère. L'OFSP peut par contre bloquer l'accès d'une communauté aux services centraux et aux autres communautés. Ils proposent de reformuler la let. a comme suit : « […] l'accès aux services centraux et aux autres communautés ». *Tessaris* fait remarquer que parallèlement au refus d'accès, un accès doit pouvoir être accordé au cas par cas, moyennant des mesures de protection particulières, à un professionnel de la santé qui devrait accéder au dossier électronique du patient pour les besoins du traitement médical. D'où la proposition d'ajouter le texte suivant à la let. a : « refuser […] patient, tout en ménageant la possibilité d'accorder au cas par cas l'accès au dossier électronique d'un patient à un professionnel de la santé pour les besoins du traitement médical et moyennant l'observation de dispositions de sécurité spécifiques ». Six participants[70] demandent que l'on examine si une disposition facultative pourrait effectivement mener au but fixé. L'OFSP doit pouvoir agir s'il y a mise en danger grave de la protection ou de la sécurité des données du dossier électronique du patient. *DSBAG*, *KDSBSON*, *privatim* ainsi que *BE* et *ZG* préconisent l'énoncé suivant pour l'art. 36 : « […] du patient, l'OFSP prend notamment une ou plusieurs des mesures suivantes : 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 électroniques ; c. ordonner une recertification extraordinaire ».

Section 3 : 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.

SG réitère sa prise de position relative à l'art. 36. *VAKA* observe qu'en cas de retrait d'un certificat à une communauté ou de refus temporaire d'accès à une communauté dans l'intérêt du patient, il n'existe aujourd'hui aucune réglementation relative à des communautés ou sociétés supplétives. La procédure, l'organisation et la gestion d'une telle « société supplétive » doivent être fondamentalement repensées et redéfinies. *RPB* ajoute que l'on pourrait imaginer un scénario édulcoré issu des dispositions de l'art. 8. *SQS* souhaite que l'on introduise dans l'art. 37 un alinéa supplémentaire qui régisse les conséquences d'une suspension ou d'un retrait de certificat afin de protéger les intérêts des prestataires et des patients concernés tout en maintenant leur accès au dossier électronique du patient.

En ce qui concerne l'al. 1, sept participants[71] estiment qu'une disposition facultative est inadéquate en cas de défaillances graves. Il serait plus indiqué d'obliger l'organisme de certification à suspendre la

[69] FR, NE, GE, VS, VD, JU
[70] DSBAG, KDSBSON, privatim, AG, BE, ZG
[71] DSBAG, KDSBSON, privatim, AG, BE, FR, ZG

validité du certificat ou à le retirer dans un tel cas. L'alinéa doit être adapté en conséquence. Pour ce qui a trait à l'al. 2, la *CDS* et onze cantons[72] signalent que le rapport de droit entre l'organe accrédité et les entreprises intéressées repose sur une base incertaine. Le premier accomplit des tâches administratives, ce qui soulève des questions de contrôle étatique, de protection juridique et de liens avec le droit fondamental. L'assertion que la procédure est régie par « les dispositions du droit civil applicables aux relations contractuelles » ne saurait donc être formulée de manière si catégorique. L'al. 2 doit donc être remanié en conséquence. Au sujet de l'al. 3, *DSBAG* et *privatim*, rejoints en cela par *AG*, *BE* et *FR*, sont d'avis que la procédure administrative est applicable étant donné que l'OFSP est l'autorité qui décide (art. 1 PA, RS 172.021). Il convient d'examiner dans ce contexte si la procédure administrative permet d'assurer la liberté d'action indispensable (rapidité, efficacité, etc.). *SQS* fait remarquer que les dispositions de la LDEP n'autorisent pas l'OFSP à intervenir activement dans le processus concret de certification et à se substituer à l'organe de certification. L'autorisation de l'OFSP telle que prévue à l'art. 37, al. 3 viole le principe de légalité et ne peut être conciliée avec une ordonnance d'exécution. L'art. 36 autorise du reste l'OFSP à prendre des mesures dans les cas où il faudrait agir rapidement. SQS demande donc la suppression pure et simple de l'art. 37, al. 3, let. b.

3.1.7 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.

K3 et *VZK* observent que les services de recherche visés aux art. 38 ss. offrent plusieurs données utiles pour la communication entre les professionnels de la santé et l'institution de santé. Ils demandent si ces registres pourraient aussi servir à la communication dirigée. Le canton de Zurich prévoit que l'infrastructure peut aussi être utilisée pour la communication primaire entre deux prestataires. Ils demandent par conséquent que le MID puisse être utilisé pour la communication dirigée entre deux prestataires. *OFAC* déclare que sa grande expérience d'exploitation informatique et opérationnelle de ce type de service à un niveau national, compte tenu de la criticité de ces applications d'un point de vue disponibilité, sécurité, protection des données, etc., l'amène à recommander fortement que les sociétés qui proposeront ces services centralisés soient elles aussi certifiées (par ex. : ISO 20000, ISO 27001, OCPD). Les organisations qui gèreront et exploiteront les services centralisés devront être soumises au moins aux mêmes exigences de certification et d'organisation que les communautés. Ce principe, selon *OFAC*, doit être inscrit dans l'ODEP et doit se retrouver dans les exigences des appels d'offres.

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.

[72] BL, GL, LU, OW, UR, NW, FR, SZ, TG, ZG, ZH

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

La Poste trouve le terme de « certificat » pas assez explicite et lui préfère celui de « certificat d'authentification ».

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.

PH CH réitère ici ses remarques à propos de l'art. 8. *VAKA* demande s'il y a des cas d'utilisation (« use cases ») dans lesquels il peut arriver que plusieurs communautés saisissent différemment des entrées identiques du HPD. Les professionnels de la santé peuvent fort bien appartenir à plusieurs communautés et exercer une activité dans de multiples organisations. Il faut s'assurer que de tels chevauchements ne pourront pas se produire. *H+* salue expressément la stratégie de l'OFSP consistant à mettre en place un service de recherche national. *La Poste* fait remarquer que c'est la première fois que le terme d'« institution de santé » est utilisé dans ce contexte. Seul le terme de « groupe » a été utilisé dans les chapitres consacrés à l'autorisation. La question qui se pose dès lors est si une institution de santé peut aussi être un groupe. Il convient de définir clairement la terminologie et de faire apparaître clairement si les groupes sont gérés ou non par le service de recherche. Un autre point qui manque encore de clarté et qu'il convient d'élucider est de savoir ce qui se passerait si deux communautés voulaient modifier les mêmes inscriptions et qui, dans un tel cas, en porterait la responsabilité. Concernant la let. a, ch. 3, *La Poste* demande en outre si c'est le but de l'ordonnance que d'obliger chaque institution de santé en Suisse à se procurer une OID en plus de son numéro GLN. Dans la suite du texte, les groupes sont décrits de telle manière qu'on peut les interpréter indifféremment comme des entités globales ou individuelles. Cette décision est laissée au patient. Dans ce scénario de cas d'utilisation, attribuer un identificateur univoque n'a aucun sens parce qu'un même groupe peut avoir d'autres membres selon le contexte. Le numéro GLN suffit en tant qu'identificateur. Il s'agit de clarifier la situation et de reformuler le ch. 3 comme suit : « OID (en tant qu'identificateur univoque au sein de l'OID de la communauté) ».

Let. b : *HL7* et *IHE* sont d'avis qu'aux ch. 1 et 3, les données personnelles doivent être mentionnées de manière exhaustive. Le ch. 3 peut être formulé comme suit : « GLN et OID (s'il existe), et dénomination […] ». *La Poste* constate ici que selon la let. a, ch. 2, le professionnel de la santé doit indiquer le GLN d'un groupe ou d'une organisation déjà inscrit(e). Ce numéro est déjà mentionné dans les renseignements à fournir selon la let. a, ch. 1. *ASPS* et *Spitex* font remarquer que l'attribution de GLN à des professionnels de la santé n'en est qu'à ses débuts et est encore très loin d'être complète. Il faut rendre obligatoire l'attribution d'un GLN à chaque professionnel de la santé.

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.

La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* observent que ces dispositions ne disent rien sur les critères qui déterminent le montant des indemnités allouées au tiers. Vu les dispositions de l'art. 42, il faut cependant s'attendre à ce que les coûts de ces indemnités soient répercutés sur les communautés ou les communautés de référence. Afin que les coûts demeurent dans un cadre raisonnable, les indemnités accordées au tiers ne doivent pas être négociées ou fixées selon les critères de l'économie privée. Il convient d'observer le principe d'équivalence. Ces participants demandent l'ajout de l'alinéa supplémentaire suivant : « Les indemnités accordées au tiers, qui se composent des éventuels émoluments pour la fourniture de prestations en vertu de l'art. 19, al. 2, LDEP ainsi que d'une indemnité supplémentaire de la Confédération ne doivent pas excéder les dépenses que devrait supporter l'OFSP s'il se chargeait lui-même de constituer et d'exploiter des services de recherche ». *KAeG SG* souhaite en outre faire ajouter la phrase suivante à la fin de ce nouvel alinéa : « Il est exclu de faire participer le corps médical ».

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 sont applicables.

La *FMH* réitère le commentaire émis à propos des art. 28 et 34. Vingt participants[73] signalent que dans l'al. 1, il est question d'un émolument annuel de CHF 13 500 tandis que le rapport explicatif fait état de CHF 20 000. *KSOW* demande d'où vient ce chiffre de CHF 13 500, ou seraient-ce quand même CHF 20 000 ? *VGIch* et *Medgate* demandent de lever cette contradiction. *BE* demande que les restrictions prévues pour les CTO en faveur des communautés et des communautés de référence soient précisées. Dix-sept participants[74] font valoir qu'il est inadéquat de vouloir, d'un côté, soutenir financièrement la mise en place de communautés et de l'autre, alourdir les frais d'exploitation de ces communautés par un émolument, ce qui revient à leur demander une restitution partielle de ces aides financières. Neuf autres participants[75] considèrent eux aussi que la perception d'un émolument annuel auprès de bénéficiaires d'aides financières fédérales n'a aucun sens. *LUKS* et *STSAG* font eux aussi référence à l'aide financière et suggèrent de renoncer à un tel émolument. *BRH* est d'avis qu'il convient de remettre en question pendant dix ans l'émolument annuel pour la constitution et l'exploitation des services de recherche, vu qu'il impliquerait un reflux d'une partie de l'aide financière dans les caisses fédérales. Il propose d'opérer une compensation avec l'aide financière reçue. *LUKS* ajoute que la Confédération devrait financier les services centraux de recherche de données et *STSAG* observe que la LDEP prévoit l'obligation pour les institutions de participer au dossier électronique du patient, ce que l'on ne saurait lier à une obligation d'y contribuer financièrement. *NW, ZG, ZH* et *ZAD* ne voient aucune raison à un tel émolument. Son irrecevabilité découle du fait que l'ordonnance ne définit pas quelle prestation l'émolument est censé indemniser. D'ailleurs, le rapport explicatif ne révèle rien non plus à ce propos. Six cantons[76] considèrent qu'il serait juste que la Confédération prenne en charge les frais opérationnels d'intérêt général, en particulier ceux de l'exploitation des services généraux. *OFAC* s'exprime dans le même sens et affirme que ces frais doivent être intégralement pris en charge par la Confédération et non par les communautés. *AR* estime qu'il convient d'éclaircir en particulier quels frais cet émolument est censé couvrir et à qui ces fonds seraient alors versés. *VAKA* est d'avis que dans la situation présente où aucune des communautés futures n'a de modèle économique pour financer son exploitation, aucun émolument ne devrait être perçu pour les services centraux. *UDC* pense qu'il serait raisonnable de simplifier les flux financiers et ce tant dans l'intérêt des communautés que dans celui de la Confédération, par exemple en fixant pour les aides financières fédérales un montant qui permette de renoncer auxdits émoluments.

[73] CDS, BL, GL, LU, OW, UR, SH, AR, ZG, SZ, AI, TG, PKS, BE, BFH, UDC, BRH, VGIch, Medgate, LUKS
[74] CDS, BL, GL, LU, OW, UR, SH, AR, ZG, SZ, AI, TG, PKS, NW, ZH, ZG, ZAD
[75] FR, NE, GE, VS, VD, JU, K3, VZK, UDC
[76] FR, NE, GE, VS, VD, JU

Au total, 25 participants[77] demandent explicitement la suppression de l'art. 42. *HIN* part de l'idée que les communautés qui se constitueront seront très hétéroclites. Cet organisme propose de percevoir ces émoluments en fonction de la taille de l'entité et suggère de formuler comme suit l'art. 42, al. 1 : « […] s'acquittent d'un émolument forfaitaire annuel fixé en fonction de leur taille, mais au maximum de 13 500 francs ». *BFH* estime que l'on pourrait prévoir ici une meilleure pondération compensatoire, en particulier pour les communautés de référence, au moyen d'un montant-seuil assorti d'une partie variable, comme le nombre de citoyens appartenant à la communauté. Des montants fixés de façon rigide n'auraient pas beaucoup de sens.

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.

La *SSIM* relève ici que les émoluments figurent dans la section 3 intitulée « Transfert de tâches à des tiers ». Ces émoluments ont sans doute une validité générale et il convient de le préciser.

[77] VAKA, FR, NE, GE, VS, VD, JU, K3, VZK, FMH, BL, CDS, GL, LU, OW, UR, SH, SZ, AR, AI, TG, ZG, NW, ZH, ZAD

3.2 ODEP-DFI

Les annexes 5b, 5c et 8 de l'ODEP-DFI sont rédigées en anglais. Il s'est ensuivi que la plupart des prises de position relatives à ces trois documents ont été soumises en anglais et intégrées sans traduction dans le présent rapport.

3.2.1 Art. 1 Numéro d'identification du patient (annexe 1)

Art. 1	Numéro d'identification du patient
La composition du numéro d'identification du patient et la procédure de vérification de la clé de contrôle en cas de saisie manuelle du numéro d'identification du patient au sens de l'art. 4, al. 2, ODEP sont définies à l'annexe 1.	

Art. 1 : *FR* rappelle qu'il est nécessaire de clarifier ce qu'il est possible de faire ou non avec le NIP.

Annexe 1

La *Fondation refdata*, *GS1*, la *SSIM* et *ICTS* réitèrent pour l'annexe 1 leur prise de position relative à l'art. 4 ODEP. *ICTS* demande en outre l'application des normes internationales pour l'identification des patients et la clé d'identification utilisée à cet effet ; dans toute la mesure du possible, il convient de renoncer à des développements isolés purement helvétiques. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* saluent la décision de créer un NIP spécifique pour le dossier électronique du patient au lieu d'utiliser le NAVS13 comme numéro d'identification comme prévu initialement.

OFAC dit n'avoir rien à déclarer concernant l'algorithme de contrôle du numéro d'identification du patient. *BINT, HL7* et *IHE* qualifient cette procédure d'usuelle ; elle correspond aux normes et, à leur avis, satisfait aux exigences. *Medshare* ne voit rien à redire non plus à l'annexe 1.

3.2.2 Art. 2 Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (annexe 2)

Art. 2	Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence
Conformément à l'art. 29, al. 2, ODEP, les critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence sont dé-finies à l'annexe 2.	

Art. 2 : *SQS* fait valoir que l'annexe 2 n'est point une disposition régissant les critères de certification, mais une consigne technique et organisationnelle destinée aux communautés et aux communautés de référence, qui est soumise aux dispositions de l'art. 11, al. 1, let. a, LDEP et doit donc être certifiée. Une certification de systèmes de gestion n'a pas pour rôle de vérifier que les consignes techniques sont respectées. Lors d'une certification ISO/IEC 27001:2013, l'équipe d'audit doit vérifier cette application par le truchement du Control A.18 dans le cadre de la certification du système de management. C'est pourquoi l'art. 2 doit avoir la teneur suivante : « Les critères techniques et organisationnels (CTO) applicables aux communautés et communautés de référence soumises à l'obligation de certification visée à l'art. 11, al. 1, LDEP, sont définis à l'annexe 2 conformément à l'art. 29, al. 2, ODEP. » Par ailleurs, *SQS* demande l'ajout de l'alinéa suivant à l'art. 2 : « Les exigences minimales posées à un système de gestion de la protection des données se fondent sur les Directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir (Directives sur la certification d'organisation et procédure) du 19 mars 2014, édictées par le Préposé fédéral à la protection des données et à la transparence ».

Annexe 2

1. Gestion (art. 8 ODEP)

Six participants[78] sont d'avis que les consignes données au ch. 1 sont beaucoup trop volumineuses et qu'il y a lieu de les simplifier. La plupart de ces consignes découlent d'ailleurs des dispositions de l'art. 8

[78] K3, VZK, ZAD, ZH, ZG, NW

ODEP. Celles qui dépassent la portée de l'article doivent y être intégrées en tant que réglementations à caractère général et abstrait (exemple : ch. 1.3 sur la gestion du personnel auxiliaire)

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

Six cantons[79] font valoir que le terme « gestion » de la version française est inapproprié et doit être remplacé par « administration » (ce qui correspond à la traduction de « Verwaltung ».

1.1.1 : *IG eHealth* et *La Poste* souhaitent que l'on définisse le terme d'« institution de santé ». Il s'agit notamment de déterminer si par principe, un médecin établi, un thérapeute ou une sage-femme ne peut œuvrer au sein d'une communauté qu'en qualité de « collaborateur/-trice » d'une institution de santé. À ce propos, *Tessaris* regrette que le terme d'institution de santé introduit à l'art. 8, al. 1, ODEP ne soit défini clairement nulle part.

1.1.2 : La *FMH* observe à propos du ch. 1.1.2.1 que la LDEP ne règle pas les processus dans les cabinets médicaux, les hôpitaux, etc. Elle ne peut régler ici que les aspects en relation avec l'utilisation du dossier électronique du patient. *IG eHealth* et *La Poste* relèvent à ce propos que les exigences visées au ch. 1.1.2.2 ne peuvent être remplies que si les services mettent à disposition les processus et les moyens techniques nécessaires. Or, ces exigences ne sont décrites nulle part. Ces organismes proposent dès lors que des instructions obligatoires soient formulées aux services conformément à l'art. 40 de l'ordonnance (ou à ses annexes).

La *CDS* et 10 cantons[80] observent au sujet du ch. 1.1.2.3 que la formulation « pour tous les professionnels de la santé admis rattachés à une institution de santé » pourrait suggérer que tout professionnel d'une institution de santé doit être admis sans exception dans le HPD. Les institutions de santé doivent être libres de ne sélectionner que les professionnels de la santé qui utiliseront effectivement le dossier électronique du patient. Il convient par conséquent de modifier l'énoncé du ch. 1.1.2.3 comme suit : « déclenchement du processus "entrée de professionnels de la santé" pour les professionnels de la santé admis rattachés à une institution de santé, auxquels cette dernière prévoit de donner l'accès au dossier électronique du patient ». *VGIch* observe à propos de ce chiffre que le rapport explicatif prévoit la possibilité de déléguer le processus d'entrée aux institutions de santé. Pour des motifs pratiques, cette disposition doit être interprétée comme une habilitation des institutions de santé à désigner elles-mêmes les personnes qui y entrent activement. La forte fluctuation du personnel dans les hôpitaux requiert une certaine modération dans l'application de cette exigence. Les Critères techniques et organisationnels doivent être adaptés en conséquence. *AR* plaide pour que les avis présentés à propos du ch. 1.1.2.3 soient intégrés dans les ordonnances. *La Poste* demande comment l'entrée d'un professionnel de la santé est possible si l'institution de santé à laquelle il est rattaché n'est pas membre de la communauté. Il convient de formuler beaucoup plus clairement la manière dont c'est envisagé. *KSSG* interprète le ch. 1.1.2.3 comme une obligation d'informer sur tous les professionnels de la santé entrant dans une communauté, ce qui est en contradiction avec les déclarations entendues dans les réunions d'information. On y a dit et répété que le nombre de professionnels de la santé admis et répertoriés pouvait être limité à quelques personnes par discipline/clinique. Cette affirmation doit être concrétisée dans l'article.

1.1.3 : *SUVA* fait remarquer que le stockage de documents dans une institution de santé correspond à un classement dans le système primaire. Avec l'obligation de détruire les documents dans les lieux de stockage de documents des institutions de santé, les documents seront définitivement perdus, ce qui ne saurait correspondre à l'esprit et à la lettre du dossier électronique du patient. En effet, même au cas où il arriverait qu'un dossier électronique du patient soit supprimé ou qu'une institution sorte d'une communauté, les documents doivent continuer d'exister dans les systèmes primaires. *SUVA* demande donc la suppression de l'obligation de détruire les données, et plus précisément du ch. 1.1.3 (1.1.3.1 à 1.1.3.2.3 compris), ou à tout le moins des précisions sur ces dispositions. *La Poste* observe à propos

[79] FR, NE, GE, VS, VD, JU
[80] BL, GL, LU, OW, UR, BS, NW, FR, SZ, TG

du ch. 1.1.3.1 que cette exigence est irréalisable quand un prestataire travaille dans plusieurs institutions ou communautés. Par exemple, un médecin qui a son cabinet à Nyon tout en étant accrédité dans un hôpital de Genève sera enregistré dans deux HPD. Il y a des médecins à la *SUVA* qui comptent jusqu'à sept employeurs institutionnels. La formulation doit être modifiée en conséquence. *TI* est d'avis que dans les dispositions relatives au ch. 1.1.3.2, il faut retenir que les données sont saisies par un professionnel de la santé pour garantir au patient la poursuite d'un traitement optimal. Les données n'appartiennent donc non pas à l'institution qui sort de la communauté, mais sont bel et bien la propriété du patient. Elles ne doivent par conséquent jamais être effacées, mais peuvent éventuellement être mutées pour garantir au patient un dossier aussi complet que possible. Dans tous les cas, la suppression des données, si tant est qu'elle ait lieu, ne pourra pas s'effectuer sans que le patient en soit préalablement averti. La *SSIM* fait valoir que le patient dont la communauté est sortie du système doit avoir la possibilité de s'affilier à une autre communauté. Ce point devra être précisé. La *FMH* estime qu'il n'est pas acceptable que la plupart des législations cantonales règlent les modalités selon lesquelles les patients se voient mettre leurs données à disposition, par ex. en cas de décès de leur médecin, alors que les données du dossier électronique du patient sont détruites ou que leur conservation ultérieure relève de la responsabilité du patient (cf. 1.1.3.2.3) et que la communauté en question en fixe elle-même la procédure. Cette pratique va à l'encontre des intérêts des patients et des règles fondamentales de la documentation médicale. Il est tout aussi inacceptable qu'une exigence d'une telle portée soit uniquement un critère de certification dans les CTO et ne soit pas définie en tant qu'exigence fonctionnelle au niveau de l'ordonnance. Il convient donc de prendre des mesures appropriées.

Six cantons[81] font valoir qu'en cas de sortie d'une institution de santé en application des ch. 1.1.3.2.1 et 1.1.3.2.2, les dossiers électroniques de patients ne doivent pas être détruits, mais doivent rester à la disposition des patients et des professionnels de la santé. Les auteurs des documents ne sont d'ailleurs pas les institutions, mais les professionnels de la santé. Il convient donc de supprimer ces deux chiffres. *BFH* juge incompréhensible que les documents d'une institution de santé puissent être tout simplement effacés à sa sortie. Même si les patients doivent être avertis à temps en vertu du ch. 1.1.3.2.3, il est nécessaire de définir une procédure claire qui empêche la perte des documents. Le ch. 1.1.3.2.3 doit être complété d'une disposition qui prévoit au minimum un transfert automatisé des documents à supprimer vers les « lieux de stockage internes spéciaux » mis à disposition par les communautés de référence pour les documents des patients concernés selon l'art. 18 ODEP (voir ch. 10.1.1. des CO). *Economiesuisse* et *SBC* insistent pour que les patients ne perdent en aucun cas leurs données dans l'hypothèse où une institution de santé sortirait de l'espace de confiance créé par la LDEP. Ce ne serait pas dans l'intérêt de la souveraineté du patient. Ils proposent l'adoption du nouvel énoncé suivant : « Les communautés doivent s'organiser pour assurer la continuité du stockage des documents de prestataires qui quittent une communauté sans en rejoindre une autre ». *Bleuer* rappelle que ces documents appartiennent au patient et ne doivent pas être supprimés sans son autorisation explicite. Il convient de veiller de manière appropriée à ce que tous les documents des institutions de santé sortantes soient conservés dans le dossier électronique du patient (rien ne devrait changer pour les utilisateurs au niveau des droits d'accès). Il est rejoint en cela par *medshare*, qui considère que le dossier électronique d'un patient lui appartient pour la vie dès son ouverture. Pour cette raison, personne, hormis ce dernier, n'a le droit de supprimer des données. Même en cas de révocation, le patient conserve le droit de décider si ses données doivent ou non être supprimées. Cette question a une importance particulière dans la perspective d'une réouverture ultérieure du dossier. *IG eHealth* et *La Poste* jugent inapplicable le ch. 1.1.3.2.1. Si une institution de santé sort d'une communauté pour en rejoindre une nouvelle, il appartient à cette dernière de la saisir correctement. Les institutions de santé et les professionnels de la santé conservent leurs identificateurs respectifs (GLN). Les associations avec les documents sont également préservées. L'important est qu'une institution de santé ne puisse pas emporter ses documents dans une nouvelle communauté, vu que l'association avec les documents est modifiée lors d'un changement d'ID du domaine d'affinité. Toutes les références dans les historiques d'audits seraient perdues, et, du même coup, leur traçabilité. Les mises à jour isolées des métadonnées (voir XDS.b) seraient également perdues parce que l'on devrait également effacer les registres, vu que les entrées de registre renvoient à des documents inexistants. Cette disposition doit donc être supprimée. *IG eHealth* et *La*

[81] FR, NE, GE, VS, VD, JU

Poste estiment en outre que la sortie d'une institution de santé ne doit pas entraîner la suppression des dossiers électroniques de patients auxquels elle avait accès. *IG eHealth* propose que l'institution de santé sortante soit tenue de laisser ses données dans un répertoire d'archivage (Repository) dont la possession serait alors transférée à la communauté. *La Poste* ajoute que l'exigence de suppression en application du ch. 1.1.3.2.1 est incompatible avec le but recherché par la loi. Elle va à l'encontre du principe de la gestion secondaire des données et de l'idée fondamentale selon laquelle la souveraineté des données appartient au patient. La communauté doit s'assurer que tous les documents restent disponibles même après la sortie d'un professionnel de la santé ou d'une institution de santé. *Integic* ne comprend pas l'énoncé du ch. 1.1.3.2.1 ; dans la perception du patient, celui-ci s'attend à ce que les documents qui le concernent se trouvent dans le lieu de stockage qui lui est alloué. Quel que soit l'édifice, une éventuelle application des ch. 1.1.3 et 1.1.3.2 entraînera de toute évidence une perte de données pour les patients, sinon il n'y aurait pas lieu de les en informer préalablement. Les documents médicaux appartiennent au patient. Leur suppression par des tiers, quels qu'en soient les motifs, est certainement illicite. Il manque dans le texte la formulation explicite d'un modèle de souveraineté des données ; les énoncés des ch. 1.1.3.2.1 et 1.1.3.2.2, par exemple, suggèrent au moins implicitement que des tiers possèdent des droits de décision relatifs à la conservation des données. Le ch. 1.1.3.2.1 n'est applicable que si le stockage du dossier électronique du patient est exclusif. Le rapport explicatif sur l'ODEP parle de cas d'exception, mais il n'en est pas question ici. Chez *privatim*, on rappelle qu'une simple suppression de documents électroniques ne suffit pas à les détruire. Une destruction irréversible de données requiert le recours à des procédés techniques appropriés. *Privatim* propose de reformuler le ch. 1.1.3.2.1 comme suit : « la destruction irréversible, à l'aide de procédés techniques appropriés, des documents […] ». Pour le ch. 1.1.3.2.2, l'énoncé proposé est le suivant : « la destruction irréversible, à l'aide de procédés techniques appropriés, des saisies du registre des documents […] ». *LU, NW, SZ et ZH* qualifient de problématique l'obligation de supprimer les documents saisis dans le dossier électronique du patient par une institution de santé sortante lorsqu'elle quitte la communauté. Il s'agit de déterminer qui, du patient ou de l'institution de santé, détient la souveraineté sur ces documents. Aucune donnée ne doit pouvoir être supprimée du dossier électronique du patient contre sa volonté. *ZG* estime que la sortie d'une institution de santé – qu'elle adhère ou non à une autre communauté – ne doit pas entraîner la suppression de données du dossier électronique du patient. Il convient d'édicter une règle qui garantit que les données des patients resteront dans le dossier électronique du patient même si l'institution de santé qui y a déposé les données quitte ultérieurement la communauté ou la communauté de référence. *Tessaris* fait remarquer que la suppression fiable d'un document dans le dossier électronique du patient, copies de sauvegarde incluses, est un processus lourd à mettre en œuvre. Se pose alors la question qui, de la communauté ou de l'institution de santé, doit en assumer la responsabilité et les coûts. Le ch. 1.1.3.2.1 doit être adapté comme suit : « la suppression complète des documents, y compris des copies de sécurité et de sauvegarde, figurant dans les lieux de stockage de l'institution de santé sortante, la vérification de sa bonne exécution ainsi que la confirmation de la suppression par la signature de la personne responsable désignée au ch. 1.1.4. ».

IG eHealth objecte à propos du ch. 1.1.3.2.2 que de telles inscriptions ne devraient pas être possibles en vertu de l'art. 9, al. 1, let. c, ODEP. Or, le rapport explicatif concernant cette ordonnance suggère qu'elles pourraient l'être pour des raisons techniques, mais ne fournit pas d'autres détails. *IG eHealth* recommande la suppression de cette exception. *HIN* reproche au terme « en temps utile » utilisé au ch. 1.1.3.2.3 de laisser une trop grande marge d'interprétation et propose, tout comme la CCM, BüAeV, GAeSO et KAeG SG, d'adopter l'énoncé suivant : « l'information des patients concernés en temps utile, c'est-à-dire au moins un mois avant la sortie, avec mention expresse aux patients que les documents stockés de l'institution de santé sortante seront supprimés à sa sortie ». *AR* demande que la notion « en temps utile » soit mieux explicitée. Six cantons[82] souhaitent que le ch. 1.1.3.2.3 soit reformulé comme suit : « l'information en temps utile des patients par les professionnels de soins concernés ». *Tessaris* observe que les droits des patients et leurs prétentions vis-à-vis de l'institution de santé dont ils ont été informés de la sortie ne sont pas clairs. Ils proposent l'énoncé suivant : « […] l'information en temps utile, sous forme écrite vérifiable, des patients concernés qui doivent également être avisés des options dont ils disposent ».

[82] FR, NE, GE, VS, VD, JU

1.1.4 : La *FMH* déplore les nombreuses ambiguïtés de procédure contenues dans le ch. 1.1.4 et insiste sur la nécessité d'apporter des précisions. *K3*, *VZK* et *VAKA* demandent la suppression du ch. 1.1.4.2.2. *BFH* relève qu'en vertu de l'art. 8, let. e, ODEP, le patient doit pouvoir identifier « en tout temps » la composition des groupes de professionnels de la santé. Or, on parle ici de « chaque trimestre au moins ». Une opérabilité « en tout temps » mobiliserait beaucoup de moyens, si tant est qu'elle fût possible. Une base trimestrielle paraît plus réaliste, mais reste en contradiction avec le texte de l'ordonnance. *Tessaris* relève que la vérification et la confirmation, au moins deux fois par année, de l'actualité et de l'exactitude des données concernant les institutions de santé et les professionnels de la santé, telles qu'elles sont saisies dans le service de recherche central, est un processus extrêmement lourd. On ne sait pas encore comment s'effectueront ces vérifications. Six cantons[83] signalent que les communautés n'ont pas les moyens de « vérifier et confirmer » les données autrement qu'en se basant sur les renseignements fournis par les institutions et les groupes. Ils proposent que le ch. 1.1.4 soit reformulé comme suit : « Chaque institution ou groupe enregistré dans le service de recherche central […] doit : 1.1.4.1 désigner en son sein un répondant chargé de communiquer les changements intervenant dans les données à la communauté ; 1.1.4.2 communiquer dans les trente jours à la communauté tous les changements intervenus dans les données enregistrées. 1.1.4.2.1 abrogé, 1.1.4.2.2 abrogé ».

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

Six cantons[84] réitèrent pour le ch. 1.2 leur prise de position relative au ch. 1.1.

1.2.2 : La *FMH* juge impraticable la disposition du ch. 1.2.2.1 et demande sa suppression. Les dispositions du ch. 1.2.2.3 contiennent des chevauchements avec celles de l'ODEP. La vérification que l'on a affaire ou non à un professionnel de la santé doit être effectuée par des services qualifiés, sans parler de la distinction à faire entre les différents groupes professionnels. La *FMH* demande donc que l'on édicte une réglementation claire à l'échelon de l'ODEP. Elle ajoute à propos du ch. 1.2.2.4 que le MID doit être enregistré dès sa délivrance, ce qui suppose également une règlementation stricte au niveau de l'ODEP. Enfin, la *FMH* pose dans sa prise de position quelques questions au sujet du ch. 1.2.2.5 et appelle de ses vœux une réglementation générale des processus au niveau de l'ODEP. Six cantons[85] trouvent que le ch. 1.2.2.4 n'est pas clair. Un MID qui n'est pas enregistré ne peut pas être utilisé. Il importe de s'entendre sur la terminologie (identification ou authentification ?) et la pertinence du verbe « garantir » dans les dispositions du ch. 1.2.2. *FR*, *GE*, *VS*, *VD* et *JU* jugent bon de préciser que les données de MedReg ne sont pas forcément à jour. Une reprise systématique de ces données n'est donc pas toujours une bonne idée. La phrase qui s'y réfère au ch. 1.2.2.5 doit par conséquent être supprimée. *IG eHealth* et *La Poste* demandent si les registres tels que MedReg, etc. ne font pas partie intégrante des services de recherche des HPI ou s'il conviendrait de les relier séparément au HPD. Ils y voient en outre une contradiction avec les dispositions légales. Les entités responsables des données sont les communautés. La question de la propriété se pose différemment pour les registres. Il s'agit ici de savoir qui a le droit de décision en présence de données contradictoires et en cas de conflits. C'est un point qui doit être éclairci. Par ailleurs, le service de recherche des institutions de santé doit intégrer également les auxiliaires afin que les membres des communautés soient identifiables sans exception et puissent être reconnus par le patient. *La Poste* ajoute que la remise et la gestion des moyens d'authentification destinés aux collaborateurs des institutions de santé ne sont pas mentionnées et se demande si la communauté les délègue à des tiers. STSAG aimerait avoir l'assurance que les services de recherche visés au ch. 1.2.2.5 permettent un traitement largement automatisé des entrées et des sorties des professionnels de la santé. *Tessaris* souhaite que le ch. 1.5.2.21.2.2.5 soit complété comme suit : « […] sont reprises et leurs modifications y sont mises à jour au fur et à mesure ». *SCH* critique la création d'interfaces avec les registres professionnels, qui engendre des frais inutiles, et demande par conséquent que l'on supprime la deuxième phrase du ch. 1.2.2.5.

[83] FR, NE, GE, VS, VD, JU
[84] FR, NE, GE, VS, VD, JU
[85] FR, NE, GE, VS, VD, JU

1.2.3 : Six cantons[86] demandent comment contrôler les accès et veulent savoir s'il s'agit de vérifier qu'un professionnel de la santé qui a consulté le dossier électronique du patient était bien autorisé à le faire. Cette étape est vérifiée dans les tests d'intrusion, mais pas dans les « processus de gestion des professionnels de la santé ». Ces cantons demandent donc la suppression du ch. 1.2.3.2. Ils déplorent en outre le manque de clarté du ch. 1.2.3.3 et aimeraient des explications à son sujet. *SBC* est d'avis que la documentation sur un patient ne doit pas figurer éternellement dans les fichiers de sauvegarde (back-up) si le patient ne le souhaite pas. Sinon, on court le risque d'une utilisation malveillante de données depuis le back-up alors que l'on croyait que tout était effacé. D'ailleurs, les données restent présentes dans le système primaire pour servir éventuellement de moyens de preuve. *SBC* demande l'adoption du texte suivant : « Les supports de données qui ont plus de 2 ans doivent être effacés. Il convient alors de s'assurer que toutes les données actuelles qui figurent sur des supports ayant moins de 2 ans sont sécurisées. » *La Poste* demande à propos du ch. 1.2.3 comment gérer les prestataires qui font partie de deux communautés. On ignore si leurs données sont dupliquées et dans ce cas, qui se charge de leur maintenance. *IG eHealth* et *La Poste* ne voient pas comment réaliser l'exigence du ch. 1.2.3.3. Ce que l'on demande doit rester dans le domaine du possible. Pour ce qui est du ch. 1.2.3.1, *Tessaris* renvoie à la recommandation concernant les données présentes dans les registres médicaux mentionnés au ch. 1.2.2.5. Comme expliqué à propos du ch. 1.1.4.2, les contrôles visés au ch. 1.2.3.2 peuvent s'avérer très coûteux suivant les moyens et les procédés engagés. *Tessaris* souhaite en outre compléter comme suit le ch. 1.2.3.3 : « les droits d'accès sont adaptés en fonction des catégories et options définies aux art. 1 à 3 ODEP ». La *FMH* demande à propos du ch. 1.2.3.3 à quoi les droits d'accès sont censés être adaptés.

1.2.4 : *GE, VS, VD, JU* et *NE* font remarquer qu'au ch. 1.2.4.2, les termes « du patient » figurent deux fois de suite dans la version française et qu'il convient d'enlever celui qui est de trop. *Tessaris* déclare qu'à son avis, les patients doivent être informés de l'entrée et de la sortie de professionnels de la santé et demande donc l'ajout d'une disposition qui deviendrait le ch. 1.2.4.4 : « les patients sont informés par écrit sous une forme vérifiable de l'entrée et de la sortie d'un professionnel de la santé dans leur communauté afin qu'ils puissent exercer leurs options concernant les droits d'accès ».

1.3 Gestion des auxiliaires des professionnels de la santé

IG eHealth et *La Poste* font valoir que la réglementation interne des communautés ne tombe pas dans le champ d'application de la LDEP, de sorte qu'il n'y a pas lieu de prévoir des prescriptions y relatives. Il convient d'expliquer les champs d'application de l'ODEP et des CTO. *VAKA* propose pour simplifier que les auxiliaires puissent être inscrits à titre facultatif, ce qui permettrait de biffer le ch. 1.3. De l'avis de l'*Insel*, l'administration des auxiliaires représente une charge de travail disproportionnée, et *IG eHealth* souligne la nécessité d'une administration unitaire de tous les auxiliaires pour qu'ils soient clairement reconnus des patients. *IG eHealth* demande la suppression du ch. 1.3.1 et *Insel* celle du ch. 1.3. *HIN* s'interroge sur l'étendue de la notion d'« auxiliaire ». Ils présument qu'elle désigne les AM, les aides-soignants, etc. Les cuisiniers d'un EMS, le personnel administratif, les équipes de nettoyage, etc. en sont sans doute implicitement exclus ; on peut dès lors se demander si des directives explicites seraient utiles. *STSAG* est d'avis que le seul personnel auxiliaire qu'il faut administrer est celui associé au traitement des données et propose le complément suivant au ch. 1.3.1 : « […] des professionnels de la santé, dans la mesure où ces auxiliaires sont directement associés au traitement des données du dossier électronique du patient ». La *FMH* estime que les processus d'administration du personnel auxiliaire doivent être réglementés de manière uniforme à l'échelon de l'ordonnance et ne doivent pas différer d'une communauté à l'autre. Par ailleurs, il convient de définir clairement quelles personnes pourront avoir accès au dossier électronique du patient et sous quelle responsabilité. Elle propose d'édicter une réglementation claire à l'échelon de l'ODEP pour le chiffre 1.3.2.1. *BFH* demande à propos des ch. 1.3.2 et 1.3.2.1 que l'on définisse également des métadonnées pour les auxiliaires. Ainsi, il convient de nommer notamment des administrateurs et du personnel d'assistance technique qui auront immanquablement besoin d'un accès au système. *VGIch* craint que l'administration des individus, groupes et

[86] FR, NE, GE, VS, VD, JU

auxiliaires exigée actuellement dans les hôpitaux soit trop lourde ou irréalisable, car elle ne correspond pas à la pratique quotidienne d'utilisation des aides électroniques telle qu'elle est vécue et a fait ses preuves en milieu hospitalier. L'hôpital doit être considéré comme un domaine de confiance (trusted domain). *KSSG* observe que les dispositions de l'ordonnance ne permettent pas une synchronisation des auxiliaires avec les services centraux, de sorte que le patient ne peut pas exclure un auxiliaire de l'accès à son dossier. La règle du droit à l'autodétermination conduit ainsi à une absurdité, d'une part, et d'autre part le patient sera dérouté si les journaux des accès lui indiquent des noms d'auxiliaires qu'il ne connaissait pas lorsqu'il a octroyé les droits d'accès. Les auxiliaires doivent également être répertoriés dans le HPD et synchronisés avec les services centraux. L'article doit donc être supprimé, et le ch. 1.2.3.3 n'a pas davantage de justification. Les droits d'accès au dossier électronique du patient sont gérés par le patient. KSSG demande quels sont les processus administratifs censés conduire à une modification des droits d'accès et se prononce pour la suppression de cette exigence. *OFAC* observe que les auxiliaires ne seront pas enregistrés dans les services de recherche, ce qui exclut de leur part toute participation à un échange intercommunautaire. Dans plusieurs professions de la santé, les travaux de gestion du dossier médical sont entièrement délégués à des auxiliaires. C'est dire qu'une bonne gestion du dossier médical requiert un certain échange avec d'autres prestataires de santé, que le personnel auxiliaire ne sera pourtant plus autorisé à avoir. Cette situation représenterait alors clairement une régression par rapport au fonctionnement du système actuel. *OFAC* considère que l'aptitude à entreprendre un échange intercommunautaire ne peut être évaluée et décidée que par le professionnel de la santé, responsable de son personnel auxiliaire. L'art. 2, let. b, LDEP dispose que le personnel auxiliaire doit être enregistré dans le service central de recherche et obtenir les droits que lui délègue le patient. Dans la pratique, il pourra arriver que les professionnels de la santé confient leur MID avec leur mot de passe à leur personnel auxiliaire, avec les problèmes que cela pourrait entraîner.

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

1.4.1/1.4.2 : *HIN* relève que seuls les professionnels de la santé sont explicitement mentionnés au ch. 1.4.1, tandis que le ch. 1.4.2 fait également référence au personnel auxiliaire. *HIN* tient pour acquis que les auxiliaires auront aussi besoin d'une identité propre. Il importe que même les auxiliaires soient tenus d'utiliser des MID conformes à l'art. 30, LDEP. Le ch. 1.4.1 doit être complété comme suit : « L'accès des professionnels de la santé et des auxiliaires au dossier électronique du patient […] ». *IG eHealth* et *La Poste* soulèvent le problème que les logins internes ne sont plus admis dans les hôpitaux. *IG eHealth* ajoute que cette section ne règle que les critères fixés aux MID pour le droit d'accès et demande quels sont les critères à remplir pour pouvoir effectuer des saisies dans un dossier électronique du patient. *IG eHealth* demande que les MID conformes au droit cantonal soient également admissibles pour l'accès au dossier électronique du patient. Ce raisonnement conduit *La Poste* à demander que l'on admette les MID des organisations, vu que ceux-ci doivent eux-mêmes répondre à des prescriptions régies par d'autres lois. La certification des MID au sein d'une organisation ne relève pas de l'ODEP. Il s'agit en outre de clarifier si l'authentification par un seul facteur est recevable pour les systèmes ne permettant qu'un affichage protégé en écriture des dossiers médicaux. *Tessaris* demande que le ch. 1.4.2 soit réadapté comme suit : « Les communautés et les institutions de santé doivent garantir, aussi bien pour les professionnels de la santé que pour les auxiliaires, que leur identificateur univoque figurant dans le moyen d'identification et leur identité enregistrée dans la communauté ou l'institution de santé soient reliés ». La *FMH* déclare avoir remarqué des redondances au ch. 1.4.2. Elle propose d'édicter une réglementation claire à l'échelon de l'ODEP.

1.4.3 : *Privatim* renvoie à ses déclarations au sujet du ch. 1.4.3 dans les remarques générales sur l'ODEP. *HIN* soutient expressément l'exigence de deux facteurs d'authentification. *STSAG* trouve que les critères imposés aux systèmes primaires sont inacceptables dans une ordonnance sur le dossier électronique du patient, pour la raison que les institutions doivent déjà se conformer en la matière à des règles fixées par une législation cantonale. Le ch. 1.4.3 constitue une intrusion dans la souveraineté et la sécurité des données dans les systèmes primaires et doit être purement et simplement supprimé. *K3* et *VZK* observent que les systèmes primaires affiliés sont probablement des systèmes centraux et très fréquemment utilisés (KIS) dont l'accès doit être rapide à l'usage ordinaire. Il convient de restreindre la

validité du ch. 1.4.3 pour qu'elle se limite à l'accès à un dossier électronique du patient depuis un système primaire. La *SSIM* et la *FMH* constatent que les ch. 1.4.3/1.4.3.1 énoncent des exigences applicables aux systèmes primaires. Elles demandent que l'on renonce à toute prescription pour l'authentification de systèmes primaires. *OFAC* fait valoir que les communautés ne sauraient garantir quoi que ce soit concernant les systèmes primaires dans la mesure où elles n'en sont ni propriétaires ni responsables, pas plus qu'elles ne sauraient assumer la responsabilité d'autres communautés.

BFH conclut du ch. 1.4.3.1 que les droits d'accès aux documents qui ont été repris de la plateforme eHealth pour être téléchargés vers le système primaire devraient suivre. On peut se demander si le texte implique l'intégration d'une « fenêtre d'un dossier électronique du patient » dans le système primaire, autrement dit que l'on ne travaille plus dans le système primaire lui-même, mais dans un contenu de navigateur représentant le dossier électronique du patient. En effet, la différence serait considérable et aurait sur les droits d'accès des conséquences directes, telles qu'elles ont déjà été commentées dans l'ODEP (art. 8, let. e). En tout cas, de telles procédures d'authentification dans les systèmes primaires ne sont guère en usage dans la pratique. Par ailleurs, de nombreuses autres personnes – qui ne figurent pas dans l'IPH parce qu'elles n'ont pas besoin d'un accès au dossier électronique du patient – travaillent avec le système primaire et peuvent fort bien accéder aux documents qui y ont été téléchargés, contournant ainsi le dossier électronique du patient. *KSSG* déclare que le ch. 1.4.3.1 aurait pour effet d'obliger les utilisateurs à s'identifier par une procédure d'authentification à deux facteurs chaque fois qu'une application communiquerait d'une manière quelconque avec le dossier électronique du patient, que ce soit comme source ou comme « consommateur » de documents. Les communautés doivent pouvoir garantir que tous les systèmes techniques, par ex. les systèmes primaires, utilisent (en tant qu'acteurs d'IHE Document Consumer) une procédure d'authentification renforcée pour les accès au dossier électronique du patient. *La Poste* et *IG eHealth* font remarquer que le ch. 1.4.3.1 assouplit les règles du ch. 1.4.1. Il s'agit de créer une cohérence dans les CTO. *La Poste* ajoute que l'on ne peut pas d'un côté exiger l'utilisation de MID certifiés par les éditeurs et d'un autre côté, accepter n'importe quel autre procédé au seul motif qu'un autre logiciel est utilisé pour l'accès aux données. Toujours à propos du ch. 1.4.3.1, *IG eHealth* et *La Poste* souhaitent que l'on définisse le terme de « traitement ». *VGIch* déclare qu'en ce qui concerne les systèmes primaires affiliés, le ch. 1.4.3.1 est en contradiction avec l'art. 8, let. d, ODEP et les explications qui s'y rapportent. L'art. 8, let. d et lesdites explications doivent être réadaptées en conséquence.

VAKA estime que l'exigence énoncée au ch. 1.4.3.2 n'est pas claire et s'étonne que l'on ne mentionne pas explicitement les systèmes primaires dans ce contexte. Selon l'exigence considérée, cela peut avoir d'énormes répercussions sur les prestataires. L'exigence doit être formulée de manière beaucoup plus claire. Six cantons[87] relèvent qu'une communauté ne peut pas « garantir » que les milliers de terminaux utilisés soient toujours fiables. Elle ne peut qu'informer les professionnels de la santé, le ch. 1.4.3.2 doit donc être supprimé. *La Poste* et *IG eHealth* demandent si l'exigence formulée au ch. 1.4.3.2 signifie que toutes les institutions de santé désirant raccorder un système primaire au dossier électronique du patient devront relier ce système primaire à un éditeur de MID certifié. Cela aurait des conséquences pour les établissements hospitaliers qui doivent s'y raccorder. L'exigence doit être formulée de manière beaucoup plus claire. Chez *ahdis*, on regrette que les spécifications souhaitées du terminal ne soient pas indiquées. Ce point devra être précisé.

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

La *FMH* déclare à propos du ch. 1.5 que la gestion des groupes n'est pas praticable telle que prévue et que cette disposition doit être remplacée par une réglementation générale à l'échelon de l'ordonnance. *ZH* est d'avis qu'il n'est ni nécessaire ni admissible d'informer le patient de toutes les modifications survenues dans la composition d'un groupe. Par ailleurs, le terme de « taille raisonnable » est non seulement trop vague, mais n'a pas sa place ici. Du reste, il convient de renoncer à la structure intitulée « Groupes de professionnels de la santé » Le ch. 1.5 doit dès lors être supprimé.

[87] FR, NE, GE, VS, VD, JU

Six cantons[88] font valoir que les communautés ne peuvent pas répondre des groupes de professionnels de la santé. Elles peuvent seulement prendre acte de la composition de ces groupes. Dans la version française, il convient de remplacer au ch. 1.5.1 l'élément de phrase « sont responsables de la gestion » par « sont responsables de l'administration ». Ces cantons ajoutent que le patient ne peut pas accéder à la liste intégrale des professionnels de la santé et du personnel auxiliaire d'un groupe ou d'une institution de santé. Ce n'est pas le cas dans la pratique d'aujourd'hui. De plus, la composition des institutions de santé ou de grands groupes change pratiquement tous les jours. Autrement dit, il n'est pas possible d'informer constamment le patient sur la composition des groupes. Un hôpital est un exemple d'institution à laquelle un patient peut octroyer des droits d'accès. Fractionner l'institution en « groupes de taille raisonnable » n'a aucun sens pratique. Le patient devrait alors donner des droits d'accès à une multitude de groupes qu'il ne connaît pas (radiologie, laboratoires, pathologie). Les ch. 1.5.2.1, 1.5.2.2 et 1.5.2.3 doivent par conséquent être supprimés. *OFAC* est d'avis que l'exigence formulée au ch. 1.5.2.2 n'est pas réalisable, vu que la composition des groupes change quotidiennement. S'agissant du ch. 1.5.2.3, OFAC objecte qu'une « taille raisonnable » ne veut rien dire de précis. *BFH* déplore qu'au ch. 1.5.2.1, le terme « en tout temps » ne soit pas clairement défini. Ce sont en particulier les charges administratives qui deviennent alors importantes pour des institutions de santé d'une certaine taille. Si par « en tout temps », l'on entend « à toute heure » ou « quotidiennement », cela se traduira par des charges supplémentaires considérables dans les grandes institutions de santé employant des médecins-assistants dans différentes disciplines, sans apporter nécessairement une plus-value identifiable. *AR* fait la même remarque à propos de l'expression « en tout temps identifiable » et demande que cette notion soit précisée. Il demande également que l'on précise ce que l'on veut dire au ch. 1.5.2.3 par « la taille du groupe reste raisonnable ». *La Poste* déclare que faute de définition du terme allemand « verhältnismässig » (« de taille raisonnable »), elle s'en tiendra aux souhaits exprimés par les clients. *KSSG* dénonce également l'imprécision du même terme et demande la suppression du ch. 1.5.2.3. Les groupes peuvent être subdivisés en domaines de spécialisation. La *SSIM* rappelle que la taille d'un groupe dépend de l'importance de l'institution et demande soit une précision de cette disposition, soit sa suppression. *STSAG* estime que la charge de travail générée par les dispositions des ch. 1.5.2.1 et 1.5.2.2 est inutilement disproportionnée ; d'ailleurs, le patient peut consulter les accès dans l'historique et on ne comprend pas non plus pourquoi il devrait vouloir prendre connaissance de tous les professionnels de la santé susceptibles d'être affiliés à un groupe d'accès. S'y ajoute que le contenu du ch. 1.5.2.3 est déjà régi par les droits d'accès définis dans les systèmes primaires. Les ch. 1.5.2.1, 1.5.2.2 et 1.5.2.3 doivent par conséquent être supprimés. *TI* pense que la réalisation de la gestion prévue des groupes de professionnels de la santé (1.5.2.1 et 1.5.2.2) sera loin d'être simple. Dans la pratique quotidienne, les patients n'ont pas non plus accès aux listes de tous les spécialistes d'institutions complexes (hôpitaux) qui ont pourtant accès à leurs données médicales. Ce genre de gestion en temps réel serait beaucoup trop coûteux en des endroits qui connaissent une forte fluctuation du personnel. Il convient dès lors de supprimer ces deux chiffres. De l'avis de *privatim*, les patients ne devraient pas seulement pouvoir suivre la composition actuelle des groupes, mais aussi leur modification (entrées et sorties). Les énoncés des ch. 1.5.2.1 et 1.5.2.2 doivent être mieux explicités. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* souhaitent que l'énoncé du ch. 1.5.2.2 se rapportant à l'art. 8, let. f ODEP soit complété comme suit : « les patients peuvent être informés et sont informés lorsque […] ». *Insel* et *VGIch* déclarent que dans un hôpital, l'exigence énoncée au ch. 1.5.2.2 est impraticable ou impossible à mettre en œuvre et qu'il convient donc de supprimer ce chiffre. *Tessaris* propose de compléter comme suit le ch. 1.5.2.2 : « […] lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé ou en sortent ». Par ailleurs, il serait souhaitable que le ch. 1.5.2.3 contienne un nouvel élément : « […] reste raisonnable et, en règle générale, n'excède pas le nombre de membres du groupe ».

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

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

Six cantons[89] réitèrent pour le ch. 2.1.1.1 leur prise de position relative à l'art. 20 ODEP. Ils estiment en

[88] FR, NE, GE, VS, VD, JU
[89] FR, NE, GE, VS, VD, JU

outre que les données ne doivent pas être supprimées. Les données ne sont pas effectivement effacées sur le papier ni dans les systèmes primaires et il n'y a donc aucune raison de les supprimer d'un système secondaire. Le grand avantage que présente le dossier électronique du patient, c'est que l'on pourra proposer un stockage de leurs données médicales sur une longue période. Dans le domaine de la santé, une limite de 10 ans n'a du reste pas de sens. Un patient pourrait par exemple être intéressé par un traitement médical reçu il y a 20 ans ou même dans son enfance. *NE* fait remarquer en outre que l'art. 64 de la loi cantonale sur la santé prescrit certes une période de 10 ans pour la conservation des données médicales, ce qui constitue cependant une durée minimale qui ne prend pas encore en compte l'informatisation des dossiers. Avec un dossier électronique, la problématique de la place qu'occupaient les dossiers papier dans le cabinet d'un professionnel de santé ne se pose plus dans les mêmes termes ni avec les mêmes contraintes. Ce (nouveau) contexte ne pose en effet pratiquement plus de contrainte logistique ou technique qui empêcherait le professionnel de santé de conserver les éléments du dossier au-delà de 10 ans dans l'intérêt du patient. La *FMH* renvoie ici à ses remarques relatives aux articles correspondants de l'ordonnance. *BFH* trouve que l'idée que l'on se fait de « mes données médicales dans mon dossier électronique du patient » diverge de manière incompréhensible, du point de vue de l'utilisateur, de l'obligation de principe de conserver les données dans un système de santé publique. Même si le patient en est informé et qu'il peut demander à prolonger ce délai de 10 ans (art. 9, al. 1, let. a), la question se pose de savoir pourquoi on lui demande de prendre une décision au sujet de la conservation de son dossier. D'ailleurs, le patient a de toute manière la possibilité d'effacer en tout temps les données qui le concernent. S'il devait y avoir une obligation de détruire les données, il conviendrait d'instaurer un transfert automatique dans le système de stockage pour les documents dits « privés ». À défaut, cette disposition devrait être purement et simplement supprimée du ch. 2.1.1.1. *Medshare* tient à rappeler ici que le patient décide seul du moment où des documents doivent être supprimés des systèmes de stockage et des registres. *STSAG* est d'avis qu'il serait bien plus judicieux de ne faire courir le délai de 10 ans visé au ch. 2.1.1.1 qu'à partir de la fin du traitement médical et qu'il conviendrait de le prolonger au fur et à mesure chez les patients souffrant d'une maladie chronique. Une autre option serait de ne présenter dans les registres que des données qui ont moins de 10 ans. *Tessaris* propose une formulation aux termes de laquelle la destruction des données du patient interviendrait par défaut au bout de 10 ans. C'est du reste pour le suivi des maladies chroniques que les données sont habituellement conservées sur une plus longue durée. *Tessaris* souhaite que le ch. 2.1.1.1 soit complété comme suit : « […] sont détruits après dix ans sous réserve d'une durée de conservation plus longue ». *OFAC* demande ce qu'il advient des données qui ont gardé leur importance après 10 ans. Elle se réfère à la dernière révision de la LPTh, qui exige par exemple des systèmes primaires qu'ils archivent pendant 30 ans les données relatives à l'utilisation de produits sanguins.

À propos du ch. 2.1.1.2, six cantons[90] sont d'avis que pour le cas où le patient voudrait réactiver son dossier ou pour des questions médico-légales, il ne faut pas supprimer immédiatement le dossier, mais le masquer un certain temps. *HIN* relève qu'il n'est pas précisé si les données de login devraient également être effacées dans un tel cas. Le texte parle de « toutes les données ». Or, l'art. 20, al. 1 prescrit la destruction de toutes les données qui ne sont pas requises pour répondre aux obligations de transparence ou de rapport. Le ch. 2.1.1.2 doit être formulé dans les mêmes termes que l'art. 20. *La Poste* rappelle que l'index des patients est une infrastructure qui peut être utilisée de multiples façons. Elle demande s'il est permis de n'effacer que les identités du MID qui ont été utilisées dans le dossier électronique du patient. D'autres identités utilisées pour d'autres processus (par ex. attributions ou transferts) sont maintenues. La LDEP autorise l'usage partagé d'infrastructures. Les exigences qui s'y opposent doivent être remplacées par d'autres qui le permettent dans des limites raisonnables. Le MID doit rester une exception et les données doivent être supprimées lorsqu'il n'existe aucun motif de les conserver. Selon *KSSG*, les dispositions régissant la conservation des données, par ex. celles qui figurent à l'art. 9, al. 1, let. c, ODEP et au ch. 2.1.1.2.1, ont pour effet que les cas d'application qui utilisent déjà un registre ne pourront plus être exploités sur l'infrastructure existante. Les dispositions d'exécution rendront nécessaire l'édification d'une infrastructure distincte pour le dossier électronique du patient et pour tous les autres cas d'application, ce qui aura pour effet de doubler les coûts. L'énoncé du ch. 2.1.1.2.1 doit être modifié de manière à indiquer qu'une suppression logique – sans suppression

[90] FR, NE, GE, VS, VD, JU

physique – doit intervenir dans le cas d'application « dossier électronique du patient ». Cette solution permettra de garantir que d'autres cas d'application pourront continuer de figurer dans la même infrastructure. En outre, les dispositions de l'art. 9, al. 1, let. c, ODEP et du ch. 2.1.1.2.2 ont pour effet que les systèmes d'archivage des hôpitaux ne pourront pas être utilisés comme lieux de stockage IHE pour le dossier électronique du patient. Ces prescriptions impliquent la mise en place d'un système de stockage séparé pour les documents effacés par le patient comme pour les données supprimées par les professionnels de la santé. Cela revient à édifier trois fois une infrastructure coûteuse contenant en partie des données redondantes. Si l'art. 2.1.1.2.2. a pour but une suppression physique des données, les supports d'archivage au coût modique (par ex. Centera) ne peuvent être utilisés à cet effet. Les répercussions sur les coûts seront particulièrement évidentes quand il s'agira d'archiver des images radiologiques dans le dossier électronique du patient. Les scanographies ou les examens IRM ont souvent un volume de plusieurs giga-octets et doivent être sauvegardés de manière redondante. Cet article a par conséquent une énorme incidence sur les frais d'exploitation. *KSSG* demande que toutes les données puissent être stockées physiquement sur le même système. La séparation et la suppression de données du dossier électronique du patient s'effectuent chaque fois à un niveau logique. Une séparation logique permet aussi de satisfaire aux exigences de protection et de sécurité des données. À propos du ch. 2.1.1.2.3, *KSSG* décrit également les avantages du MID et rappelle que le canton de Saint-Gall utilise depuis plusieurs années un MID pour la communication transhospitalière. Telles que définies actuellement, les dispositions d'exécution empêcheraient de continuer à exploiter le MID actuel, vu qu'un patient ne peut figurer dans le MID que s'il a donné son consentement à l'ouverture d'un dossier électronique et qu'il doit en être rayé s'il supprime son dossier. Comme il ne peut y avoir qu'un seul MID, il n'est pas possible d'en créer un deuxième pour le dossier électronique du patient. La mise en œuvre des dispositions d'exécution actuelles constituerait un recul dans les processus de traitement. *KSSG* demande que le MID puisse être utilisé à la fois pour le dossier électronique du patient et pour d'autres processus, mais ne soit pas relié à l'ID du dossier électronique du patient de la CdC si le patient n'a pas donné son consentement. En cas de suppression du dossier électronique du patient, le lien à l'ID sera tout simplement effacé.

ISSS relève qu'aux ch. 2.1.1.1 et 2.1.1.2, il est question de « détruire » les données et documents. On ignore ce que cela signifie concrètement et si la suppression (électronique) est ou non suffisante. *ISSS* propose d'introduire un ch. 2.1.1.3 qui règle les conditions de cette destruction. *Tessaris* est d'avis que l'obligation de détruire « toutes les données » s'étend aussi et surtout aux données sécurisées et aux copies de sauvegarde (back-up).

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

ZH, K3, VZK ZAD font valoir que les dispositions du ch. 2.2 découlent déjà des dispositions de la LDEP et de l'ODEP et que l'on peut dès lors les supprimer. *AR* considère judicieuses les dispositions du ch. 2.2.1.1. *BINT, Integic* et *KSSG* font remarquer quant à eux que l'architecture du stockage est en constante évolution et ne doit pas être ancrée de manière immuable dans un texte d'ordonnance. Dix-sept participants[91] craignent que cette disposition n'alourdisse les charges des prestataires. La *SSIM* et la *FMH* critiquent en outre le fait que les dispositions du ch. 2.2.1.1 obligent les prestataires à créer un lieu de stockage redondant, ce qui a pour effet supplémentaire de compliquer l'échange bidirectionnel de données visé par la LDEP. *BFH* demande si le système de stockage des documents peut être exploité dans un environnement virtualisé. *SUVA* considère qu'il est peu utile de vouloir dicter à la communauté l'architecture du système de stockage. Ces architectures évoluent très rapidement et vouloir les fixer dans les prescriptions d'une ordonnance n'a guère de sens. Neuf participants[92] au total se prononcent pour la suppression du ch. 2.2.1.1. La *CDS* et 10 cantons[93] demandent au minimum que ces règles soient simplifiées et que l'on autorise également le recours au système de stockage des documents utilisé pour le KIS (ZAD utilise dans sa prise de position le terme de « système primaire »), moyennant le cas échéant l'observation de certaines consignes techniques de sécurité. *ZH* souligne

[91] K3, VZK, SSIM, FMH, ZAD, CDS, BL, GL, LU, OW, UR, ZG, FR, NW, ZH, TG, SZ
[92] BINT, Integic, VAKA, SSIM, FMH, KSSG, K3, VZK, SUVA
[93] CDS, ZAD, BL, GL, LU, OW, UR, FR, NW, ZG, ZH, SZ

que les éventuelles consignes techniques de sécurité ne doivent pas être trop restrictives sous peine d'entraîner une flambée des coûts chez les prestataires. *HIN* relève qu'une séparation logique devrait suffire et propose l'énoncé suivant pour le ch. 2.2.1.1 : « les documents du dossier électronique du patient peuvent être séparés en tout temps d'autres documents mémorisés dans le lieu de stockage par un procédé qui assure une séparation logique contrôlée ». *IG eHealth* et *La Poste* trouvent ambigu le terme « uniquement », car on pourrait l'interpréter comme une nécessité de stocker en duplicata. Une telle pratique serait contraire au bon sens, car elle doublerait les coûts et rendrait la manutention irréalisable et fortement sujette à des erreurs. Ils proposent donc de biffer le terme « uniquement » du ch. 2.2.1.1.

IG eHealth constate que dans le texte du ch. 2.2.1.2, il est question de l'« annexe 3 » alors qu'il faudrait sans nul doute parler de l'annexe 4, une erreur à rectifier. *La Poste* demande s'il est permis d'introduire des documents « on demand » (à la demande) dans le dossier électronique du patient. La norme CDA-CH-MTPS est basée sur les documents « on demand ». *La Poste* fait aussi valoir que les dispositions en la matière sont extrêmement restrictives et empêchent toute adaptation à de nouvelles technologies, ce qu'il s'agit d'éviter. Si par « formats de fichier autorisés », on entend la liste énoncée au ch. 1.9 (MIME Type du document) de l'annexe 3, *ZH* fait valoir qu'il est problématique de restreindre le nombre de formats de fichier autorisés. D'abord, la conversion en un format autorisé n'est pas toujours réalisable techniquement, et ensuite, elle ne devrait pas toujours être nécessaire. Les formats tels que PNG ou SVG notamment, mais aussi des documents texte, devraient pouvoir être pris en charge. Par ailleurs, l'indication de formats tels que TIFF ou XML est trop vague. *ZH* recommande donc le remaniement ou la suppression pure et simple du ch. 2.2.1.2.

GE, *VD*, *VS*, *JU* et *FR* jugent les dispositions du ch. 2.2.1.3 trop restrictives. Il existe aujourd'hui la norme PDF/A-3, introduite par la révision selon ISO 19005. D'autre part, on pourrait aussi utiliser la norme PDF/X (ISO 15930). Ces normes évoluent régulièrement. Des détails techniques n'ont pas leur place dans un texte législatif contraignant et il convient dès lors de supprimer ce chiffre. *IG eHealth* observe qu'une restriction du choix des formats à la norme PDF/A-1 ou PDF/A-2 pourrait bien se traduire par une conversion obligatoire des données. Cette transformation implique le risque d'une perte d'information ou d'intégrité. Le système ne doit pas procéder à des conversions de format. Par conséquent, le système doit accepter des données du format PDF/A-1 ou PDF/A-2. Tous les autres formats sont rejetés, ce qui pourrait créer un grand problème d'acceptation chez les utilisateurs. Ces cantons demandent donc la suppression du ch. 2.2.1.3. *Integic* reproche aux indications concernant les normes PDF/A-1 et PDF/A-2 d'être trop imprécises, étant donné que les exigences et surtout la lisibilité divergent fortement entre ces deux sous-versions. Le format PDF/A-1a, par exemple, se prête à un archivage de longue durée et à des applications accessibles à tous, tandis que le format PDF/A-1b ne s'y prête pas du tout. Les normes PDF/A-1 et PDF/A-2 sont plutôt le fruit de technologies évolutives qui se chevauchent, tandis que leurs sous-versions régissent la sémantique de manière plus concrète[94]. *Integic* demande que l'on fournisse des précisions sur les sous-versions autorisées de PDF/A-1 et PDF/A-2. *ZH* rappelle que les formats PDF/A-1 et PDF/A-2 ont été développés précisément pour l'archivage. Si l'ordonnance prescrit que seuls ces formats peuvent être utilisés, cela se traduira par l'obligation de convertir de nombreux documents sans qu'il y en ait un besoin manifeste. Les besoins du dossier électronique du patient n'imposent pas de prescrire ces formats et il convient donc de supprimer cette disposition. La *FMH* demande à propos du ch. 2.2.1.3 si l'on n'en est pas déjà à la version PDF/A-3. Le législateur n'a pas à introduire des spécifications si précises dans un texte de loi, surtout pas dans ce domaine en constante évolution. *La Poste* considère que le ch. 2.2.1.3 dicte une exigence inutilement contraignante. Les données doivent être effacées au bout de 10 ans. La plupart des applications ne proposent pas ce format d'archivage en standard. Elle demande donc que l'on définisse le comportement attendu du système. Le système ne doit procéder à aucune conversion de format parce qu'il y a toujours un risque que des données importantes pour le traitement soient perdues ou modifiées.

2.3 Gestion sur demande des patients (al. 2)

[94] http://www.pdfa.org/wp-content/uploads/2011/10/Flyer-PDFA2-Uebersicht-DE.pdf

Pour le ch. 2.3, la *FMH* renvoie à ses remarques relatives aux articles correspondants de l'ordonnance. *OFAC* relève qu'en plus de la matrice de niveau de confidentialité/droits d'accès, on demande une gestion « à la carte » des types de document par patient. Outre le côté surréaliste de cette demande du point de vue technique, il est probablement dangereux du point de vue médical d'entretenir un dossier électronique incomplet. Et cela en raison du fait que des professionnels de la santé prendront probablement, dans des situations d'urgence, des décisions médicales sur la seule base du dossier du patient. Une telle complexité serait donc non seulement inutile et irréalisable mais aussi probablement dangereuse pour la santé du patient. *IG eHealth* et *La Poste* reprochent à la disposition formulée au ch. 2.3.1.1.1 de manquer de clarté. La publication de documents est l'affaire des professionnels de la santé et non des communautés. C'est du patient, et non des communautés, que les professionnels de la santé doivent en principe recevoir leurs instructions. En outre, les communautés ne savent pas comment interpréter la notion de « données déterminées ». L'exigence doit être formulée plus précisément, car elle est inapplicable en l'état. *KSSG* déplore que la disposition au ch. 2.3.1.1.1 soit impossible à mettre en œuvre. Si, par exemple, un patient ne veut pas que son test VIH effectué dans le cadre d'un bilan complet (série d'analyses) soit publié dans le dossier électronique du patient, la seule option alternative à la publication des résultats de laboratoire complets est de ne pas publier de rapport du tout. Cette disposition exige par ailleurs que l'aval du patient soit recueilli avant toute publication. *KSSG* demande donc la suppression de l'art. 9, al. 2, let. a ODEP et du ch. 2.3.1.1.1, étant donné que le patient a toujours la possibilité de définir le niveau de confidentialité « secret » pour ses données. Il convient par ailleurs de mieux définir les termes « données » et « documents ». *STSAG* considère que les exigences formulées au ch. 2.3.1.1.1 constituent une charge disproportionnée pour les communautés. Il s'agit d'une tâche dont tout patient capable de discernement peut au besoin se charger lui-même. Et comme la communauté de référence a aussi une fonction de service d'assistance pour le patient, c'est à elle que reviendrait cette tâche s'il fallait la déléguer. *STSAG* demande donc la suppression pure et simple de ce chiffre. Six cantons[95] sont d'avis que le patient qui ne souhaite pas voir ses données médicales inscrites dans son dossier électronique doit en parler au professionnel de la santé qui l'a pris en charge. La communauté ne peut pas empêcher l'enregistrement de données médicales. Ils demandent donc la suppression du ch. 2.3.1.1.1.

Les mêmes cantons demandent également la suppression du ch. 2.3.1.1.2, vu que les données médicales ne doivent pas être détruites et qu'une demande de prolongation n'a aucun sens. Aussi déclarent-ils qu'un patient ne devrait pas pouvoir effacer de données médicales de son dossier électronique. De plus, supprimer des données d'un système secondaire n'a pas de sens vu que ces données restent dans le système primaire. Un patient qui voudrait masquer ses données peut les classer secrètes. En cas de problème médico-légal, il sera important de savoir à quelle date le patient a masqué ses données et si le professionnel de la santé avait la possibilité de le savoir d'avance. Il convient donc de supprimer également le ch. 2.3.1.1.3. Pour ce qui est des ch. 2.3.1.1.1 à 2.3.1.1.3, *K3* et *VZK* déplorent qu'il manque une réglementation contraignante pour les documents provenant d'une autre communauté et consultables (par le biais de XCA) dans le dossier électronique du patient. XCA est un accès en « lecture seule » sans droits d'écriture, de mutation ni de suppression. La suppression intégrale des données nécessite une réglementation à laquelle serait soumise l'association suisse des communautés, espace de confiance du dossier électronique des patients. Cette remarque vaut aussi pour les autres chiffres. *K3* et *VZK* proposent que l'on crée des règles appropriées. *ZH* estime à propos du ch. 2.3.1.1.3 qu'il n'est pas nécessaire que le patient puisse demander la destruction de données de son dossier électronique. Le dossier électronique du patient doit en effet rester complet. Ce n'est qu'ainsi que l'on pourra garantir que les données resteront à disposition, par exemple dans un contentieux juridique. Il suffit amplement que le patient puisse leur attribuer le niveau de confidentialité « données secrètes ». Ce chiffre doit donc être supprimé. Chez *medshare*, on souligne à propos du ch. 2.3.1.1.2 qu'un dossier électronique d'un patient lui appartient pour la vie dès son ouverture et que dès lors, lui seul a le droit d'en supprimer le contenu. Ils demandent donc la suppression de ce chiffre. Pour le ch. 2.3.2, *privatim* renvoie à son commentaire dans les remarques générales relatives à l'ODEP.

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

[95] FR, NE, GE, VS, VD, JU

K3, *VZK*, *ZAD* et *ZH* relèvent que les prescriptions découlent déjà des dispositions de la LDEP et de l'ODEP. *VAKA* propose que le patient ait la possibilité de n'accorder aucun droit d'accès. D'après *OFAC*, la traduction des niveaux de confidentialité en français est une véritable catastrophe. Certains niveaux portent le nom d'une catégorie de données personnelles telles que définies à l'art. 3 LPD et, selon le sens commun, la plupart des données appartiennent de fait à plusieurs catégories : une donnée médicale est aussi en même temps une donnée utile et sensible ! Il n'est pas logique que les données médicales d'un dossier électronique du patient ne se trouvent qu'au deuxième niveau et soient surclassées par deux niveaux supérieurs. Six cantons[96] demandent que l'on explique tous les échelons et leur fonctionnalité dans la pratique puis que l'on complète ces explications par des exemples concrets. *Integic* relève qu'aux termes des dispositions du ch. 2.4.1.3, et en fonction des paramétrages d'accès choisis, les professionnels de la santé ne pourraient plus voir les données qui auraient été classées « sensibles ». Il convient donc de dire clairement qu'il faut absolument donner aux professionnels de la santé le droit de modification des niveaux de confidentialité, quitte à instaurer un droit distinct pour la modification. *SQS* fait remarquer que les descriptions des quatre niveaux de confidentialité mentionnés sont traduites à l'annexe 3 Métadonnées, 1.5 Niveaux de confidentialité. Le niveau de confidentialité pourvu du code 30002 est appelé « useful medical data » en anglais et « nützliche Daten » en allemand. Les autres codes ont la même désignation en anglais et en allemand, ce qu'il convient de faire aussi dans ce cas. *STSAG* demande l'énoncé suivant pour le ch. 2.4.1 : « Les communautés de référence doivent garantir […] » et ajoute à propos du ch. 2.4.1.3 que cette fonction doit être automatisée et rendue réalisable par l'entremise de services ad hoc.

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

La *FMH* fait remarquer qu'il ne s'agit pas ici d'une « décision d'accès […] demandée à la communauté de référence », mais d'une demande de vérification à laquelle il faut donner une réponse favorable. Ailleurs, le texte allemand parle d'« Authorisierungsentscheid » (décision d'autorisation). Il s'agit donc de revoir et d'uniformiser la terminologie utilisée dans cette langue. Pour *GE*, *FR*, *VS*, *VD* et *JU*, le ch. 2.5.1.1 est peu clair. Ils demandent si les communautés doivent demander à la communauté de référence quels droits le patient leur a accordés et sous quelle forme. Ces droits sont contenus dans un registre d'autorisations lié au MID et auquel les communautés doivent avoir accès. Il convient de clarifier et de préciser l'use case.

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

À propos du ch. 2.6, la *FMH* renvoie aux remarques qu'elle a formulées à propos des articles de l'ordonnance qui s'y rapportent, tandis que *ZH*, *K3*, *VZK* et *ZAD* demandent une simplification de ses dispositions, les jugeant trop compliquées. *STSAG* est d'avis que les tâches figurant au ch. 2.6.1 devraient être déléguées aux communautés de référence. *TI* considère que ces dispositions ne sont pas praticables dans une situation d'urgence. Il faut simplifier la procédure en proposant des réponses à choix. Le professionnel de la santé qui force l'accès dans un cas d'urgence doit motiver ultérieurement son acte. De même, la *SSIM*, *BINT*, *IG eHealth*, *SUVA* et la *FMH* demandent le remplacement du terme « au préalable » par « ultérieurement » au ch. 2.6.1.1, car une justification ultérieure des motifs du professionnel de la santé suffit amplement. À propos du ch. 2.6.1.1, *medshare* rappelle qu'en cas d'urgence, chaque minute compte pour le patient, raison pour laquelle les prestations médicales ont priorité absolue sur les procédures administratives. Le texte doit donc être adapté comme suit : « qu'une justification […] est donnée dans les 24 heures qui suivent ». *VAKA* estime au contraire que l'on peut se passer entièrement d'une justification, et donc supprimer le ch. 2.6.1.1.

USB plaide pour le maintien d'un accès aussi simple que possible pour les professionnels de la santé en cas d'urgence. Il propose à cet effet de fusionner les ch. 2.6.1.1 et 2.6.1.2 et de reformuler le texte comme suit : « L'accès en cas d'urgence est saisi en tant que tel dans l'historique et se distingue des

[96] FR, NE, GE, VS, VD, JU

autres accès ». *IG eHealth* et *La Poste* font remarquer qu'en cas d'urgence médicale, l'exigence énoncée au ch. 2.6.1.2 complique singulièrement le travail avec le dossier électronique du patient et qu'il faut veiller ici à un minimum de convivialité. Ils demandent que les professionnels de la santé puissent toujours voir clairement qu'ils sont en présence d'un cas d'urgence et que l'accès a lieu sur une autorisation d'urgence. C'est pareil pour les documents apportés au dossier par le patient. Le professionnel de la santé ne doit pas non plus confirmer à chaque fois que la source des données est connue. *SCH* rappelle que dans une situation d'urgence, l'accès doit être très rapide et que le professionnel de la santé est déjà enregistré. Compliquer la procédure d'accès n'apporte aucun avantage supplémentaire vu que le professionnel de la santé est déjà identifié. Il convient donc de supprimer le ch. 2.6.1.2. *SUVA* plaide pour que l'accès en cas d'urgence soit possible rapidement sans formalisme et puisse aussi être justifié a posteriori. Le ch. 2.6.1.2. doit se lire ainsi : « qu'un accès en cas d'urgence est possible même sans double confirmation ». *ISSS* demande entre autres comment protéger ces accès en cas d'urgence contre les abus et en quoi consiste exactement l'action manuelle dont il est question ici. Une formulation détaillée du processus est nécessaire.

La *SSIM* préconise de remplacer le terme « aussitôt » par « ultérieurement » au ch. 2.6.1.3. *La Poste* demande à ce propos ce que l'on entend par « aussitôt » et si l'on peut opter pour la voie postale. La *FMH* estime que l'information systématique et subséquente avec justification éventuelle en cas de suspicion d'abus est une solution appropriée et doit dès lors suffire.

Integic souhaite que les conditions cadres soient complétées d'un exposé de la façon dont doit se faire la prise de contact. *HIN* observe à propos du ch. 2.6.1.4 que l'information peut contenir des données sensibles, mais doit alors bien entendu être communiquée uniquement par des canaux sécurisés conformément aux exigences de la protection des données. La disposition doit être modifiée ou complétée comme suit : « […] en cas d'urgence et transmise par […] (p. ex. SMS, courriel, etc.) doit, si elle contient des données sensibles, être communiquée par des canaux sécurisés conformément aux exigences de la protection des données. À défaut, cette information ne doit contenir que la mention qu'un accès d'urgence a eu lieu, avec date et heure exacte de l'intervention, ainsi que le renvoi au dossier électronique du patient pour y lire les circonstances exactes de l'accès au dossier ». Un avis partagé par la *CCM*, *BüAeV*, *GAeSO* et *KAeG SG*, qui demandent la modification suivante de l'énoncé : « que seules sont transmises l'information qu'un accès d'urgence a eu lieu, avec date et heure exacte de l'intervention, ainsi que la mention que les circonstances exactes de l'accès figurent dans le dossier électronique du patient ».

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

BINT critique le fait que la disposition énoncée au ch. 2.7 pourrait faire monter les frais indéfiniment étant donné que l'on ignore le scénario et la fonctionnalité. Six cantons[97] estiment que le cadre des scénarios de tests doit être laissé à l'appréciation de l'organisme de certification et des fournisseurs. Suivant le nombre de tests, une automatisation n'est pas nécessaire et complique inutilement la structure. En outre, ce genre de détail n'a pas sa place dans un cadre législatif contraignant. Ils demandent donc la suppression du terme « automatisés » au ch. 2.7.1. Dans le contexte des scénarios de tests automatisés, *privatim* demande à quelles données l'accès sera possible et par qui. Ils demandent que les règles en soient précisées et soulignent l'importance d'éviter tout accès non autorisé aux données. De son côté, *SQS* demande qui décide au juste quand les fonctionnalités et les évaluations des règles peuvent être considérées comme correctes. Il convient donc de compléter cette disposition d'un ch. 2.7.2, de fixer ou déterminer les valeurs admises pour la vérification et de définir qui est compétent pour fixer ces valeurs.

2.8 Métadonnées (al. 3, let. c)

Pour le ch. 2.8, la *FMH* renvoie à ses remarques relatives aux articles correspondants de l'ordonnance. *HIN* et *SQS* présument à propos des métadonnées qu'il est question de l'annexe 3 et non de l'annexe

[97] FR, NE, GE, VS, VD, JU

4, une erreur à corriger. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* relèvent eux aussi la référence erronée à l'annexe 4 de l'ODEP-DFI. En effet, l'annexe 4 traite des formats d'échange et non des métadonnées. Il faut donc admettre qu'il est question ici de l'annexe 3. *IG eHealth* et *La Poste* critiquent l'énoncé très rudimentaire et minimaliste du ch. 2.8.1. Ils rappellent la nécessité de tenir les métadonnées à jour et demandent que les CTO prescrivent aux communautés comment appliquer les ajustements des métadonnées relatives à la vitesse, l'intégralité, etc.

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

Là aussi, la *FMH* renvoie à ses remarques relatives aux articles correspondants de l'ordonnance. *SQS* demande s'il existe un règlement de traitement des données pour la CdC, car il a cherché en vain un tel règlement sur le site zas.admin.ch. C'est là un point à vérifier et à préciser. Six cantons[98] reprochent au ch. 2.9 d'être truffé de détails techniques qui sont susceptibles d'évoluer et n'ont donc pas leur place sous cette forme dans un cadre législatif contraignant. Son texte doit être simplifié et purgé de toute référence à des normes évolutives. *ZH* se rallie à cette requête et relève qu'il n'est pas raisonnable de donner autant de consignes techniques. Invoquant que l'on ne peut pas demander à tous les acteurs de la branche d'observer toutes les régulations si la CdC en est dispensée, *medshare* propose d'obliger la CdC à implémenter le système IHE XCPD et d'inviter les communautés à l'utiliser pour la recherche de NIP de dossiers électroniques auprès de la CdC.

2.9.1/2.9.2 Interface standard avec la base de données d'identification de la CdC : *VAKA* met en garde contre l'obligation d'utiliser des interfaces supplémentaires. Les profils mis à disposition par *IHE* sont déjà difficiles à mettre en œuvre. À l'instar de *K3* et *VZK*, il demande la suppression des interfaces supplémentaires. De l'avis de *privatim*, ce n'est pas le rôle des points d'accès des communautés de le garantir, mais bien celui des communautés elles-mêmes. Le texte doit être réadapté, les points d'accès n'étant pas des sujets tenus par une obligation d'agir. Six cantons[99] font remarquer qu'il est inutile de rappeler des tautologies, d'autant plus que la communauté doit démontrer qu'elle a connaissance des prescriptions, mais non qu'elle les respecte. Ils réclament la suppression du ch. 2.9.2. Une demande partagée par *VAKA*, *K3* et *VZK*, qui ajoutent que de telles dispositions ne doivent pas être ajournées, mais doivent impérativement trouver leur place dans le texte des présentes ordonnances.

2.9.3 Profils d'intégration, adaptations nationales des p. i. et p. i. nationaux : *BINT* et *Integic* soulignent la nécessité de pouvoir prouver cette conformité auxdits profils IHE. Ce critère ne pouvant pas être certifié de manière crédible sans déclaration de conformité ni preuve de réussite des tests IHE Connect-A-Thon, il y a lieu d'en exiger la production pour les profils IHE souhaités. *La Poste* critique le fait que le champ d'application du ch. 2.9.3 n'est pas clairement défini. Cette disposition ne doit servir qu'à l'échange entre communautés et non à l'intérieur d'une communauté. Le ch. 2.9.3 doit donc être complété comme suit : « Pour la transmission d'information entre communautés, celles-ci doivent pouvoir utiliser […] ».

2.9.4 Acteurs et transactions des profils d'intégration – Communication intercommunautaire : *BINT* et *HIN* sont d'avis […] que les accès intercommunautaires doivent être gratuits. Donner aux communautés le droit de percevoir des taxes de roaming compromettrait la généralisation du dossier électronique du patient et réduirait la portée fédératrice de la LDEP. Cela poserait aussi le risque de voir apparaître des monopoles, le portail des patients étant déjà sous le contrôle restreint de son opérateur. Ils demandent donc que le ch. 2.9.4 soit complété ainsi : « […] supporter gratuitement […] selon l'annexe 5 ODEP-DFI ». *IG eHealth* et *La Poste* observent que l'exigence formulée au ch. 2.9.4.2 ne devrait pas être nécessaire. Le ch. 2.9.2 définit l'interface avec la CdC. Cette dernière offre aussi un service Web. Ces intervenants rappellent aussi que SEDEX n'est pas gratuit et demandent qui devra assumer ces frais. Ils proposent de supprimer cette exigence. *BINT*, *Integic*, *IG eHealth* et *ahdis* se prononcent pour la suppression du ch. 2.9.4.4. La Patient Location Query dans l'annexe 5 ODEP-DFI est explicitement exclue. *BINT*, *Integic* et *ahdis* plaident en outre pour l'introduction d'un ch. 2.9.4.5 ; Update Document

[98] FR, NE, GE, VS, VD, JU
[99] FR, NE, GE, VS, VD, JU

Set Cross Community [ITI-xxx]. Ils disent que les transactions intercommunautaires sont nécessaires pour modifier les niveaux de confidentialité de métadonnées d'un document dans une autre communauté. Ils souhaitent aussi l'introduction d'un ch. 2.9.4.6 ; On-Demand Documents Option (voir ITI TF-2a, 3.18.4.1.2.5).

SQS fait remarquer qu'il est impossible de procéder à des vérifications techniques si approfondies dans le cadre de l'audit d'un système de gestion ; ce serait d'ailleurs contraire à l'esprit d'un audit (contrôle par sondage). Les exigences énoncées ici sont des critères de réception qui doivent être obligatoirement remplis, validés et historisés dans le cadre des mises en service de systèmes et d'interfaces. Ces réceptions doivent être réglées hors de la procédure de certification proprement dite, par ex. dans le cadre d'un examen technique. Les contrôles effectués dans le cadre de la certification ont pour but exclusif de vérifier si ces examens ont bel et bien eu lieu et si les éventuelles constatations ont fait l'objet d'un suivi. La gravité d'un constat n'est pas définie dans la norme de certification. *SQS* demande en l'occurrence que les ch. 2.9.4 à 2.9.21 soient complétés de dispositions régissant la fourniture de preuves que les conditions techniques ont fait l'objet d'un examen technique, une exigence qu'elle répète pour tous les chiffres concernés.

2.9.5/2.9.6 Acteurs et transactions des profils d'intégration – Communication d'identités attestées : Au sujet du ch. 2.9.5, *KSSG* écrit qu'à son avis, XUA ne suffit pas et qu'il faut utiliser XUA++. *ahdis* fait remarquer que le ch. 2.9.6 omet d'expliquer comment l'acteur X-Service User obtient l'assertion de l'acteur X-Assertion Provider et quelle doit être sa relation avec le User Authentification Provider.

2.9.9 Acteurs et transactions des profils d'intégration – Mise à disposition de documents : *KSSG* demande s'il est impératif que les documents soient enregistrés dans le lieu de stockage au moyen du Provide and Register Document Set-b. On pourrait aussi imaginer que les documents sont enregistrés dans le lieu de stockage par HL7 MDM puis stockés dans le registre à l'aide de la transaction Register Document Set. C'est la solution qui a été choisie à Saint-Gall parce que certaines sources de documents ne prenaient pas en charge le Provide and Register Document Set-b. Pour les dispositifs médicaux, il est plutôt improbable que cette exigence ait été développée pour le marché suisse. Cette disposition doit être étendue à d'autres variantes de documents pour qu'on puisse autoriser leur enregistrement dans le lieu de stockage.

2.9.10 Acteurs et transactions des profils d'intégration – Mutation des métadonnées de documents : *IG eHealth* et *La Poste* demandent qui peut assumer le rôle de « Document Administrator ». Si les droits d'auteur étaient reconnus, il est évident que chaque auteur serait implicitement le « Document Administrator » des documents qu'il a publiés. Mais ce ne serait plus possible dans le cas contraire. Ils ajoutent que Update Document et Delete Document sont des fonctions puissantes et qu'il faut savoir qui sera habilité à les exercer. Ils demandent que la question soit tirée au clair au cas où cette fonction ne reviendrait pas implicitement à l'auteur. *IG eHealth* ajoute à propos du ch. 2.9.10.1 qu'en vertu de l'art. 1, al. 1, ODEP, il faut toujours indiquer un niveau de confidentialité. Ils recommandent en outre la suppression du ch. 2.9.10.2, car il suffit de modifier les métadonnées.

2.9.11 Acteurs et transactions des profils d'intégration – Registre de documents : *IG eHealth* et *La Poste* soulignent que la LDEP met l'accent sur l'espace de confiance entre les communautés. Les transactions XDS.b sont « hors champ d'application » (out of scope). Les champs d'application de la LDEP, de l'ODEP et des CTO doivent être mieux définis. *Integic* signale à propos du ch. 2.9.11.2 que la désignation correcte est « Registry Stored Query », à corriger. Il dit également avoir relevé des incohérences dans les transactions mentionnées. En effet, une partie des transactions indiquées sont de celles que les acteurs doivent pouvoir exécuter ou réceptionner/traiter eux-mêmes. Il y a des lacunes dans les transactions qui doivent être prises en charge par les acteurs IHE respectifs (réception et envoi). Par exemple, 2.9.12. doit prendre en charge ITI-42, car cette transaction s'effectue du Document Repository au Document Registry, alors qu'elle n'est indiquée que pour Document Registry (2.9.11). Il convient donc de corriger ces incohérences.

2.9.12 Acteurs et transactions des profils d'intégration – Lieux de stockage des documents : *Integic* réitère d'une part la prise de position émise au sujet du ch. 2.9.11, et critique d'autre part l'absence totale de la transaction ITI-64, essentielle aux processus de clearing et à l'amélioration de la qualité des données dans les registres de référence, ainsi que du profil IHE XAD-PID Change Management qui lui est associé. La transaction ITI-64 doit donc être complétée. *KSSG* réitère à propos du ch. 2.9.12.1 sa position déjà prise à l'égard du ch. 2.9.9.

2.9.15 Acteurs et transactions des profils d'intégration – Gestion de l'index des patients : *BINT* réitère son commentaire du ch. 2.9.4 pour le ch. 2.9.15.3 et propose, comme *Integic* et *ahdis*, de supprimer ce dernier chiffre. Il n'est pas nécessaire de prévoir un message de mise à jour pour les ID du patient. Le cas d'application n'est pas reconnaissable.

2.9.16 - 2.9.18 Acteurs et transactions des profils d'intégration – Authentification des systèmes et historisation des transactions IHE : *Integic* et *ahdis* demandent la suppression de l'élément de texte « grouped with Any IHE Actor » aux ch. 2.9.16 et 2.9.17. D'après *medshare*, Secure Applications et Secure Nodes doivent être traités à égalité. Les sous-points des ch. 2.9.17 et 2.9.18 doivent figurer dans les deux chiffres. *IG eHealth*, *Integic* et *ahdis* demandent l'ajout d'un ch. 2.9.18.2 « Maintain Time [ITI-1] », conformément à l'annexe 5 ODEP-DFI, point 1.4.2.4 ATNA Secure Application.

2.9.22 – 2.9.24 Authentification avec des certificats valables : À propos des certificats électroniques délivrés par les services de certification en vertu de la loi sur la signature électronique (SCSE), *OFAC* déclare que la SCSE règle les conditions de reconnaissance des prestataires de services de certification dans le domaine de la signature électronique, ainsi que leurs droits et devoirs. La SCSE définit le cadre qui permet aux personnes physiques de signer électroniquement des documents, mais elle est limitée au domaine de la signature électronique et ne couvre en aucun cas les modalités d'identification et d'authentification des personnes morales et leurs différents points d'accès techniques. L'exigence d'acquérir les certificats auprès de fournisseurs de signatures électroniques n'est pas fondée et n'apporte du reste au dossier électronique du patient aucune garantie supplémentaire sur le marché vis-à-vis de l'organisme de certification. *La Poste* demande à propos du ch. 2.9.22 si les certificats logiciels sont autorisés. *medshare* fait valoir que la CdC ne devrait pas être traitée différemment des services centraux de recherche. Elle propose de fusionner ce chiffre avec le ch. 2.9.22.3 et de faire de même dans l'art. 38, al. 1, ODEP. Au ch. 2.9.23, *medshare* signale que la référence aux documents fait défaut. Par ailleurs, *medshare* réitère pour le ch. 2.9.24 le commentaire déjà émis à l'égard du ch. 2.9. CT (consistent time) est une condition sine qua non pour l'ATNA. L'ATNA est une condition dictée par les autres profils IHE. Il serait plus judicieux selon *medshare* que CT prenne comme source l'heure suisse.

2.9.25 Cohérence de l'heure en Suisse : *SQS* veut savoir qui décide quels sont les systèmes pertinents de traitement de l'information et comment. Un smartphone ou une tablette, par exemple, sont-ils des systèmes pertinents ? Des déclarations de ce type peuvent être interprétées et évaluées différemment dans des audits. *SQS* demande concrètement une description explicite de la notion de « système pertinent de traitement de l'information ». *IG eHealth* et *La Poste* demandent de leur côté pourquoi l'on ne référence pas ici le profil CT.

2.10 Données historisées (al. 3, let. e) – Exigences concernant le système d'historisation

FMH renvoie à ses remarques faites à propos des articles pertinents de l'ordonnance, mais tient surtout à rappeler que l'historisation des accès engage également la responsabilité civile des personnes traitantes. Elle doit impérativement servir à établir quelles données ont été consultées par un professionnel de la santé au moment de son accès.

2.10.2 : Sept participants[100] demandent ce qu'on entend par « ce qui est nécessaire » ou comment on le définit. *K3*, *VZK*, *ZAD* et *ZH* demandent la suppression de cette dénomination. *ZH* demande en plus

[100] IG eHealth, Integic, K3, VZK, ZG, ZH, ZAD

que l'historique – contrairement à ce qui est dit au ch. 2.10.2 – montre quelles données ont été consultées, sinon le patient n'est pas en mesure d'apprécier si l'accès était ou non licite. Il faut aussi veiller à ce que l'historisation soit complète en toutes circonstances. Ce n'est qu'ainsi que l'on peut créer la confiance en ce système. *IG eHealth* souhaite que la notion « erforderliches Mass » (version allemande de « ce qui est nécessaire ») soit incluse dans les définitions terminologiques, faute de quoi la mesure de ce qui est nécessaire devra être régie par un règlement d'exploitation au niveau national. *ZG* propose que l'on précise cette notion. D'après *medshare*, la notion de « donnée médicale » est floue et il convient de la préciser.

2.10.3 : *IG eHealth* et *La Poste* demandent s'il est approprié qu'il suffise de pouvoir établir qu'une modification a eu lieu ultérieurement. Ils proposent de modifier comme suit l'énoncé du ch. 2.10.3.2 : « […] des données historisées doit être impossible. » À propos des modifications ultérieures de données historisées, *Tessaris* observe qu'il pourrait fort bien s'agir de données dont la pratique a révélé qu'elles étaient erronées ou incomplètes. Dans ce cas, il devrait être possible de corriger ou de compléter des données historisées, mais non de les modifier rétroactivement. Les compléments, correctifs ou modifications d'inscriptions historisées doivent être marqués comme tels, complétés d'informations sur l'auteur et horodatés.

Bleuer fait valoir à propos du ch. 2.10.3.3 que l'historisation d'une consultation par le patient de ses propres données constitue une ingérence dans la sphère privée des citoyens et doit par conséquent être expressément autorisée par le patient. Selon *ZH*, le dossier électronique du patient doit être paramétré de telle manière qu'un administrateur système n'a aucun accès aux données médicales du patient. Les données doivent être cryptées et les clés de cryptage administrées de manière à empêcher toute lecture de ces données par les administrateurs OS et les administrateurs DB. Le cryptage doit être effectué sur toutes les données. Au sujet des ch. 2.10.3.3 et 2.10.3.4, *privatim* fait remarquer que le patient doit pouvoir se rendre compte que des administrateurs système ont eu accès à son dossier électronique. Il demande que la réglementation soit adaptée en conséquence.

SQS relève à propos du ch. 2.10.3.4 qu'il sera toujours possible de contourner des restrictions techniques moyennant des droits d'accès appropriés. Le problème devra par conséquent être résolu par la voie administrative. La restriction des droits d'administrateur doit faire l'objet d'une directive. *KSSG* adhère à ce point de vue et considère que des données historisées sont toujours manipulables jusqu'à leur archivage, ce qui pose des limites à la portée effective de cette règle. Il convient par conséquent de biffer le ch. 2.10.3.4 ou de l'adapter. *SCH* met également en doute la faisabilité technique du ch. 2.10.3.4 et propose la variante suivante : « Les logs système doivent pouvoir être sauvegardés de manière conforme aux critères de révision ». *BFH* est d'avis que les administrateurs système ne doivent pas non plus pouvoir effacer ni désactiver l'historisation d'autres activités, et demande d'adapter comme suit le ch. 2.10.3.4 : « […] effacer ou désactiver l'historisation des activités ».

2.10.4 : *Integic* fait valoir que les saisies dans l'historique visées au ch. 2.10.4 constituent une atteinte à la vie privée du citoyen dans la mesure où elles impliquent la consultation de ses propres données. Le patient doit pouvoir décider s'il autorise ou non ce processus. *SUVA* déclare également que cette disposition viole la sphère privée du patient. Le patient doit rester libre de décider quand et comment consulter ses propres données sans qu'un professionnel de la santé ne le sache. Il faudra sans nul doute trouver une autre solution compatible avec la LPD. Six cantons[101] critiquent la traduction française du ch. 2.10.4.1.3 et proposent l'énoncé suivant : « configuration des autorisations ou gestion des autorisations ».

Au sujet du ch. 2.10.4.2, *La Poste* et *IG eHealth* demandent s'il est bien utile que le patient voie aussi dans l'historique les tentatives d'accès qui ont été refusées. On doute en effet qu'il soit vraiment nécessaire d'afficher toutes les recherches avec leurs critères dans l'historique parce qu'elles pourraient créer une certaine confusion, surtout lorsqu'elles n'ont rien trouvé ou apporté à leur auteur. Ces intervenants demandent donc des précisions. À propos du ch. 2.10.4.2.1, ils rappellent qu'il figure dans la liste des

[101] FR, NE, GE, VS, VD, JU

« saisies de l'historique consultables par le patient ». Ils demandent s'il est approprié qu'un patient puisse vérifier pour n'importe quel professionnel de la santé quand celui-ci s'est connecté et déconnecté, à moins qu'il soit question ici des (dé-)connexions du patient, à préciser le cas échéant. Le terme allemand de « Fokus » doit être repensé, l'historisation en elle-même est acceptable en la forme. Ils proposent de préciser : « authentification du patient dans le système […] ». *La Poste* objecte à propos du ch. 2.10.4.2.3 « que les entrées dans l'historique risquent d'être très nombreuses, notamment parce que les médecins font souvent des recherches non spécifiques. La limitation du nombre de résultats dans les profils IHE est facultative et il manque une disposition légale qui en ferait une exigence contraignante. Un déluge d'informations ne contribue pas à la sécurité des données. Le texte de ce chiffre doit être revu et rendu plus cohérent ». Pour *medshare*, le texte de ce chiffre est incompréhensible. En effet, il permet la recherche de documents, mais pas du dossier électronique du patient. Il s'agit de préciser où on veut en venir. En outre, *medshare* demande des précisions et une justification pour le ch. 2.10.4.2.5. *KSSG* fait remarquer que les saisies dans l'historique consultables par le patient sont générées par le profil IHE ATNA et à leur avis, le profil IHE ATNA ne prend pas en charge cette exigence. Ils demandent donc la suppression du ch. 2.10.4.2.7. L'historisation d'un nouveau MID peut être demandée dans Systemlogs, mais pas dans ATNA. Il en résulte que les saisies de son historique ne sont pas consultables par le patient. *SCH* explique à propos du ch. 2.10.4.2.7 que l'enregistrement d'un nouveau MID est un processus isolé dans Identity Provider, mais que l'Identity Provider n'est pas forcément une composante TI de la communauté ; il peut être sous-traité à des tiers. Le protocole SAML prescrit pour la communication des portails avec les Identity Providers ne prévoit aucun échange de données historisées entre l'Identity Provider et les portails. Par conséquent, les informations sur l'enregistrement de nouveaux MID ne sont en général pas disponibles dans la communauté et ne peuvent dès lors pas être historisées.

2.10.5 : Six cantons[102] font remarquer qu'une recherche n'a pas besoin d'être historisée si son résultat ne concerne pas qu'un seul patient. De plus, il est techniquement impossible de tracer une impression ou d'empêcher une capture d'écran. Il convient donc de supprimer les ch. 2.10.5.1 à 2.10.5.3. *Integic* réitère sa prise de position au sujet du ch. 2.10.4. *SUVA* rappelle que ses remarques concernant le ch. 2.10.4 restent valables tant qu'il s'agit de recherches effectuées par le patient dans ses propres données. Comme le déplore *privatim*, le texte n'indique pas si le patient trouvera dans l'historique les noms de ceux qui ont eu accès à ses données. C'est en tout cas une information importante qui devrait figurer dans l'historique. En règle générale, la personne qui accède aux données est connue du système, sinon l'historique doit faire état d'un accès par inconnu. La disposition doit être précisée, évent. complétée des éléments manquants. La *SSIM* et la *FMH* considèrent que l'historisation de la fonction de recherche et de ses paramètres va trop loin et qu'il faut la supprimer. Même les accès par create, read, update et delete sont historisés. *BFH* critique le fait que le ch. 2.10.5 évoque ce que l'historique « doit contenir au moins », mais fait suivre les exemples donnés aux ch. 2.10.5.1 à 2.10.5.3 de la mention « etc. ». Il demande que l'on dresse une liste exacte des attributs minimum à historiser. *La Poste* demande la suppression du ch. 2.10.5.3 au motif qu'il est impossible à appliquer.

2.10.6 : *Tessaris* propose de compléter comme suit le ch. 2.10.6 : « Les données historisées doivent être conservées pendant toute la durée de conservation prescrite des données dans le dossier électronique du patient jusqu'à leur suppression du dossier, mais au moins pendant 10 ans ». Par souci de clarté, d'après *privatim*, il faut prescrire la destruction des données historisées à l'expiration de ces dix ans. Une adaptation de l'énoncé doit être envisagée.

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

OFAC pose deux questions : comment reconstituer le dossier complet si on n'enregistre pas l'association patient-document dans les registres, et pourquoi interdire l'utilisation du numéro patient dans les systèmes primaires ? *Privatim* renvoie à ses déclarations dans les remarques générales sur l'ODEP. *ZH, K3* et *VZK* signalent que l'interdiction d'associer le NIP aux documents est inapplicable. L'attribution d'un cas interne se fait une seule fois ; par la suite, il faut pouvoir garantir que l'on pourra toujours utiliser

[102] FR, NE, GE, VS, VD, JU

cette même et unique attribution. *ZH* ajoute qu'une communauté n'est pas en mesure de garantir que le NIP n'est pas utilisé dans les systèmes primaires. Le terme allemand « persistent » (persistant) doit être remplacé par « dauerhaft » (durable), ce que souhaitent également *K3*, *VZK* et *SBC*. Mais de manière plus générale, ZH demande que le ch. 2.11.1 soit revu ou supprimé. *SUVA* fait valoir que les communautés ne peuvent pas assumer la responsabilité pour les établissements affiliés, de sorte que le ch. 2.11.1 doit être supprimé. *SBC* et *BINT* demandent également sa suppression. *BINT* déclare à ce sujet que les communautés doivent pouvoir garantir que les systèmes primaires CdC-NIP ne seront pas utilisés, mais c'est quelque chose que les communautés ne peuvent imposer. *BINT* ajoute que ce chiffre doit être précisé et pose les questions suivantes : que faut-il mettre dans les contrats ? Qu'est-ce qui doit être contrôlé et par qui ? Où se situent les responsabilités ? En outre, l'argumentation distincte en faveur du NIP du dossier électronique du patient conduit à devoir formuler une disposition inverse, à savoir : « Le NIP doit être maintenu de manière persistante dans les métadonnées de documents », une formulation que retiennent également *Integic* et *Bleuer. GE*, *FR*, *VS*, *VD* et *JU* font valoir que la communauté ne peut pas garantir le contenu des systèmes primaires. Si un médecin conserve un NIP associé à des documents médicaux, cela échappe à la connaissance de la communauté. Elle peut par contre émettre des recommandations. S'y ajoute que le terme de « lieu de stockage » n'est pas clair. Le MID peut se trouver dans le même lieu de stockage (data center) que des documents mais en être séparé physiquement. Le ch. 2.11.1 doit être clarifié, mais en vertu du principe d'économicité, il n'y a aucun avantage à générer un NIP sans pouvoir l'utiliser pour une identification univoque et sécurisée du patient.

Selon *IG eHealth*, il est crucial que les communautés soient tenues de garantir que le NIP de la CdC ne soit pas mémorisé de façon permanente dans les lieux de stockage ou les registres de documents, comme l'ordonne le texte de l'ordonnance. Mais l'obligation de maintenir de façon persistante le NIP dans les métadonnées de documents est clairement rejetée. Si le NIP est noté sur tous les documents, un changement voulu ou nécessaire de NIP entraînerait la perte de toutes les associations, ce qui veut dire qu'on ne pourrait plus attribuer de documents à un patient préalablement identifié de manière sûre. Cela pose des problèmes de protection des données. Le concept d'associer des documents par le MID et des clés locales est certes plus complexe, mais permet au moins de traiter les documents séparément Et c'est possible parce que le nom et la date de naissance du patient figurent sur chaque document. *HIN* objecte que le ch. 2.11.1, la deuxième partie surtout, est techniquement impossible. Après tout, chacun peut ajouter le numéro au système primaire après avoir copié une capture d'écran dans le presse-papiers. Enfin, il faut également tenir compte de la contradiction apparente avec la figure 2 de l'annexe 5, Adaptations nationales des profils d'intégration. *HIN* demande ici la mention explicite que la résolution de ces exigences passera surtout par des mesures organisationnelles.

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

Six cantons[103] estiment que le niveau de détail des objets de ce chapitre correspond davantage à des spécifications fonctionnelles (« comment ») qu'à des exigences qui ont leur place dans des ordonnances (« quoi »).

3.1. Conformité aux dispositions légales

ZAD, *K3*, *VZK* ainsi que *ZH* et *ZG* estiment que le portail d'accès doit répondre aux CTO. Il ne rime à rien de faire inscrire dans les CTO que le portail doit se conformer aux « exigences légales en la matière » quand il y est tenu de toute façon. D'ailleurs, aucun organisme de certification n'est en mesure de confirmer que le portail d'accès répond vraiment à toutes les exigences. *VAKA* qualifie de purement déclaratoire cette disposition du ch. 3.1.1 qui semble traduire un certain sentiment d'impuissance. Sept participants[104] demandent la suppression du ch. 3.1.1, dont *medshare* qui se satisferait qu'on se limite à une mention nominale de ces exigences. *privatim* saisit mal le but poursuivi par cette disposition. Pour qu'une telle réglementation ait un sens, il faudrait énumérer les principales exigences légales (liste non

[103] FR, NE, GE, VS, VD, JU
[104] ZG, ZH, ZAD, K3, VZK, VAKA, medshare

exhaustive) auxquelles doit répondre ce portail d'accès.

3.2 Présentation

Pour *K3*, *VZK*, *ZAD*, *ZH* et *ZG*, les dispositions du ch. 3,2 n'ont aucune utilité et doivent dès lors être supprimées. Huit participants[105] signalent qu'au ch. 3.2.1.1, le mot « Gesundheitsfachperson » (professionnel de la santé) a été oublié dans le texte allemand et doit être réinséré : « ob ein Dokument durch eine Gesundheitsfachperson oder durch […] ». *SQS* signale également que la phrase allemande est incomplète et doit être corrigée.

VAKA demande comment interpréter l'exigence faite au ch. 3.2.1.2 en regard du rôle des auxiliaires, et notamment si ceux-ci seront habilités à agir au nom du professionnel de la santé primaire/de leur supérieur hiérarchique. Des explications claires et nettes sont souhaitées sur ce point. *La Poste* demande à ce sujet comment caractériser les données que l'on publie soi-même et s'il suffit d'en indiquer l'auteur. On se demande dès lors comment interpréter la locution « le professionnel de la santé qui accède », soulignée dans la version allemande par le terme « selbst » (lui-même), quand des auxiliaires ou d'autres membres du même groupe peuvent être impliqués. Le texte doit spécifier concrètement que les auxiliaires doivent pouvoir agir au nom du médecin.

La *CDS* et neuf cantons[106] signalent à propos du ch. 3.2.1.3 que le droit d'exécution et les explications y relatives font intervenir les termes et concepts de « destruction », de « suppression » et d'« annulation » en relation avec les données du dossier électronique du patient. La question qui se pose est celle de la distinction de ces termes du point de vue technique. La *CDS* et huit cantons[107] suggèrent de traiter ces concepts dans le rapport explicatif et de bien les délimiter pour qu'ils puissent être appliqués de manière cohérente. Par ailleurs, le patient doit aussi être conscient des différences qu'il y a par exemple entre un document annulé et un document supprimé. *SBC* demande également ce que signifie ici « annulé » et souhaite que cette notion soit expliquée. *La Poste* demande que l'on détermine si les documents annulés des patients doivent être affichés et s'il ne suffirait pas d'indiquer leur statut dans l'historique.

À propos des ch. 3.2.1.3 et 3.2.1.4, *VGIch* déclare d'une part qu'il convient de garantir une version par document et d'autre part que l'on parle de documents « valides » ou « annulés ». Par ailleurs, il est dit que selon les métadonnées, un document peut présenter un état de disponibilité « autorisé » ou « refusé ». Il convient alors de bien expliquer et au besoin d'unifier cette terminologie. À propos du ch. 3.2.1.4, *VAKA* avertit que l'établissement de plusieurs versions ne fait en général qu'ajouter à la confusion du patient et demande si l'on ne devrait pas plutôt en restreindre la disponibilité. Il propose que seule la version actuelle soit mise à la disposition du patient. Dans la même veine, *La Poste* demande s'il ne serait pas plus simple de ne faire voir au patient que la toute dernière version, ce qu'elle propose de faire.

3.3 Accessibilité

VAKA applaudit à l'accessibilité dans son principe, mais elle est déjà très coûteuse à mettre en œuvre et s'il est question de la certifier de surcroît, on la renchérira d'autant plus. Les communautés et les communautés de référence prévoiraient dans tous les cas de ménager la libre accessibilité des portails d'accès. La disposition qui s'y rapporte dans les CTO doit être supprimée. *KSSG* relève que cet article demande qu'il n'y ait pas d'obstacle ni au portail d'accès, ni à l'intégration dans le système primaire. Cela signifie implicitement que tout le KIS doit être parfaitement accessible. *KSSG* demande donc que le ch. 3.3 en corrélation avec le portail d'accès pour les professionnels de la santé soit supprimé. *SBV* critique cette apparente fixation sur l'accessibilité par le Web et demande ce qu'il en est des applis et si l'on en tient compte dans l'établissement du document, car là aussi, il faudrait en définir les exigences

[105] CCM, BüAeV, GAeSO, KAeG SG, HIN, Medgate, privatim, pharmaSuisse
[106] BL, GL, LU, OW, UR, FR, NW, SZ, TG
[107] BL, GL, LU, OW, UR, FR, NW, SZ

d'accessibilité. *ZG* et *ZH* considèrent que ces dispositions ne sont pas nécessaires et en demandent également la suppression. *GE*, *VS*, *VD*, *JU* et *NE* font remarquer qu'il y a des professionnels de la santé âgés qui maîtrisent très bien l'informatique, alors que des médecins plus jeunes ont de fortes réticences à utiliser ces outils. Ils demandent en outre de quels handicaps il s'agit (troubles visuels ou handicaps psychiques ?) Ils demandent la suppression du ch. 3.3.1.1. Six cantons[108] ajoutent à propos du ch. 3.3.1.2 que cette décision fait référence à une norme susceptible d'évoluer qui n'a pas sa place sous cette forme dans un cadre législatif contraignant. Tandis que *GE*, *VS*, *VD*, *JU* et *NE* demandent la suppression de cette disposition, *FR* se prononce plutôt pour une simplification. *SQS* réitère pour le ch. 3.3.1.2 les observations déjà faites à propos du ch. 2.9.4 et demande qu'il soit complété d'une disposition réglant la preuve que les critères techniques ont été dûment contrôlés. *SBV* est d'avis que le degré de conformité AA selon le ch. 3.3.1.2 est insuffisant pour les personnes malvoyantes ou souffrant d'un handicap visuel. L'objectif doit être de satisfaire aux conditions de conformités selon la norme WCAG 2.0 et d'atteindre le niveau de conformité AAA.

3.4 Formats de fichiers : mise à disposition

Pour *K3*, *VZK*, *ZAD*, *ZH* et *ZG,* les dispositions du ch. 3.4 n'ont aucune utilité et doivent dès lors être supprimées. *SCH* déclare qu'a priori, on ne sait pas sous quels formats les patients ou les prestataires veulent transférer par le portail les données à enregistrer dans le dossier électronique du patient. On ne peut notamment pas exclure que les patients ou les prestataires veuillent utiliser des formats propriétaires pour lesquels il n'existe aucun programme capable de les convertir complètement. D'ailleurs, une conversion dans l'un des formats admis constitue un traitement de données au sens de la loi sur la protection des données. *Bleuer* observe à ce propos que c'est dans l'annexe 4 (et non 3) que sont définis les formats d'échange et qu'il convient d'apporter les correctifs nécessaires au ch. 3.4.1.1.

Les six cantons[109] considèrent qu'il est dangereux pour l'intégration des données que le portail transforme un fichier source. Les professionnels de la santé devraient répondre des formats adéquats. Ces cantons demandent en outre si cela signifie que le portail d'accès doit être en mesure de lire plusieurs formats. Ils demandent la suppression du ch. 3.4.1.2. *Bleuer* fait remarquer que les conversions peuvent introduire dans les données des erreurs susceptibles d'en modifier le sens, raison pour laquelle il importe de conserver une copie des formats originaux. Or, la conservation du format original rend problématique l'idée de restreindre les formats admis. Dans tous les cas, il convient d'admettre les formats courants, en particulier ZIP et ISO. *Bleuer* souhaite que le ch. 3.4.1.2 soit reformulé : « convertir les autres fichiers dans l'un des formats énumérés à l'annexe 4. Les fichiers à convertir doivent être également conservés dans leur format original ». *BINT* et *Integic* partagent cet avis et recommandent de conserver une copie des fichiers à convertir dans son format original. Cela implique aussi l'admission d'objets transmis au format Bitstream. *SUVA* observe qu'une conversion n'est pas compatible avec les critères de révision, raison pour laquelle elle se prononce pour le maintien des fichiers dans leur format d'origine. *La Poste* s'interroge sur la nécessité de convertir même des types de documents usuels et demande qui porte la responsabilité d'une perte éventuelle d'informations durant la conversion automatique et des erreurs de traitement qui en résulteraient. *K3* et *VZK* plaident pour l'inadmissibilité des conversions durant la procédure d'envoi. En effet, une conversion risque de falsifier le contenu et de porter atteinte à l'intégrité des données. Le résultat est hors du contrôle de l'auteur et le document pourrait acquérir une tout autre signification. La disposition doit être modifiée de manière à interdire toute conversion de fichier téléchargé en amont. Aucun document ne doit pouvoir être converti, cette prescription doit donc être supprimée. *Integic* pose deux autres questions en rapport avec le ch. 3.4.1.2 : quelles sont les voies prévues pour la conversion et comment pratiquer le téléchargement en amont de fichiers de Fitness Tracker ou d'autres applis ? Pour *HIN*, les fabricants de systèmes primaires devraient avoir tout intérêt à proposer des conversions appropriées. La voie à privilégier devrait être que le portail n'autorise que certains types de fichiers. *HIN* demande que le ch. 3.4.1.2 soit reformulé : « accepter les fichiers des formats définis à l'annexe 3. Les fichiers soumis dans d'autres formats doivent être convertis automatiquement ou refusés ». *Medshare* demande que l'on apporte la précision suivante à l'art.

[108] FR, NE, GE, VS, VD, JU
[109] FR, NE, GE, VS, VD, JU

3.4.1.2 : « […] dans un format autorisé en vertu du ch. 3.4.1.1 ».

3.5 Formats de fichiers : requête

Pour *K3*, *VZK*, *ZAD*, *ZH* et *ZG,* les dispositions du ch. 3.5 n'ont aucune utilité et doivent dès lors être supprimées. *La Poste* demande pourquoi les types de documents courants, tels que Word, ne sont pas pris en charge.

3.5.1 : Pour le ch. 3.5.1.2, *privatim* renvoie à ses déclarations dans les remarques générales sur l'ODEP. *SBC* signale que le « bulk download » ouvre une faille sécuritaire, raison pour laquelle le ch. 3.5.1.3 doit être supprimé. *Integic* demande si dans un « bulk download », l'utilisateur doit confirmer la vérification de chaque document ou si le regroupement se fait en une fois. Ce point doit être clarifié et complété. *BINT, Integic* et *IG eHealth* font remarquer à propos du ch. 3.5.1.5 que la lisibilité « par l'être humain » n'est pas un problème de téléchargement, mais de présentation. Ils se posent la question si l'on parle ici d'un rendu côté serveur. Dans l'affirmative, il convient de le dire clairement. *SUVA* souhaite quant à elle des précisions sur ce que l'on entend par « lisible par l'être humain ». *KSSG* considère que l'on ne peut espérer que le portail d'accès pourra gérer n'importe quel type de données structurées, mais qu'il faut partir du principe qu'il ne travaillera qu'avec les formats d'échange mentionnés à l'annexe 4 de l'ODEP-DFI. Il convient donc de préciser au ch. 3.5.1.5 qu'il vaut uniquement pour les formats d'échange mentionnés à l'annexe 4 de l'ODEP-DFI. Six cantons[110] demandent que le ch. 3.5.1.1 soit supprimé et que les ch. 3.5.1.2, 3.5.1.3 et 3.5.1.5 soient reformulés comme suit : « 3.5.1.2 permettre d'enregistrer des fichiers présents dans le système primaire ("upload") ; 3.5.1.3 prévoir la publication, non seulement un par un, mais aussi en masse ("bulk upload") des documents sélectionnés ; 3.5.1.5 […] données structurées brutes ou d'exporter la forme affichée de ces données ». *OFAC* fait remarquer à propos du « bulk download » au ch. 3.5.1.3 qu'un lot important de données concernant le patient échapperait ainsi au contrôle de la communauté. De plus, cette disposition est en contradiction totale avec le concept du « Patient Empowerment » (responsabilisation du patient).

3.5.2 : *medshare* signale une faute de frappe dans la version allemande (il manque le t dans « erlaubte »). *K3* et *VZK* critiquent la formulation qu'ils jugent imprécise. *SQS* demande à ce propos que l'on précise qui est responsable de définir les limites supérieures admises. *Integic*, *BINT* et *IG eHealth* sont d'avis que le principe d'une limite absolue est inadmissible. Il faut pouvoir reconnaître et consulter en toute simplicité d'autres documents disponibles. Pour *La Poste*, l'argumentation des « rate limits » est indéfendable. Si le patient a décidé de donner le droit d'accès à son dossier électronique au professionnel de la santé qui le demande, il semble inapproprié d'y mettre arbitrairement un verrou. D'après *Bleuer*, il y a un risque que les documents soient lus incomplètement par le système. Il demande donc la suppression du ch. 3.5.2. *SUVA* se prononce également pour la suppression de cette disposition et fait remarquer qu'elle se traduirait par la production de données incomplètes sur le patient. Pour les données que le patient a ajoutées lui-même, cela pourrait conduire à une intrusion dans sa sphère privée vu que le patient n'a pas la faculté de transférer les données souhaitées. *HIN* considère qu'il faut pouvoir habiliter et obliger les communautés à définir les « rate limits ». Il convient donc de compléter le ch. 3.5.2 comme suit : « […] renforcée. Les communautés déterminent les « rate limits ».

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

ISSS demande l'ajout d'un ch. 4.25 qui garantisse que les données du patient ne demeureront pas éternellement dans les sauvegardes de sécurité une fois détruites. Il demande d'ajouter le texte suivant : « 4.25 Sauvegarde des données (back-up) : Sauf dispositions légales ou réglementaires contraires, les sauvegardes de données sont détruites après deux ans au plus tard. Cette durée peut être prolongée à trois ans au plus si les nécessités d'exploitation le justifient ». *SQS* fait remarquer que tout le texte du ch. 4 contient l'essentiel des normes ISO/IEC 27001:2013 et des contrôles de l'annexe A. Il serait plus judicieux de les remplacer par des renvois aux normes ISO/IEC 27001:2013, annexe A comprise, et de ne définir que les ajouts spécifiques à l'ODEP, par exemple l'annonce à l'OFSP d'incidents affectant la

[110] FR, NE, GE, VS, VD, JU

sécurité. À cela s'ajoute que l'annexe utilise une terminologie qui ne correspond pas aux normes ISO/IEC 27001:2013. Concrètement, SQS propose la séparation des éléments respectifs de la norme ISO/IEC 27001:2013 et des contrôles de l'annexe A, ainsi que l'intégration de la terminologie ISO/IEC 27001:2013. Pour la réglementation relative à la protection des données, la *FMH* conseille de s'aligner sur les normes et les bonnes pratiques existantes ; pas besoin d'édicter de nouvelles règles. La FMH rejoint la SSIM dans sa demande de remanier tout le ch. 4. *Tessaris* postule qu'une communauté disposant de ressources humaines et matérielles restreintes, comme l'est un cabinet ou un petit centre médical communautaire, ne peut gérer seule les lourdes exigences organisationnelles et techniques qui découlent du ch. 4 et devra faire appel à des tiers (entreprises sous-traitantes). En fournissant leurs services aux communautés, de telles entreprises sous-traitantes doivent toujours satisfaire aussi aux exigences de l'art. 11 ODEP et du ch. 4, sous peine de créer une faille dans le dispositif servant à garantir la protection et la sécurité des données.

4.1. Exigences envers les tiers

Chez *privatim*, on salue cette réglementation, jugée adéquate du point de vue de la protection des données. Bien qu'elle découle déjà des législations fédérale et cantonales sur la protection des données, il paraît opportun de l'inclure aussi dans les CTO par souci de clarté et d'intégralité.

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

4.2.1 : *HIN* se réjouit de la mention explicite de la norme ISO 27001. *SQS* rappelle que la norme ISO/IEC 27001:2013 ne décrit pas un système de gestion de protection et de sécurité des données, mais bien un ISMS. Le système de gestion de protection et de sécurité des données à exploiter doit être basé sur ou conforme à la norme ISO/IEC 27001. En revanche, les directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (Directives sur la certification de l'organisation et de la procédure), édictées par le PFPDT le 14 juin 2014 et appliquées lors d'une certification selon l'art. 11 LPD, sont parfaitement appropriées pour la description du système de gestion de protection et de sécurité des données. *SQS* propose les deux variantes suivantes pour l'énoncé du ch. 4.2.1 : « Les communautés doivent exploiter un système de gestion de protection et de sécurité des données tel que décrit dans la norme ISO/IEC 27001:2013, qui : […] » et « Les communautés doivent exploiter un système de gestion de protection et de sécurité des données, tel que décrit dans les directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (directives sur la certification d'organisation et procédure), édictées par le PFPDT le 14 juin 2014, qui : […] ». *ZH, ZG, ZAD, K3* et *VZK* ne trouvent pas judicieuses les dispositions du ch. 4.2.1 et en souhaitent la suppression. *OFAC* fait savoir que les systèmes de gestion de la protection des données (SGPD) et les systèmes de gestion de la sécurité de l'information (SGSI) fonctionnent parfaitement de manière conjointe, mais jamais confondue. Les deux systèmes devraient être gérés de manière distincte. En outre, à l'instar de *SQS*, elle rappelle que la norme ISO 27001:2013 ne définit pas de système de gestion de la protection des données. Il conviendrait donc de reformuler cette disposition, car la phrase prête à confusion.

4.2.2/4.2.3 : *ISSS* écrit qu'il convient aussi, par le biais des ch. 4.2.2.3.1 – 4.2.2.3.3 et 4.2.2.3.5, de demander les composantes pour les disciplines spécifiques d'ICT, telle que sécurité contre les attaques, sécurité contre les pannes d'exploitation et back-up du système et des données, cela aux fins de l'Awareness et pour servir de base au Management Review et aux audits/certifications. Il propose les adjonctions suivantes pour les chiffres susmentionnés : ch. 4.2.2.3.1 : « hardware (inventaire des dispositifs de stockage des données, serveurs, systèmes de back-up, fonctions de sécurité) ; ch. 4.2.2.3.2 : logiciels (software) (inventaire de systèmes d'exploitation et d'application EPD, endpoint protection, back-up, monitoring, gestion des mises à jour et des patchs) ; ch. 4.2.2.3.3 : ensemble de données (description de la conservation des données, de l'organisation des données, de la sécurité des données, autorisations) ; ch. 4.2.2.3.5 : processus (du système de gestion de protection et de sécurité des données, en particulier aussi pour les scénarios de pannes, reprises, tests, audits, responsabilités). Concernant le ch. 4.2.2.3, *La Poste* demande si l'inventaire comprend l'ensemble des systèmes primaires connectés

ou s'il ne s'agit ici que des composants centraux. Elle demande donc que le champ d'application des CTO soit clairement défini. *SQS* déplore que les dispositions énoncées aux ch. 4.2.2 et 4.2.3 n'aient pas de congruence avec l'art. 11 ODEP. Il convient dès lors soit de compléter l'art. 11 ODEP, soit d'adapter les deux chiffres en question. À propos du ch. 4.2.2.3, *SQS* relève que l'inventaire dans la norme ISO/IEC 27001:2013 ne concerne pas que les équipements d'exploitation. Cette norme parle des actifs (assets) et valeurs de l'organisation. En font aussi partie, par exemple, les collaborateurs. En outre, l'organisation structurelle n'est pas analysée de manière suffisamment détaillée. *SQS* propose dès lors l'énoncé suivant : « Un inventaire actuel des valeurs suivantes de l'organisation ». En conséquence, il convient également d'adapter le ch. 4.2.3 : « […] apportés aux valeurs de l'organisation qui ont une incidence […] ».

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

Vingt participants[111] sont d'avis que l'on peut fort bien renoncer à instituer des responsables de la protection et de la sécurité des données. Quatorze participants[112] ajoutent que le gain en sécurité par de tels responsables n'apparaît pas clairement, sans parler du coût élevé de l'aménagement de tels postes. *ZAD*, la *CDS* et huit cantons[113] signalent que les dispositions des CTO divergent de la partie du rapport explicatif traitant de l'art. 11 ODEP, qui évoque une « indépendance technique et organisationnelle » du responsable de la protection des données. *AR* est d'avis que cette tâche devrait revenir au responsable désigné de la protection des données, pour autant qu'il dispose de capacités de travail suffisantes, et que l'on peut dès lors se dispenser de créer un poste indépendant. Six participants[114] demandent expressément la suppression du ch. 4.3.

En ce qui concerne le ch. 4.3.1.1, *SZ* est d'avis qu'il n'est pas judicieux d'exiger que les responsables de la protection des données puissent exercer leur fonction de manière indépendante. À l'instar de *K3*, *VZK*, *ZG* et *ZAD*, *SZ* veut savoir en outre ce que l'on entend au juste par là. De l'avis de *privatim*, il serait souhaitable que l'on ajoute au ch. 4.3.1 un point supplémentaire qui dispose que le responsable de la protection des données doit avoir toutes les connaissances requises pour assumer cette tâche. Par ailleurs, il faut préciser au ch. 4.3.1.2 que le terme de « ressources » fait référence aussi bien aux ressources temporelles que financières. *VGIch* qualifie de trop vague l'énoncé du ch. 4.3.1.2 et demande qu'il soit précisé à l'aide de critères bien définis. En outre, *medshare* souhaite lui apporter les précisions suivantes : « il dispose des ressources et des compétences décisionnelles nécessaires […] », et *BS* préfère la formulation suivante : « il dispose des compétences et des ressources nécessaires […] ».

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

KSSG attire l'attention sur le fait que la mise en place d'un SIEM prend beaucoup de temps et qu'un délai de transition de trois ans ne sera guère suffisant pour l'implémenter. Il convient dès lors soit d'assouplir les dispositions du ch. 4.4, soit de prolonger les délais prévus pour sa mise en œuvre. *VGIch* considère que le SIEM doit se restreindre aux parties techniques et organisationnelles de l'infrastructure communautaire qui servent à la mise à disposition du dossier électronique du patient, mais ne doit s'appliquer ni aux extensions (logiquement séparées) requises pour la mise en place de la communication dirigée, ni à l'infrastructure et à l'organisation des institutions affiliées. Six cantons[115] déclarent qu'à leur avis, un SIEM ne doit pas pouvoir s'appliquer aux systèmes primaires des professionnels de la santé et demandent par conséquent d'introduire le complément suivant au ch. 4.4.1.1 : « […] de la communauté à l'exclusion des systèmes primaires, qui détecte […] ». *ISSS* est d'avis que les personnes chargées de la mise en œuvre pratique de ces dispositions doivent être dûment formées, suivre un cours ou obtenir une attestation. Il convient donc de compléter le ch. 4.4.1.3 comme suit : « […] technique, conformément au ch. 4.5. En particulier, il convient d'apporter aux personnes chargées de ces

[111] NW, TI, FR, ZG, K3, VZK, SSIM, FMH, BL, CDS, GL, LU, OW, UR, SZ, ZH, ZAD, ZG, K3, VZK
[112] NW, TI, FR, ZG, K3, VZK, BL, CDS, LU, OW, UR, SZ, ZH, ZAD
[113] BL, GL, LU, OW, UR, SZ, ZH, TG
[114] ZH, K3, VZK, ZG, TI, NW
[115] FR, NE, GE, VS, VD, JU

tâches un soutien adéquat et récurrent au sein de la communauté par des mesures de sensibilisation, des formations ou des échanges d'expériences avec d'autres responsables. »

La Poste critique le flou des dispositions du ch. 4.4.2.2. Juger de ce qui est inhabituel, définir comment le reconnaître est une tâche difficile, tant pour la communauté que pour l'auditeur. De plus, on ne sait pas ce qu'est une « mutation critique » au sens du ch. 4.4.2.3. Le texte de ces deux chiffres doit être reformulé en termes concrets.

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

VAKA, *K3* et *VZK* demandent ce qui distingue une procédure « formelle » d'une procédure normale. *medshare* est d'avis que le texte du ch. 4.5.1.1 doit être complété d'un renvoi au document de l'ODEP, car aucun n'y figure. La *FMH* et la *SSIM* demandent que l'on précise l'énoncé du ch. 4.5.1.1. Il ne rime à rien de tout signaler. *La Poste* aurait aimé trouver ici une description claire de l'étendue des problèmes à corriger. *ISSS* demande que le ch. 4.5.1.1 soit reformulé comme suit pour être conforme au Règlement général sur la protection des données de l'UE (RGPD-UE) : « avoir défini une procédure formelle selon le ch. 4.13 pour l'annonce d'événements pertinents pour la protection et la sécurité des données aux patients concernés ». *SQS* fait valoir que ce n'est ni la fonction ni la tâche d'un organisme de certification que de recevoir des annonces d'événements relatifs à la protection et à la sécurité de données ou d'en contrôler la suppression de la cause. L'organisme de certification en tant que site d'escalade doit être biffé du ch. 4.5.1.1. *Medshare* souhaite que l'on précise comme suit l'énoncé du ch. 4.5.2.2.1 : « […] pour isoler la communauté, par blocage de son point d'accès et de son portail d'accès, du traitement des données […] ».

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

ZAD ainsi que *NW*, *TI* et *ZH* trouvent que la réglementation au ch. 4.6 est trop détaillée. Il faut la supprimer et il serait plus adéquat de le remplacer par des principes généraux à inscrire dans l'ODEP. *La Poste* réitère pour le ch. 4.6.1.1 la demande qu'elle a faite au sujet du ch. 4.5.1.1.

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

NW, *ZH* et *ZAD* réitèrent leur prise de position faite à propos du ch. 4.6, mais contrairement à son commentaire relatif au ch. 4.6, ZAD propose de simplifier le ch. 4.6 au lieu de le supprimer. À l'instar de *NW* et de *ZH*, *K3* et *VZK* demandent la suppression du ch. 4.7. Ils précisent que la réglementation est juste dans son principe, mais beaucoup trop détaillée. *ISSS* demande d'ajouter des chiffres supplémentaires à l'énoncé suivant : « 4.7.4 Pour soutenir la gestion des failles de sécurité, les communautés doivent effectuer des analyses automatisées de vulnérabilité au moins tous les trois mois » et « 4.7.5 Pour soutenir la gestion des failles de sécurité, les communautés doivent faire effectuer un test de pénétration du système par un prestataire indépendant au moins une fois par année ». *VAKA* approuve le principe des mesures proposées au ch. 4.7, mais considère que guetter en permanence toutes les failles de sécurité de l'ensemble des logiciels constitue une charge relativement lourde. De plus, il s'agit souvent de logiciels « closed source », de sorte qu'en règle générale, une faille de sécurité restera de toute manière inconnue.

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

K3, *VZK*, *ZAD* ainsi que *NW* et *ZH* trouvent cette réglementation trop détaillée pour une utilité pratique somme toute faible, et souhaitent une simplification du ch. 4.8.

4.8.1 : Six cantons[116] font remarquer que cela fait partie de l'obligation de diligence à laquelle les professionnels de la santé sont tenus, comme d'ores et déjà dans la pratique actuelle. *Bleuer* fait valoir que la pertinence pour le traitement du patient ne peut pas être définie a priori. *VAKA* considère que la

[116] FR, NE, GE, VS, VD, JU

décision visée au ch. 4.8.1 doit être prise par les professionnels de la santé sur la base d'une évaluation de cas en cas. *KSSG* demande comment répondre à ces exigences si aucune directive ne dit quelles sont les données pertinentes pour le traitement. Dans le même ordre d'idées, *BINT* et *Integic* demandent comment comprendre la notion de « pertinence pour le traitement » dans ce contexte et suggèrent que la manière dont elle est perçue doit varier considérablement. La *SSIM* trouve elle aussi que la notion de « pertinent pour le traitement » est trop vague et demande une définition plus concrète, comme elle l'avait fait dans son avis sur le projet de loi de 2011. *VGIch* critique également le fait que l'on ignore quelles données et quels documents il faut considérer comme pertinents. Pas moins de neuf participants[117] demandent la suppression pure et simple du ch. 4.8.1, tandis qu'*Integic* et *KSSG* accepteraient qu'on lui apporte les précisions nécessaires. *VGIch* propose que l'OFSP fournisse un modèle non contraignant de « Best Practice » pour la mise à disposition de fichiers par les hôpitaux. *OFAC* demande comment les communautés pourraient garantir quoi que ce soit concernant les institutions affiliées. Qui assurerait le contrôle dans le temps, comment et de quel droit ? Les tâches des communautés sont décrites de manière exhaustive à l'art. 10 LDEP. Les institutions affiliées sont, indépendamment de leur affiliation, soumises au droit suisse de la protection des données. Il faut, de plus, noter que le droit auquel les institutions sont soumises dépend de leur nature juridique.

4.8.2 – 4.8.4 : *La Poste* réitère pour le ch. 4.8.2. sa prise de position à propos du ch. 4.5. Six cantons[118] signalent que dans la version française, le terme « sensible » utilisé au ch. 4.8.2 n'a pas le même sens qu'aux art. 1 et 2 ODEP ou dans la LDEP et qu'il faut dès lors clarifier ce terme. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* observent que là encore, le texte allemand parle de « schützenswerte Daten » (traduit en français par « données sensibles ») sans que cette notion ait été définie. Il en résulte un flou juridique. Ces intervenants suggèrent de fournir ici une définition légale. *Integic* voit dans le ch. 4.8.3.8.1 l'obligation pour chaque acteur IHE d'utiliser son propre certificat client et demande dès lors que cette règle soit précisée. *KSSG* relève à ce sujet que la mémorisation du certificat client TLS dans l'inventaire est un processus incertain. Les certificats clients doivent être conservés dans un endroit sécurisé. *KSSG* souhaite donc que ce chiffre soit supprimé ou reformulé. L'inventaire ne doit contenir que le nom du certificat client, mais non le certificat lui-même. Six cantons[119] estiment que la communauté ne peut tenir un inventaire de milliers de systèmes primaires utilisés, pas plus qu'elle n'est en mesure de fournir des indications sur le certificat TLS installé sur ces systèmes. Ils demandent la suppression du ch. 4.8.3.8. *SQS* n'arrive pas à comprendre le sens du ch. 4.8.4.3. On ignore à la lecture de quelle confirmation il s'agit, il faut que cela soit précisé dans le texte ou alors qu'il soit reformulé. *ahdis* demande que le ch. 4.8.3.8.1 utilise les désignations plus précises de « Serial ID, HASH du certificat client TLS » en lieu et place de « certificat client TLS » afin de limiter le risque d'abus. *OFAC* observe qu'il manque dans la liste les interfaces entre la communauté et le reste du monde. On n'y trouve aucune disposition exigeant que le transport et les échanges entre le système primaire et la communauté se fassent selon les protocoles IHE. De manière générale, toutes les interconnexions entre la communauté et des tiers doivent figurer à l'inventaire en tant qu'interfaces.

4.9 Prescriptions relatives à la protection et à la sécurité des données imposées aux institutions de santé affiliées ainsi qu'à leurs professionnels de la santé et applicables aux terminaux (let. e).

HIN salue le fait que l'on pose des exigences en matière d'appareils terminaux. La *SSIM* et la *FMH* critiquent le fait que les exigences posées aux institutions de santé affiliées et à leurs professionnels de la santé interfèrent avec la souveraineté des systèmes primaires. Elles demandent le remaniement de toute la section et en particulier la suppression des ch. 4.9.1.2.3, 4.9.2 et 4.9.3. *VGIch* considère que le SIEM doit se restreindre aux parties techniques et organisationnelles de l'infrastructure communautaire qui servent à la mise à disposition du dossier électronique du patient, mais ne doit s'appliquer ni aux extensions (logiquement séparées) requises pour la mise en place de la communication dirigée, ni à l'infrastructure et à l'organisation des institutions affiliées. Il convient donc de délimiter son champ d'action en lui attribuant un propre chiffre. *OFAC* déplore que les communautés ne puissent offrir aucune

[117] VAKA, BINT, FR, NE, GE, VS, VD, JU, Bleuer
[118] FR, NE, GE, VS, VD, JU
[119] FR, NE, GE, VS, VD, JU

garantie concernant les institutions affiliées dont elles ne sont ni propriétaires ni responsables. Le rôle de la communauté vis-à-vis des institutions affiliées se limite à décrire les exigences techniques et organisationnelles de ses interfaces.

4.9.2/4.9.3 : Sécurité des terminaux utilisés par les professionnels de la santé : *BINT* observe que le ch. 4.9.2 a pour effet de transférer la responsabilité aux affiliés, ce qui est parfaitement approprié dans ce contexte. Il ne peut cependant être imposé ni cautionné, d'autant moins que son champ d'action enfreint la limite de compétences de la LDEP ; il faut donc biffer ce chiffre. *ISSS* préférerait un texte incluant un catalogue d'exemples, et propose donc la formulation suivante : « […] à garantir une configuration sûre (y compris par une limitation à des usages spécifiques, p. ex. Internet, enregistrements vidéo ou audio, transferts de données, synchronisations) des terminaux utilisés par les professionnels de la santé pour accéder […] ». Au sujet des ch. 4.9.2 et 4.9.3, *La Poste* observe que les communautés ne peuvent ni contrôler ni valider individuellement les ordinateurs connectés. Les communautés ne peuvent pas répondre à cette exigence, impossible à appliquer en l'état, mais elles doivent définir dans les conditions générales les exigences de sécurité à observer par les utilisateurs. Dans son commentaire sur le ch. 4.9.3, *Integic* souhaite qu'il soit complété d'une disposition sur les « utilisateurs individuels et l'interdiction définitive/refus d'accès à des utilisateurs collectifs ou groupes d'utilisateurs ». *VGIch* estime que le ch. 4.9.3 constitue une ingérence dans la compétence d'exploitation des hôpitaux, raison pour laquelle il convient de le supprimer. Une convention entre la communauté et l'institution est amplement suffisante. *K3*, *VZK*, *ZAD* et *ZH* considèrent qu'il s'agit là d'évidences dont on tient déjà compte dans la pratique. Il convient donc de supprimer le ch. 4.9.3 ou, si l'on opte pour son maintien, de l'alléger en introduisant une règle générale abstraite simplifiée dans l'ODEP. *VAKA, K3* et *VZK* font remarquer qu'un pare-feu n'est pas un élément du terminal du professionnel de la santé et proposent de biffer le texte qui s'y rapporte ou d'adapter le titre de l'alinéa. *OFAC* observe que la relation entre la communauté et les institutions affiliées est de nature purement contractuelle. Si l'OFSP décide de contraindre les professionnels de la santé à des règles ou à des normes strictes en matière de sécurité de l'information ou de protection des données, cela ne devra pas se faire au travers du dossier électronique du patient. Il n'y a aucune base légale pour cela dans la LDEP.

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

ZAD, *NW* et *ZH* réitèrent pour le ch. 4.10 leur prise de position relative au ch. 4.6, à laquelle se joignent aussi *K3* et *VZK*.

4.10.1 : *ÄTG* et *HÄ CH* font remarquer que la protection des données et une bonne gestion des données sensibles constituent d'ores et déjà une tâche importante pour les professionnels de la santé. Pour que les communautés puissent atteindre le but visé, il faut toutefois veiller à ce que les exigences soient raisonnables et mesurées en évitant toute disproportion dans le temps et les moyens financiers engagés (utilité marginale). *La Poste* demande s'il est question ici de l'exploitation des systèmes énoncés par la LDEP (administration, engineering, helpdesk, etc.) et souhaite que l'on donne des exemples concrets.

4.10.2 : Six cantons[120] observent à propos du ch. 4.10.2.1, que la communauté ne peut pas garantir que les personnes assument leur responsabilité ou qu'elles sont compétentes. Ce n'est pas à la communauté d'assumer la responsabilité d'évaluer les connaissances qu'auraient ou n'auraient pas les utilisateurs et il convient donc de biffer ce chiffre. La *CDS* et six cantons[121] objectent que la disposition du ch. 4.10.2.3 est irréalisable. Une obligation contractuelle de personnes ayant accès aux données du dossier électronique du patient n'est pas justiciable au même titre que le secret médical. Sept autres participants[122] font la même observation. Ils ajoutent que l'obligation de secret médical est régie par le droit fédéral, complété le cas échéant par le droit cantonal. Ni les communautés ni les communautés de référence n'auraient les compétences de réglementation nécessaires. *K3, VZK* et *ZAD* pensent qu'il convient d'élucider dans quelle mesure les collaborateurs de communautés et de communautés de

[120] FR, NE, GE, VS, VD, JU
[121] BL, GL, LU, OW, UR, SZ
[122] NW, ZG, ZH, TI, ZAD, K3, VZK

référence doivent être considérés comme auxiliaires au sens des dispositions de l'art. 321 du Code pénal suisse (CP). *ZH* considère à ce sujet que les collaborateurs de communautés et de communautés de référence ne sont pas assimilés à des auxiliaires au sens de l'art. 321 CP, et que sans adaptation du CP, la responsabilité pénale du médecin n'est pas engagée si un secret médical a été divulgué avec le consentement – juridiquement valable – du patient au sens de l'art. 321, al. 2, CP. *SQS* demande ce qu'il faut entendre par obligation analogue au secret médical. Le secret médical fait partie des obligations de garder le secret régies par l'art. 321 CP. L'énumération des professions visées par l'art. 321 CP est exhaustive et exclut notamment les auxiliaires des médecins. Les prestataires TI en particulier ne tombent pas dans la catégorie des personnes astreintes au secret médical. Il convient dès lors de préciser le ch. 4.10.2.3 et de le reformuler comme suit : « les personnes […] du patient doivent être soumises au secret médical en vertu de l'art. 321 CP ou être astreintes au secret par une disposition contractuelle. L'obligation contractuelle de garder le secret concerne toutes les données du dossier électronique du patient dont les personnes ont connaissance dans l'exercice de leur profession, et doit s'appliquer sans limite de temps au-delà du cadre de l'activité professionnelle et après la fin du mandat ». À propos du ch. 4.10.2.3, *Tessaris* considère que les personnes qui ne sont pas soumises ou contractuellement tenues au secret médical dont la violation est punie par le Code pénal (p. ex. les employés d'organisations visées au ch. 4.1.1) doivent être astreintes à une stricte confidentialité par des mesures appropriées (signature d'une convention de confidentialité). Il propose donc l'énoncé suivant pour ce chiffre : « Les personnes qui ont accès à des données figurant dans le dossier électronique du patient doivent s'engager par des mesures appropriées, et notamment par la signature d'une convention de confidentialité, à garder le secret sur les informations dont elles ont connaissance au sujet des patients dans l'exercice de leur activité au service de la communauté ». *ISSS* propose de préciser comme suit le ch. 4.10.2.3 : « […] analogue au secret médical (p. ex. une obligation contractuelle de garder le secret) ». *AR* veut savoir à propos du ch. 4.10.2.1 quelles sont les personnes visées ; qui est réputé être « compétent » et comment ces personnes sont censées se montrer « attentives » dans ce contexte. Pas moins de quatorze participants[123] se prononcent pour la suppression du ch. 4.10.2.3. *Tessaris* écrit au sujet du ch. 4.10.2.4, que les exigences posées au management du personnel devraient se concentrer sur les aspects de la protection et de la sécurité des données, et propose la formulation suivante : « les processus visant à assurer la protection et la sécurité des données […] ».

4.10.3 : La *SSIM* considère le ch. 4.10.3 et les points qu'il contient comme disproportionnés et demande leur suppression. *ZH* réitère ici la position qu'il a prise au sujet des ch. 4.6 et 4.10. *La Poste* demande que le ch. 4.10.3 donne les références exactes à d'autres lois pour que les usagers puissent prendre connaissance de ses implications légales concrètes. Pour *IG eHealth* se pose la question d'une violation du principe d'égalité de traitement si l'on exige un niveau de protection si élevé à l'échelon fédéral tout en tolérant, pour les mêmes données médicales, un niveau de protection beaucoup plus bas à l'échelon cantonal. Ils recommandent d'harmoniser ce point avec les exigences cantonales. Pour *BS*, il convient de préciser aux ch. 4.10.3.1 et 4.10.3.2 que la « liste des personnes-clés » ne se réfère pas aux professionnels de la santé. Il faut être bien clair qu'il ne s'agit pas de soumettre les professionnels de la santé à un contrôle de sécurité relatif aux personnes tel que prévu par la loi sur l'armée. En revanche, ce dernier contrôle devrait pouvoir être effectué sans trop d'efforts auprès des communautés de référence. D'où la proposition d'ajouter le texte suivant au ch. 4.10.3.1 : « gérer une liste […] de toutes les personnes qui ne sont pas des professionnels de la santé au sens de l'art. 2, let. b, LDEP, et qui ont accès […] ». Chez *privatim*, on salue cette disposition du ch. 4.10.3.1 que l'on juge irréprochable du point de vue de la protection des données, mais on saisit mal quelles personnes cette liste doit inclure effectivement. Il n'est guère concevable que tous les professionnels de la santé ayant accès au dossier électronique du patient puissent être des personnes-clés. Des précisions sont nécessaires. Six cantons[124] souhaitent que la disposition du ch. 4.10.3.1 soit clarifiée par des exemples concrets.

[123] K3, VZK, ZAD, CDS, BL, GL, LU, OW, UR, SZ, NW, ZG, ZH, TI
[124] FR, NE, GE, VS, VD, JU

Quinze participants[125] ne voient pas pourquoi une communauté ou une communauté de référence devrait se soumettre à un contrôle de sécurité (CSP) en vertu de la loi sur l'armée. Six participants[126] ajoutent que même sur le fond, demander un tel contrôle de sécurité est une mesure inappropriée. Pour ce qui est du ch. 4.10.3.2, *Insel*, *Integic* et *KSSG* considèrent qu'en comparaison transversale avec d'autres institutions, cette exigence est complètement disproportionnée, tandis que *STSAG* parle d'« efforts inadéquats ». *Bleuer* écrit que cette exigence constitue une ingérence disproportionnée dans la sphère privée des salariés et que l'on peut douter du bien-fondé de la base légale, respectivement de la légitimité d'une telle exigence, avis que partage entièrement *Integic*. *SQS* souligne la nécessité d'une base légale pour le CSP et précise que les résultats d'un tel contrôle ne peuvent être révélés qu'aux destinataires désignés spécifiquement par les lois spéciales en vigueur. Il considère que la base légale fait défaut pour cette disposition et qu'en raison du principe de légalité, il ne suffit pas d'inscrire l'exigence de ce contrôle dans une annexe d'ordonnance départementale. *SUVA* fait remarquer qu'un tel contrôle n'est prévu ni par la loi sur l'armée ni par l'ordonnance sur le CSP (OCSP). Elle s'interroge sur le bien-fondé légal d'un contrôle aussi sévère et observe qu'il ne respecte plus le principe de la proportionnalité. Une telle disposition n'est pas compatible avec le droit actuel et n'est au demeurant plus nécessaire au vu des possibilités que donne aujourd'hui la législation sur la protection des données. *SCH*, qui fait également valoir l'absence de proportionnalité, est d'avis qu'il appartient aux communautés d'intérêts de recommander des contrôles d'intégrité pour des personnes ayant accès à des données de patients. *Tessaris* relève que dans l'esprit de la conception défendue ici, le CSP prévu par la loi sur l'armée et par la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) n'est pas applicable aux personnes-clés visées par les dispositions de la LDEP. Les CSP effectués en vertu de ces lois impliquent une consultation du casier judiciaire et l'obtention de renseignements sur la vie privée de la personne faisant l'objet de ce contrôle, ce qui constitue une atteinte à ses droits fondamentaux qui doit être justifiée par une loi formelle. *KSSG* considère qu'une mise en œuvre de ces exigences dans le délai imparti de trois ans est un objectif irréaliste. *BINT* objecte que l'astreinte au CSP empêche d'avoir recours à du personnel étranger. *VGIch* considère que l'exigence visée au ch. 4.10.3.2 est disproportionnée et contraire au principe d'égalité de traitement entre professionnels de la santé. Elle viole en outre les principes du droit quant à la forme et au fond.

Pas moins de 26 participants[127] demandent la suppression du ch. 4.10.3.2. Six cantons[128] considèrent que l'OCSP est inadaptée à ces circonstances. *SCH* pourrait approuver que ce chiffre soit non pas supprimé, mais reformulé comme suit : « effectuer dans chaque cas un contrôle d'intégrité approprié », tandis que Tessaris se demande si ces personnes doivent vraiment se soumettre à un CSP en vertu de la législation fédérale ou de celle du canton compétent et demandent le cas échéant à passer un tel CSP. *VAKA* souhaite une adaptation générale de la formulation du ch. 4.10.3.2. *BS* propose de modifier ce chiffre comme suit : « […] CSP par analogie à la loi sur l'armée ». *HIN* signale qu'il manque un verbe dans le texte allemand du ch. 4.10.3.2 (probablement « dafür sorgen, dass ») et qu'il faut le compléter. *ISSS* demande si le CSP doit être passé une seule fois au début ou doit être répété périodiquement et propose le complément suivant : « effectuer pour chaque personne avant son entrée en service et, dans les cas justifiés, pendant son activité, un contrôle de sécurité […] ». *Tessaris* relève au sujet du ch. 4.10.3.3 que les communautés n'ont pas la compétence de prévoir des « procédures définies et officielles », raison pour laquelle ce passage au début du texte doit être supprimé.

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

K3, *VZK*, *ZAD* ainsi que *ZH* et *NW* demandent que l'on vérifie si les dispositions énoncées au ch. 4.11 sont nécessaires. Dans l'affirmative, il faudrait examiner la possibilité de les remplacer par des normes générales et abstraites dans la LDEP. *OFAC* demande pourquoi l'on ne retrouve aucune référence aux exigences de l'art. 10a LPD. *La Poste* relève à propos du ch. 4.11.1 que la liste de tiers est une bonne idée, mais demande quelle est l'utilité de faire viser cette liste par le responsable de la protection des

[125] CDS, BL, GL, LU, OW, UR, AR, SZ, NW, TG, ZG, ZH, ZAD, K3, VZK
[126] K3, VZK, ZAD, ZH, NW, ZG
[127] BINT, Bleuer, Insel, Integic, KSSG, CDS, BL, GL, LU, OW, UR, AR, SZ, NW, TG, ZG, ZH, ZAD, K3, VZK, SQS, STSAG, SUVA, SCH, Tessaris, VGIch
[128] FR, NE, GE, VS, VD, JU

données. La formulation semble assez vague. La notion de « composants d'infrastructures informatiques » doit être définie un peu plus étroitement, sinon Intel, Samsung, Microsoft, etc. devraient également figurer sur cette liste. Elle demande que l'exigence du visa ainsi que le terme « le cas échéant » soient supprimés. *SQS* fait remarquer que dans la version allemande du ch. 4.11.2, il manque un mot dans la première phrase : « Gemeinschaften müssen sicherstellen, dass kein Datenzugriff […] ». *Tessaris* fait la même remarque et demande que l'on corrige cette petite faute de syntaxe. Par ailleurs, on se demande ce que désigne le mot « intermédiaires » par opposition au terme de « tiers ». *La Poste* demande où est la différence entre les deux chiffres 4.11.3 et 4.11.4. Selon *privatim*, les contrats visés au ch. 4.11.5 doivent impérativement inclure les clauses suivantes : une règle en vertu de laquelle le tiers doit garantir que seuls ont accès à ces données ceux de ses collaborateurs qui en ont effectivement besoin pour accomplir leurs tâches ; la signature par les collaborateurs d'une déclaration de confidentialité les obligeant à garder le secret jusqu'au-delà de la fin des rapports de travail ; l'interdiction de transmettre des données à des tiers sans le consentement de la communauté. La règle du ch. 4.11.5.4 doit aussi préciser qui a le droit d'effectuer les contrôles périodiques requis : les exploitants de la communauté ou le préposé à la protection des données de cette même communauté ? Il faut également inclure dans la réglementation que la communauté est habilitée à confier ces contrôles à des tiers qualifiés. En outre, *privatim* demande une reformulation des ch. 4.11.5.5 à 4.11.5.7. Les rapports de sous-traitance doivent être évités dans la mesure du possible. En effet, plus il y a d'acteurs, plus il est difficile de garder une vue d'ensemble et d'effectuer les contrôles. La disposition doit être reformulée pour préciser que les contrats de sous-traitance ne sont admis qu'à titre exceptionnel et seulement avec le consentement de la communauté (de cas en cas – pas de consentement général).

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

K3, *VZK*, *ZAD* et *ZH* réitèrent ici leur prise de position relative au ch. 4.11. *SQS* répète ses remarques concernant l'art. 11, al. 2 ODEP et le ch. 4.12.1 et propose de retirer à l'organisme de certification son rôle de lieu de déclaration des incidents classés comme affectant la sécurité.

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

K3, *VZK*, *ZAD* et *ZH* réitèrent ici leurs prises de position relatives aux ch. 4.11. et 4.12. et la *FMH* le commentaire exprimé à propos du ch. 4.5.1.1. *SQS* demande que les organismes de certification ne soient pas désignés comme des lieux de déclaration des incidents de sécurité. Dès lors, il n'y a pas besoin de définir de procédure de déclaration par les communautés. *SQS* propose dès lors que l'on supprime l'élément de texte « l'organisme de certification et » du ch. 4.13.1. *ISSS* observe que selon les dispositions en vigueur dans d'autres contextes, p. ex. dans le RGPD-UE, les informations sur des incidents affectant la sécurité des données doivent être aussi communiquées aux patients s'il s'avère qu'il existe probablement un risque élevé. Le ch. 4.13.1 doit dès lors être complété de la phrase suivante : « […] Par ailleurs, les communautés doivent définir une procédure formelle pour déclarer immédiatement des événements de sécurité aux patients concernés qui se retrouvent probablement exposés, par suite d'une violation de la protection de leurs données personnelles, à un risque élevé pour leurs droits et leurs libertés. »

4.14 Sécurité d'exploitation (al. 3)

4.14.1 : *HIN* relève à propos du ch. 4.14.1.1.1 qu'il s'agit d'une forte authentification à deux facteurs, fait qu'il convient de saluer. *SQS* veut savoir à ce propos à partir de quel point une authentification à deux facteurs peut être qualifiée de forte, et demande des précisions à ce sujet. Au sujet du ch. 4.14.1.1, *KSSG* fait savoir que la mise en place d'une authentification à deux facteurs pour un système d'exploitation, mais surtout pour une base de données et d'autres composants techniques, est considérée comme disproportionnée et difficilement réalisable. Cela signifierait que tous les utilisateurs dans l'Active Directory devraient se soumettre pour chaque objet (même hors contexte du dossier électronique du patient) à une authentification à deux facteurs, ce qui serait à la fois extrêmement coûteux et surtout plus du tout praticable pour l'exploitation. Suivant la banque de données, une authentification à deux

facteurs est même impossible à mettre en place. Le ch. 4.14.1.1 doit par conséquent être supprimé. *STSAG* craint également que les dispositions des ch. 4.14.1.1 et 4.14.1.3 à 4.14.1.10 occasionnent des coûts inadéquats et demande que l'on supprime purement et simplement ces dispositions. Dix participants[129] signalent que dans le texte allemand du ch. 4.14.1.1.2, une phrase est incomplète et qu'il y manque au moins un mot. Ce texte doit être complété. *HIN* propose concrètement d'introduire ici le mot « système ». Six cantons[130] voient difficilement comment on peut garantir qu'un système ne permettra pas d'exporter des données de patients alors qu'un accès privilégié permet de consulter ces mêmes données. Cet accès privilégié repose sur le secret professionnel. Ces cantons demandent la suppression du chiffre 4.14.1.1.3. *ISSS* considère que le ch. 4.14.1.2.3 est éloigné des réalités pratiques. Dès lors que le fournisseur doit garantir l'infrastructure et donc son fonctionnement permanent, on ne peut pas attendre un « cas de besoin » pour activer un accès. Cela empêcherait d'honorer des SLA (cf. 4.23.1.2). Ils demandent donc la suppression de ce chiffre. *ISSS* propose également de préciser au ch. 4.14.1.4 : « […] et qu'elles sont cryptées et conservées en un lieu sûr et physiquement séparé. ». À propos du ch. 4.14.1.5, ISSS reproche à cette disposition son manque de clarté et demande ce que l'on entend ici par « principe du double contrôle ». Il suppose probablement que le mot de passe est connu de plus d'une personne, mais les modalités d'implémentation technique doivent absolument être expliquées, sinon il vaut mieux renoncer à cette disposition. Pour ce qui est des ch. 4.14.1.4 et 4.14.1.5, *KSSG* considère qu'il n'y a pas de proportionnalité entre le cryptage des back-up et l'accès au matériel de cryptage en application du principe du double contrôle. Il faudrait édifier une infrastructure de back-up séparée pour le dossier électronique du patient, ce qui occasionnerait des coûts énormes. Il convient donc de reformuler ces chiffres pour obliger les exploitants informatiques à conserver les back-up en lieu sûr, à charge pour eux de trouver des solutions pratiques concrètes. *HIN* rappelle que les tâches exigées au ch. 4.14.1.7 seront automatisées si un fournisseur reprend l'exploitation de l'infrastructure informatique et y effectue régulièrement des sauvegardes. Une séparation physique du lieu de stockage est donc irréaliste vu qu'elle impliquerait des opérations manuelles. On peut donc biffer ce chiffre. *VAKA* souhaite également la suppression de ce chiffre, étant donné que l'exigence (déconnexion du réseau pendant le back-up) est sans doute excessive. *La Poste* trouve aussi que la déconnexion du réseau est une mesure exagérée. Les back-up sont déjà cryptés et les clés de cryptage protégées selon le principe du double contrôle. *SCH* relève à ce propos qu'en règle générale, on ne prévoit plus de systèmes de stockage de back-up à déconnecter du réseau après la copie, parce que le stockage de données selon les critères de sécurité ISO 27001 (cryptage, principe du double contrôle à l'accès, etc.) est considéré comme sûr. *SCH* demande également la suppression de ce chiffre. *HIN* est d'avis que le ch. 4.14.1.11 doit comporter, comme le ch. 2. 1, des précisions concernant la méthode d'effacement et propose de le compléter comme suit : « […] toutes les données sont préalablement contrôlées et documentées, puis intégralement et irréversiblement effacées selon les normes actuelles de bonne pratique. » En outre, *privatim* juge que le ch. 4.14.1.11 est formulé de manière trop imprécise au regard du droit sur la protection des données et propose l'énoncé suivant : « Les données de patients enregistrées sur des supports de données qui ne sont plus utilisés sont irréversiblement effacées, et les supports de données éliminés ensuite correctement. ». *SQS* fait remarquer que la disposition énoncée au ch. 4.14.1.12 figure déjà au ch. 2.9.25 et devrait donc être supprimée.

4.14.2/4.14.3 : Au sujet du ch. 4.14.2.5, *ISSS* demande si tous les systèmes doivent vraiment être dotés de composantes dédiées dans leur propre segment de réseau, et propose de reformuler la disposition comme suit : « […] de l'exploitant par une séparation appropriée (en cas de séparation sur une base non physique, de plus amples mesures de sécurité et de contrôle sont impératives et doivent être documentées en détail) ». *STSAG* observe que les exigences figurant au ch. 4.14.2 occasionnent des charges inadéquates et qu'il convient dès lors de les supprimer. Six cantons[131] déclarent à propos du ch. 4.14.3 que les exigences à satisfaire représentent une lourde charge et impliquent des coûts importants. Cela justifie qu'un délai jusqu'à cinq ans soit admis pour procéder à la certification complète. *KSSG* demande comment la disposition du ch. 4.13.3.4 doit être mise en œuvre, si un Change Management suffit ou si un automatisme (application) doit être activé à cet effet. La *CCM*, *GAeSO*, *BüAeV* et

[129] CCM, BüAeV, GAeSO, KAeG SG, HIN, La Poste, privatim, medshare, Medgate, SQS
[130] FR, NE, GE, VS, VD, JU
[131] FR, NE, GE, VS, VD, JU

KAeG SG réitèrent pour le ch. 4.14.3.10 leur prise de position sur le ch. 4.8.2. Concernant ce même ch. 4.14.3.10, *SCH* fait remarquer que l'impression de données et de documents en tant qu'action manuelle dans le système d'exploitation n'est pas connectée au système de protocole intégré. De ce fait, l'impression ne peut pas être automatisée ni réalisée de manière conforme aux critères de révision sans mise en œuvre de moyens substantiels.

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

KSSG juge irréalisable une surveillance des entreprises de développement par la communauté et demande la suppression intégrale du ch. 4.15. Une demande partagée par *K3*, *VZK*, *ZAD* et *ZH*, qui estiment que l'on peut se passer de ces dispositions. *Integic* fait valoir que la réalisation des points énoncés au ch. 4.15.2 est difficile dans des constellations impliquant des fabricants externes et requiert la participation des fabricants. Cela n'est cependant guère réaliste, de sorte qu'il convient de remanier ce texte. La CDS et huit cantons[132] estiment qu'il n'est pas possible d'exploiter des environnements de test – pour autant que l'on parle bien d'environnements d'intégration et de consolidation – sans disposer de données de patients. Rejointe en cela par *KSSG*, elle préconise de garantir la mise en œuvre des moyens techniques et organisationnels nécessaires pour sécuriser les données des patients dans un environnement de test du dossier électronique du patient de la même manière que dans un environnement de production. Elle demande que le ch. 4.15.2.5 soit reformulé ainsi : « les exigences de protection et de sécurité des données applicables à la conservation des données valent également pour les données de patients présentes dans les environnements de consolidation et d'intégration. Les autres environnements de test et de développement ne comportent aucune donnée de patients. » *KSSG* ajoute dans ses commentaires qu'un environnement d'intégration est également connecté aux environnements d'intégration des systèmes primaires. Il y a une volonté explicite de tester ces environnements d'intégration avec des données réelles. Le chiffre concernant les environnements d'intégration doit être biffé. *AR* observe au sujet du ch. 4.15.2.5 que les environnements de test qui utilisent des données de patients réelles doivent se conformer aux directives relatives à la protection des données. De l'avis de *H+*, les autres lois relatives au dossier électronique du patient doivent offrir un cadre qui permette l'utilisation de données de patients dans des tests de logiciels. *VGIch* est du même avis et trouve qu'il faut autoriser l'utilisation de données de patients pour les environnements d'intégration et de consolidation tant que les directives de protection et de sécurité des données des systèmes productifs sont appliquées. *SQS* préconise l'énoncé suivant pour le ch. 4.15.2.5 parce que plus réaliste : « Les environnements de test et de développement ne comportent aucune donnée de patients autre que des données anonymisées ou pseudonymisées. » *VAKA* et *La Poste* demandent la suppression du ch. 4.15.2.6. *VAKA* regrette que le texte ne précise pas ce qui est supervisé et chez qui. *La Poste* demande comment cela se passe avec des logiciels commerciaux et qu'est-ce que l'organisation d'exploitation a à voir avec le développement de logiciels. Cette exigence pourrait poser problème lors de la certification. *OFAC* signale une contradiction entre les exigences du ch. 4.15.1 et du ch. 4.15.5. La validation finale d'une nouvelle version avant sa mise en production nécessite un test de non-régression qui n'est réalisable qu'avec les vraies données que le système est appelé à traiter. Des mesures peuvent être mises en œuvre pour que les tests de validation n'engendrent pas de vulnérabilité et soient aussi strictement contrôlés que les systèmes de production. C'est plus une affaire d'organisation du Change Management que de conformité à une prescription légale. Le principe consiste à toujours pouvoir démontrer un bon équilibre entre la qualité des tests effectués et le respect de la sphère privée des patients.

4.16 Cryptage de la communication (al. 3)

La *SSIM* et la *FMH* plaident pour que la communication et le stockage des données soient entièrement cryptés. *STSAG* juge exagérées les exigences du ch. 4.16.1 vis-à-vis de la communauté et demande la suppression de ce passage.

4.17 Enregistrement crypté des données (al. 3)

[132] BL, GL, LU, OW, UR, FR, BS, SZ

Insel veut savoir à propos du ch. 4.17, s'il faut comprendre par « données sensibles » toutes les données des patients ou seulement celles qui méritent d'être protégées et demande une définition plus précise. La *SSIM* et la *FMH* renvoient à leur commentaire sur le ch. 4.16 et la *CCM*, *GAeSO*, *BüAeV* et *KAeG SG* réitèrent pour le ch. 4.17.1 leurs prises de position sur les ch. 4.8.2. et 4.14.3.10. Six cantons[133] renvoient également à leurs prises de position sur le ch. 4.8.2. à propos du ch. 4.17. De l'avis de treize participants[134], il faut choisir : ou l'on crypte toutes les données, ou l'on n'en crypte aucune. On ne voit pas pourquoi seules les « données sensibles » doivent être cryptées. On ne comprend pas davantage pourquoi la sauvegarde sous forme cryptée doit être réservée aux données des niveaux de classification « secret » et « sensible ». Cela ne permettra de réaliser aucune économie, vu que des frais seront immanquablement perçus pour les possibilités de cryptage. Le ch. 4.17.1 doit donc être remanié en conséquence. *TG* et *AI* partagent le sentiment que l'on ne pourra pas réaliser d'économies et demandent donc que le cryptage soit appliqué à toutes les données. *VAKA* considère que l'élément en fin de phrase « de manière à ce que leur intégrité soit protégée » n'est d'aucune utilité pour des données de toute manière déjà cryptées, et qu'il peut dès lors être supprimé. *VAKA* s'étonne par ailleurs des déclarations concernant le cryptage de terminal à terminal (end-to-end-encryption) dans le rapport explicatif. L'argumentation n'est pas convaincante et la formule « renoncé dans un premier temps » résonne comme une menace. *VAKA* n'est pas opposé par principe aux nouvelles technologies, mais s'étonne tout de même qu'une technologie qui n'a encore jamais été discutée dans les cénacles de eHealth Suisse soit mentionnée de manière aussi prééminente. D'autant plus qu'il reste de nombreuses questions à élucider en la matière. *Tessaris* fait valoir que le qualificatif de « sensibles » est réservé aux données du dossier électronique qui se rapportent à la santé et au traitement médical du patient (« informations pertinentes pour le traitement »). Les autres données (adresse, renseignements administratifs, métadonnées) servent à l'administration et à l'exploitation du dossier électronique du patient, ainsi qu'à la transmission des données pertinentes pour le traitement. Pour des raisons pratiques et pour éviter tout problème de délimitation, il pourrait être préférable de sauvegarder aussi sous forme cryptée les données du patient pertinentes pour le traitement et les métadonnées. *Tessaris* propose dès lors l'une des deux formulations suivantes : « Les <u>données du dossier électronique du patient, à l'exception des métadonnées</u>, doivent être sauvegardées sous une forme cryptée, à l'aide de mesures cryptographiques <u>adéquates et conformes à l'état actuel de la technique</u> […] » ou, si l'on préfère : « Les <u>données du dossier électronique du patient</u> qui se rapportent au traitement du patient doivent être […] ».

<u>4.19 Sécurité de la communication : gestion des réseaux (al. 3)</u>
ISSS propose d'ajouter un nouveau chiffre 4.19.1.4 dont l'énoncé est « les points d'accès WLAN non autorisés sont détectés et identifiés », tout en observant que cette exigence supplémentaire, selon l'interprétation qu'on lui donne, est éventuellement déjà prévue au ch. 4.19.1.2.

<u>4.20 Sécurité de la communication : services réseau (al. 3)</u>

<u>4.20.1 :</u> Six cantons[135] demandent ce que sont les « services d'information, d'utilisateurs et de systèmes d'information » et souhaitent que l'on donne des exemples concrets de tels services. *VAKA* demande que l'on examine si les exigences énoncées au ch. 4.20.1.1 ne figurent pas déjà sous cette forme dans l'ATNA. Si c'est le cas, ce dernier chiffre doit être supprimé. *SQS* réitère pour les ch. 4.20.1.1.2.1 à 4.20.1.1.5 ses commentaires relatifs au ch. 2.9.3. Elle demande que les ch. 2.9.4 à 2.9.21 soient complétés de dispositions régissant la fourniture de preuves que les conditions techniques ont fait l'objet d'un examen technique, En ce qui concerne les ch. 4.20.1.1.2.1 et 4.20.1.1.2.2, *SCH* fait valoir que les certificats EV (à validation étendue) font également l'objet de critiques pour occasionner plus de frais et de charges administratives que les certificats TLS publics tout en n'offrant qu'en apparence une plus grande sécurité. La protection effectivement conférée par un certificat EV peut être identique, mais peut même être inférieure à celle d'un certificat ordinaire. *SCH* demande par conséquent que l'exigence de « validation étendue » soit supprimée du texte des deux chiffres. *ISSS* préconise d'ajouter à l'article un ch. 4.20.1.1.6 rédigé comme suit : « seuls les services nécessaires au fonctionnement du système, les

[133] FR, NE, GE, VS, VD, JU
[134] CDS, BL, GL, LU, OW, UR, ZG, SZ, ZH, NW, K3, VZK, ZAD
[135] FR, NE, GE, VS, VD, JU

protocoles et les démons sont activés ».

4.20.2/4.20.3 : *EHS* et *VGIch* déplorent le fait que le ch. 4.20.2.1 empêche d'exploiter la synergie de la communication dirigée et non dirigée via une plateforme eHealth et cause des frais supplémentaires inutiles, encourageant ainsi l'utilisation de systèmes propriétaires pour la communication dirigée. Une séparation logique claire suffit amplement. Ce chiffre doit être adapté comme suit : « Des mesures sont prises pour permettre l'utilisation des composants (Repository, Registry, Index des patients) en vue de recourir en toute sécurité à la communication dirigée et non dirigée selon les dispositions de la LDEP/ODEP », un point de vue partagé par *Insel*. Au ch. 4.20.2.1, *ISSS* regrette que l'on ait utilisé le verbe « séparer » (« separiert » dans le texte allemand) qui laisse une marge d'interprétation beaucoup trop grande, d'où sa proposition de compléter le texte comme suit : « […] moins élevé. En cas de séparation sur une base non physique, de plus amples mesures de sécurité et de contrôle sont impératives et doivent être documentées en détail ». *VAKA* préconise la suppression de certains éléments du texte pour que le ch. 4.20.2.1 ait la teneur suivante : « séparer, au niveau du réseau, le registre de documents, le lieu de stockage des données, la gestion des autorisations et l'index des patients de tous les autres systèmes ». *SCH* déclare à propos du ch. 4.20.3.1 que les zones dites « démilitarisées » (DMZ) ne représentent qu'une possibilité parmi d'autres de sécuriser des réseaux via une gestion d'accès échelonnée au moyen de pare-feu ; il existe aujourd'hui bien d'autres concepts, en particulier dans l'architecture Cloud. À propos du ch. 4.20.3.2, *SQS* demande sur quelle base ou exigence il est possible d'exploiter ou de documenter un pare-feu applicatif Web (WAF) et quels sont les aspects de l'implémentation d'un WAF auxquels il faut prêter attention. Un WAF peut se présenter sous forme d'un applicatif matériel, d'un plug-in logiciel sur serveur Web, d'un add-on pour pare-feu réseau ou d'un équilibreur de charge. L'exigence de documentation pour l'infrastructure HW/SW du portail d'accès devrait être formulée en termes plus génériques. Il convient par conséquent de compléter ou de reformuler le texte de ce chiffre.

4.21 Expiration des sessions dans le réseau (« session timeout »)

Privatim souhaite que ces dispositions soient reformulées par souci de clarté. Par ailleurs, il convient de vérifier si deux heures d'inactivité ne sont pas excessives pour un professionnel de la santé : « Le système ferme automatiquement les sessions réseau restées inactives (aucune opération effectuée) pendant une période définie. Cette période d'inactivité est de 20 minutes pour les patients et d'une heure pour les professionnels de la santé ». *VGIch* réitère ici sa prise de position relative au ch. 4.9.3. *Insel* relève que les patients percevront une durée de session aussi courte comme une entrave significative à la commodité d'utilisation du système et propose à la place que cette disposition s'inspire des solutions de services bancaires en ligne. Le patient peut choisir lui-même le paramétrage du time-out et en assumer personnellement le risque. *K3*, *VZK*, *ZAD* et *ZH* trouvent peu judicieux de vouloir prescrire des chiffres absolus pour une fin de session automatique. Une réglementation générale et abstraite devrait suffire. Le ch. 4.2.1 doit être supprimé et remplacé par une disposition à inscrire dans l'ODEP-DFI. *SQS* trouve que vouloir imposer la durée d'une session n'a guère de sens. À son avis, il est également discutable de fixer un intervalle de deux heures aux professionnels de la santé. Il faut supprimer les mentions de temps ou déterminer une durée maximale. Une fin de session au bout de 20 minutes au maximum devrait être valable pour tous. La *FMH*, la *SSIM* et *STSAG* jugent disproportionné de vouloir déterminer au niveau d'une ordonnance le temps écoulé avant une fin de session et demandent donc la suppression du ch. 4.21. *Bleuer* attire l'attention sur le risque d'ouverture incomplète de documents que comportent les limites de durée fixées au ch. 4.21et qu'il convient donc de les supprimer ou au moins de les prolonger. *BINT* demande la suppression du ch. 4.21 car il pourrait avoir pour effet que les données obtenues sur le patient soient incomplètes. Pour les données personnelles du patient, cette disposition représente en outre une ingérence dans la sphère privée. On se demande pourquoi cette question doit être réglée au niveau de l'ordonnance et pourquoi une durée plus brève est définie pour le patient. D'après *ISSS*, il est juste de prévoir une fin de session, mais il serait plus judicieux de la définir ailleurs et de se borner ici à en indiquer la référence. Une éventuelle modification de la durée des sessions ne devrait pas contraindre à revoir toute l'annexe. D'ailleurs, il serait sans doute plus adéquat de parler de sessions en général plutôt que de « sessions de réseau », les mêmes principes

pouvant s'appliquer aux postes de travail hors ligne. *ISSS* propose de reformuler comme suit le ch. 4.21.1 : « […] prennent fin automatiquement après une période d'inactivité définie » et le ch. 4.21.2 : « […], faute d'interaction de l'utilisateur avec le dossier électronique du patient pendant la période d'inactivité ». *SCH* rappelle que d'après les expériences recueillies sur le portail de santé de Swisscom, les utilisateurs perçoivent une courte durée de session comme une entrave significative à l'usage de ce portail, surtout si on leur impose à nouveau la procédure d'authentification à deux facteurs après la fermeture d'une session. La limitation de la durée de session est aujourd'hui une mesure courante de prévention du piratage. Étant donné que l'ordonnance exclut d'ores et déjà tout téléchargement massif de documents dans le dossier électronique du patient, le dommage escompté en cas d'incident se limiterait à un nombre restreint de documents. Il n'est pas exclu que des opérateurs informatiques innovants développent d'autres procédés pour empêcher le piratage de sessions afin de répondre au souhait d'une meilleure convivialité. *SCH* propose que l'exploitant des communautés démontre qu'il a pris des mesures adéquates conformes aux progrès techniques pour prévenir les piratages de sessions. Six cantons[136] font valoir à propos du ch. 4.21.1 qu'une durée de deux heures est beaucoup trop courte pour un professionnel de la santé et qu'une durée de quatre heures, voire d'une demi-journée serait mieux indiquée. Il faut en effet éviter à un médecin de devoir se reconnecter trop souvent. Ils demandent concrètement que le temps soit modifié et que la notion de « sessions dans le réseau » soit mieux définie. *SUVA* ne comprend pas pourquoi les sessions dans le réseau doivent se fermer après une période d'inactivité de 20 minutes pour les patients et de deux heures pour les professionnels de la santé. Cela constitue une grave ingérence dans la sphère privée du patient, sans compter que la différence de durée en fonction des utilisateurs n'est conforme ni à la loi, ni au principe de proportionnalité. Il convient dès lors soit de biffer le ch. 4.21.1, soit d'harmoniser les limites de durée des sessions.

4.22 Système intermédiaire (al. 3)

KSSG estime qu'un coaching de telles données doit être possible pour que le dossier électronique du patient atteigne une performance acceptable ou continue de fonctionner en cas de panne du service CPI central.

4.23 Accessibilité (al. 3)

ISSS critique le flou de la formule « disponibilité convenue contractuellement d'au moins 98 % sur la durée » au ch. 4.23.1.2. Cela correspond à sept jours d'interruption sur une durée de référence d'une année. Il lui préfère une formulation qui prévoit une durée d'interruption fixe et/ou définie durant une certaine période, d'où sa demande de compléter le chiffre comme suit : « […] forte sollicitation ; la durée maximale d'une interruption continue ne doit pas dépasser 48 heures ». *La Poste* veut que l'on précise le ch. 4.23.1.2 ; elle demande notamment ce que l'on entend par « forte sollicitation ». Par ailleurs, les systèmes externes pertinents pour les communautés doivent aussi répondre à ces exigences. *La Poste* demande par conséquent que cette obligation de la CdC et des Services Centraux soit inscrite au bon endroit dans les ordonnances. HIN fait remarquer à propos du ch. 4.23.1.3 qu'il n'y a pas de protection intégrale contre des attaques par déni de service (DoS) sans recours à des terminaux spécifiques. D'ailleurs, pourquoi mentionner explicitement cette menace et non les autres ? *HIN* ose croire que l'adhésion aux différentes normes (ISO, etc.) implique une protection des ressources Internet à la hauteur des progrès techniques. En remplacement, *HIN* propose l'introduction de contrats de service (Service Level Agreements, SLA) pour les demandes intercommunautaires et de portails pour patients/professionnels de la santé, ainsi que la suppression du ch. 4.23.1.3. Chez *Tessaris*, on déclare à ce propos qu'une protection absolue contre les attaques par déni de service, telle qu'ils la conçoivent, est irréalisable à leur avis. Il n'empêche qu'il faut engager les moyens offerts par les progrès techniques pour se défendre contre de telles attaques. Ils proposent l'énoncé suivant : « […] contre les attaques DoS (par déni de service, denial of service) en fonction des progrès techniques ». *STSAG* considère que le ch. 4.23.1.4 occasionne des charges inadéquates et doit donc être supprimé.

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

[136] FR, NE, GE, VS, VD, JU

Privatim renvoie ici à ses déclarations relatives à l'art. 11, al. 4, ODEP. *AR* approuve le stockage des données sous le régime du droit suisse. La *CDS* et huit cantons[137] objectent que les arguments présentés pour soumettre le dossier électronique du patient au droit suisse ne sont pas convaincants Il faut craindre que l'objectif ne puisse être atteint par ce moyen, c'est pourquoi le ch. 4.24 doit être entièrement revu. *ZAD*, *ZH* et *ZG* demandent également une refonte complète. Ils avancent que la formule « personnes morales soumises au droit suisse » est peu usitée et demandent ce que l'on entend par là. La même remarque vaut pour la formule : « agissent exclusivement sous le régime du droit suisse pour accomplir leurs prestations ». Une garantie que ne pourrait guère offrir une entreprise également active hors du territoire national, d'où la question du but poursuivi par une telle disposition. La formule « fournissent toutes leurs prestations sur le territoire suisse » mérite aussi d'être éclaircie. Les intervenants demandent ce qu'il en est d'une entreprise qui a ses serveurs et son administration en Suisse, mais fait appel à des prestataires à l'étranger pour certains services (ce qui devrait être le cas de la plupart des entreprises d'une certaine importance). *ZAD* et *ZH* ajoutent qu'il convient d'examiner si l'exigence de mandater une entreprise suisse est compatible avec les dispositions relatives aux marchés publics (et en particulier avec l'AMP et les accords bilatéraux).

La *CCM*, *BüAeV*, *GAeSO, KAeG SG* et *HIN* observent que la formulation du ch. 4.24.1.1 demandant de garantir que l'exploitation interne à la communauté du dispositif de stockage du dossier électronique du patient incombe à des personnes morales « soumises au droit suisse » manque de clarté dans sa version allemande (« unter Schweizer Recht sind »). Ils présument qu'elle a le même sens que « Schweizer Recht unterstehen », ce qu'ils proposent en remplacement ainsi que l'option « in der Schweiz domiziliert sind » (« domiciliées en Suisse »). *SCH* rapporte à propos du ch. 4.24.1.2 qu'en vertu de l'annexe, toutes les prestations doivent être fournies sur le territoire suisse. Ne serait-ce qu'en raison du leadership démontré par d'autres pays dans ces technologies, les solutions informatiques développées exclusivement avec des partenaires domiciliés en Suisse sont l'exception. Exiger que la totalité des prestations soit fournie à l'intérieur de nos frontières contraindra la communauté à délivrer aux prestataires une autorisation expresse pour tout traitement de données effectué à l'étranger. Outre qu'elle n'est pas nécessaire pour assurer le respect du droit suisse, une telle exigence risque de déstabiliser la fourniture de prestations. Même pour le stockage de données par des entreprises suisses dans des centres de calculs en Suisse, il est dans l'intérêt du client de consentir le cas échéant au traitement de ses données par des sous-traitants ou des collaborateurs à l'étranger. La finalité devrait être que la prestation principale soit fournie pour l'essentiel en Suisse. *SCH* propose l'énoncé suivant pour le ch. 4.24.1.2 : « fournissent leur prestation principale pour l'essentiel sur le territoire suisse ».

SWICO demande la suppression pure et simple du ch. 4.24.1.3. Du côté de *Tessaris*, on fait remarquer qu'à leur avis général, cette réglementation, qui s'adresse à des communautés gérées dans une très large mesure comme des organisations de droit privé, contrevient à l'art. 3 et à l'art. 23, al. 3 de l'accord sur les marchés publics (RS 0.632.231.422) parce qu'on ne peut pas, de bonne foi, tenir pour acquis que la protection et la sécurité des données du dossier électronique du patient ne pourront être assurées que par une entreprise se trouvant en majorité en mains suisses. Ils demandent également la suppression de ce chiffre. *EHS* et *VGIch* font remarquer à propos des ch. 4.24.1.3 et 4.24.1.4 que les personnes morales en Suisse sont soumises au droit suisse, quels que soient les rapports de propriété. Un appel d'offres pour une plateforme eHealth par une entité suisse responsable de cybersanté serait soumis aux règles du GATT-OMC et dans une telle hypothèse, des soumissionnaires étrangers ayant une succursale en Suisse pourraient alors y participer, mais ne seraient pas autorisés ensuite à exploiter eux-mêmes une telle plateforme. *EHS* et *VGIch* qualifient d'inadmissibles les dispositions de ces deux chiffres parce qu'elles contreviennent à un droit supérieur. Une telle réglementation n'a rien à faire dans les CTO. Six cantons[138] demandent à propos du ch. 4.24.1.4 s'il signifie que les personnes morales doivent exercer leur activité en Suisse seulement. Ce chiffre doit être reformulé. *La Poste* demande à propos de cette disposition si elle s'applique aux prestations contractuelles. Le contraire, pour autant

[137] BL, GL, LU, OW, UR, FR, NW, SZ
[138] FR, NE, GE, VS, VD, JU

qu'il s'agisse d'une règle de portée générale, reviendrait à exclure des prestataires qui fournissent également des prestations à l'étranger. Ce ne serait pas raisonnable, notamment parce que cela reviendrait à exclure aussi *La Poste*. Celle-ci observe également que le texte allemand et sa traduction française n'ont pas la même signification et demande des explications.

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

Treize participants[139] réitèrent pour le ch. 5.1.2.2 leurs commentaires relatifs au ch. 4.10.2.3. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* saluent la mise en place d'un service-desk. Il manque cependant une disposition déterminant qui doit assumer les coûts de son exploitation et de l'assistance prodiguée par le service-desk. Le service d'assistance destiné aux professionnels de la santé ne devrait pas leur occasionner de frais supplémentaires, vu que l'introduction du dossier électronique du patient leur coûte déjà très cher. Ils demandent que le ch. 5.1.1 soit complété comme suit : « […] afin de les aider gratuitement dans l'utilisation du dossier électronique du patient ». *STSAG* demande que la disposition visée au ch. 5.1.1 soit restreinte aux communautés de référence, ce qui implique de remplacer le terme de « communauté » par celui de « communauté de référence » dans le texte. Six cantons[140] précisent à propos du ch. 5.1.2.2, que le personnel est soumis au secret professionnel, si bien qu'il est inutile de rappeler qu'ils doit être soigneusement sélectionné ; ce chiffre peut donc être supprimé. *GE*, *VS*, *VD*, *JU* et *FR* ajoutent à propos du ch. 5.1.2.4 qu'une documentation des accès est techniquement impossible avec les logiciels commerciaux et demandent par conséquent de supprimer le passage « et que l'accès est documenté automatiquement ». *HIN* salue la disposition du ch. 5.1.2.4 exigeant de documenter les accès à distance, mais estime qu'une documentation automatisée ne devrait pas être obligatoire et recommande donc de supprimer le terme « automatique ». À propos des accès à distance, *La Poste* se demande comment informer à leur sujet et comment ils sont autorisés et documentés.

6. Information du patient (art. 14 ODEP)

K3, *VZK*, *ZAD* ainsi que *ZG* et *ZH* sont d'avis que les règles établies au ch. 6 découlent déjà des dispositions de la LDEP et de l'ODEP et que l'on peut par conséquent les supprimer purement et simplement.

6.1.2/6.1.3 : Six cantons[141] estiment que les points à expliquer au patient sont trop longs et trop compliqués pour qu'il soit en mesure de les comprendre. L'expérience des cantons romands, qui porte sur plusieurs dizaines de milliers de patients, montre que le temps de concentration et de patience dont ils sont capables ne dépasse pas 15 minutes. Seuls les points essentiels doivent être expliqués. Selon leurs estimations basées sur la pratique, il faudrait au minimum 30 minutes supplémentaires pour expliquer les points du chapitre 6.1 à une personne d'âge moyen et en bonne santé psychique. Pour une communauté de 100 000 patients, il faudrait donc 4 500 000 minutes, soit 9375 jours/homme ou 42 années/homme. Entre dix employés, cela représente quatre ans de travail à raison d'un million de CHF/an de salaires. Seuls les points suivants doivent être retenus en première intention : 6.1.2.5, 6.1.3.5, 6.1.4.1-2-5, 6.1.5.2. Le patient doit avoir la possibilité de se renseigner sur les autres sujets. *VAKA*, *K3* et *VZK* considèrent que les informations à donner en vertu du ch. 6.1.2.1 dépasseraient sans doute l'entendement de tout patient ordinaire, c'est pourquoi il convient de biffer cette disposition. *VAKA* ajoute à propos du ch. 6.1.2.3 que c'est ce que ferait toute communauté de référence dans son propre intérêt et qu'il n'y a donc pas besoin de prescrire cette règle ; dès lors, elle peut aussi être biffée. *KSSG* relève que la communauté de référence peut certes informer le patient de cette possibilité, mais n'a pas le moyen de la lui garantir. *OFAC* relève qu'il faut préciser qu'on parle d'un dossier patient unique conforme à la LDEP. Il est hébergé par une communauté de référence certifiée qui utilise un NIP unique généré par la CdC. Les dossiers pilotes cantonaux, non certifiés selon les exigences de la LDEP, et ceux qui n'utilisent pas le NIP unique n'entrent pas en ligne de compte. Au sujet du ch. 6.1.3.4, l'*OSP* veut savoir ce que l'on entend par « les conséquences qui s'ensuivent » (d'un changement de la com-

[139] AR, BL, CDS, GL, LU, OW, UR, SZ, ZG, ZH, ZAD, TI, NW
[140] FR, NE, GE, VS, VD, JU
[141] FR, NE, GE, VS, VD, JU

munauté de référence). S'il s'agit des processus énoncés aux ch. 8.4.2.2 et 8.4.2.3, il n'y a rien à changer, sinon, il convient d'exposer toutes les conséquences individuellement. *VAKA*, *K3* et *VZK* voient dans le ch. 6.1.3.5 une contradiction avec l'obligation de conserver la déclaration de révocation ; il convient donc d'en modifier le texte. *IG eHealth* ajoute à propos du ch. 6.1.3.6 que le dossier électronique du patient peut être supprimé en vertu de l'art. 20, al. 1, ODEP. La suppression du dossier est suivie de l'annulation du NIP dans la banque de données d'identification de la CdC. Après révocation de la tenue d'un dossier électronique, le patient a cependant la possibilité de faire ouvrir un nouveau dossier. Un nouveau NIP est attribué au patient en cas de réouverture du dossier. *IG eHealth* salue la possibilité donnée au patient d'ouvrir à plusieurs reprises un dossier électronique. Avant toute suppression d'un dossier électronique du patient, il faudra toutefois avertir le patient que les données enregistrées dans son dossier seront perdues à jamais. À la réouverture de son dossier électronique, le patient devra y réintroduire les documents souhaités.

6.1.4/6.1.5 : Au sujet du ch. 6.1.4.6, *La Poste* demande d'expliquer comment obtenir l'autorisation pour l'accès à distance et comment cet accès doit être documenté. *ZH* et *ZAD* jugent problématique de prévoir un accès à distance aux terminaux des patients pour les collaborateurs du service d'assistance. Des accès à distance conformes à la procédure de sécurité ne doivent pas pouvoir être exécutés sans la participation du patient. Une communauté de référence ne doit pas assurer la possibilité d'un tel accès, comme le signalent aussi *K3* et *VZK*. *ZH*, *ZAD*, *K3* et *VZK* demandent par conséquent la suppression du ch. 6.1.4.6. *VGIch* réitère pour le ch. 6.1.5 sa prise de position sur l'art. 14, al. 2, ODEP. *STSAG* demande que l'alinéa soit complété d'un ch. 6.1.5.6 formulé comme suit : « risque de compromettre la sécurité du traitement par le paramétrage des droits d'accès et de devoir en assumer l'éventuelle responsabilité ».

7. Consentement (art. 15 ODEP)

K3, *VZK*, *ZH* et *ZG* réitèrent ici leur prise de position relative au ch. 6. *SCH* demande que dans la perspective d'une extension généralisée du numérique, la signature électronique qualifiée soit clairement acceptée comme équivalente à la signature manuscrite en application de l'art. 14, al. 2bis, CO, mais d'autres moyens doivent également être admis pour l'identification univoque des personnes. Cette précision doit être clairement formulée dans le texte de l'ordonnance (et pas seulement dans le rapport explicatif). Le ch. 7.1.1 doit donc être complété de la phrase suivante : « […] avec sa signature. Sont assimilés à la signature manuscrite la signature électronique qualifiée ainsi que d'autres moyens auxiliaires destinés à l'établissement univoque de l'identité du patient.

8. Gestion (art. 16 ODEP)

ZH, *K3*, *VZK* et *ZAD* demandent la simplification du ch. 8, qu'ils jugent trop détaillé. Cette réglementation découle déjà en grande partie de la LDEP et de l'ODEP et n'a pas sa place ici. Cela s'applique en particulier aux ch. 8.6. et 8.7.

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

La Poste signale à propos du ch. 8.1.1.1 que la phrase du texte allemand doit être complétée comme suit : « […] zur Sicherstellung der Vorgaben nach […] ».

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

Pour *K3* et *VZK*, soumettre les patients à des critères aussi stricts que les professionnels de la santé pour les MID leur donnant accès à leur propre dossier électronique du patient est une exigence qui va trop loin. Elle revient à contraindre tous les patients à se procurer un MID payant (à renouveler, de surcroît) pour pouvoir gérer leur dossier électronique. Les patients doivent pouvoir accéder gratuitement à leur dossier électronique par des moyens comparables par ex. à ceux des services bancaires en ligne. Cela vaut pour le ch. 8.2.2, le ch. 8.3.1 et, selon la situation, pour le ch. 8.8.2. *La Poste* observe à propos

du ch. 8.2.2.1.1 qu'elle a besoin du NAVS13 pour obtenir un NIP auprès de la CdC. À son avis, aucun éditeur de MID n'a le droit de saisir et d'éditer un NAVS13. Toutes ces règles d'utilisation du MID manquent leur but. En ce qui concerne le ch. 8.2.2.2, *OFAC* réitère sa prise de position relative au ch. 6.1.3.2 et *KSSG* renvoie à ses remarques à propos du ch. 6.1.3.2. *KSSG* demande en outre que ce chiffre soit supprimé ou que l'on mette à disposition une possibilité technique d'interrogation. *Integic* souhaite que l'on explique comment s'assurer que la disposition au ch. 8.2.2.2 est respectée.

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

VAKA, *K3* et *VZK* sont d'avis qu'il faut absolument mentionner au ch. 8.3.3 la possibilité de s'authentifier par mTan. *HIN* rappelle sa satisfaction d'avoir obtenu l'authentification à deux facteurs et prône le maintien en l'état du ch. 8.3.3.1. *La Poste* se plaint que le ch. 8.3.3.1 est incompréhensible. Il permet la mise en place de n'importe quelle procédure d'authentification une fois que l'on dispose du MID d'un éditeur certifié. Elle demande l'instauration d'une procédure standard valable pour tous.

8.4 Changement de communauté de référence (let. e)

Du côté de *privatim*, on est d'avis que le ch. 8.4.2 doit prévoir l'obligation pour les « anciennes » communautés de référence de détruire toutes les informations dont elles disposent sur un dossier électronique du patient, à l'exception des documents dont la conservation est exigée par la loi (par ex. art. 20, al. 2, let. a, ODEP). Ils proposent concrètement la formulation suivante : « toutes les données liées au dossier électronique du patient sont supprimées de manière irréversible, à l'exception des documents dont la conservation est exigée par la loi ». *Medgate* signale une erreur dans le texte allemand du ch. 8.4.2.2, qu'il propose de corriger comme suit : « die Ermächtigung von Gesundheitsfachpersonen gemäss […] ». *BFH* comprend mal pourquoi le ch. 8.4.2.3 prévoit la perte automatique de la qualité de représentant lors d'un changement de communauté de référence. Ce fait devrait être communiqué activement au patient. *GE*, *VS*, *VD*, *JU* et *FR* sont d'avis qu'en cas de changement de communauté de référence, la suppression du dossier électronique du patient devrait être possible mais pas obligatoire. Six cantons[142] estiment qu'un médecin qui quitte un patient doit garder un accès au dossier médical même s'il n'en a plus besoin. En outre, de l'avis de ces cantons, il n'y a pas de raison de croire qu'un patient qui change de communauté voudrait changer du même coup son représentant. Il convient donc de supprimer les ch. 8.4.2.2 et 8.4.2.3. La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* saluent le fait que la suggestion de réglementer le changement de communauté de référence, émise durant la procédure de consultation sur la LDEP, ait été suivie. Il est cependant douteux que ce changement fonctionne selon les règles établies si une communauté de référence est dissoute, et on ignore ce qui se passe si la communauté de référence ne peut pas procéder au changement. Les participants suggèrent que l'on intègre ici l'obligation d'établir des dispositions de référence. Ils demandent l'ajout d'un ch. 8.4.2.4 à la teneur suivante : « le patient peut changer de communauté de référence même lorsque cette dernière ne peut procéder au changement ».

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

KSSG considère que le ch. 8.5.1 est formulé de manière incompréhensible et impossible à interpréter. Les dispositions des ch. 8.5 et 8.5.1 doivent être reformulées de manière à être clairement comprises.

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

VAKA dit ne pas comprendre ce que ce chiffre apporte au texte. Il ne fait que refléter les informations contenues dans l'ODEP et devrait être supprimé. Pour le ch. 8.6.2.3, *BFH* renvoie à son commentaire sur la problématique relative à l'art. 8, let. e, ODEP.

8.7 Options du patient (art. 3 ODEP)

[142] FR, NE, GE, VS, VD, JU

VAKA rappelle ici sa position exprimée à propos du ch. 8.6. *AR* renvoie pour le ch. 8.7.2.1 à ses commentaires et à ses propositions d'amendement de l'art. 3, let. a, ODEP. *KSSG* rappelle qu'en milieu hospitalier, ce sont surtout les médecins-assistants qui changent relativement souvent de spécialité et donc de groupe. Or, le ch. 8.7.2.6 priverait précisément les médecins-assistants – les plus tributaires des données figurant dans le dossier électronique du patient – de l'accès aux informations pertinentes. Il doit donc être supprimé. Il suffit amplement que le patient soit informé des nouvelles entrées et des mutations. *La Poste* relève à propos du ch. 18.7.2.8 que cette option devrait être paramétrée par défaut. Il convient de déterminer jusqu'où va la chaîne des droits d'accès. Six cantons[143] ne trouvent pas claire la disposition du ch. 8.7.2.9 et souhaitent qu'on l'explique à l'aide d'exemples concrets.

8.8 Représentation (art. 16, al. 3)

La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* signalent que l'art. 16, al. 3, ODEP n'existe pas. Ce renvoi dans le titre doit être supprimé et peut être éventuellement remplacé par celui à l'art. 3, let. g, ODEP. Six cantons[144] signalent qu'aux ch. 8.8.2 et 8.8.3.4, les termes « du patient » figurent à double dans la version française et qu'il faut y biffer les mots de trop. À propos du ch. 8.8.3.4, ils précisent que le représentant peut disposer de plusieurs moyens d'authentification (mTan, SwissID, etc.). Ils ajoutent que dans la pratique, il sera très difficile de garantir la réalisation de cette exigence lors d'un audit de certification et demandent des exemples concrets de la façon de garantir la « manière univoque et correcte ». Le ch. 8.8.3.4 doit être reformulé comme suit : « le compte utilisateur servant au représentant du patient est relié de manière […] ».

9. Service d'assistance pour les patients (art. 17 ODEP)

9.1. Conformité aux dispositions légales

9.1.1 : *VAKA* signale à propos du ch. 9.1.1 qu'il s'agit sans doute d'une inscription erronée et en demande la suppression. *La Poste* demande ce qu'il faut comprendre dans le texte allemand par « einschlägig rechtlichen Anforderungen » (exigences juridiques en la matière) et demande une clarification du ch. 9.1.1. Même écho du côté de *privatim*, qui se demande à quelles dispositions légales le texte se réfère ici. Il doit être plus précis dans son énoncé et citer quelques-unes de ces dispositions à titre d'exemple. Pour *ZG*, *ZH*, *K3*, *VZK* et *ZAD*, il est évident que les exigences juridiques en la matière doivent être respectées. Cela ne se discute pas. Mais il est faux d'en faire une condition de certification car un organisme de certification n'est pas en mesure de vérifier si toutes les dispositions sont effectivement respectées. Il demande donc la suppression du ch. 9.1.1.

9.1.3 : Six cantons[145] trouvent que le ch. 9.1.3.1 n'est pas clair. Quand le patient met ses données à disposition, c'est qu'il donne son consentement. Il faut donc clarifier la situation. *Medgate* signale une faute de frappe dans la version allemande : « […] nur dann im elektronischen Patientendossier erfasst […] ». *La Poste* relève que les ch. 9.1.3.1 et 9.1.3.2 sont contradictoires. En effet, certains documents sont saisis hors du dossier électronique du patient et ne peuvent y être transférés qu'avec son consentement. D'un autre côté, il est interdit d'effectuer des sauvegardes intermédiaires hors du dossier électronique du patient. Il y a lieu de préciser les modalités. *SBC* demande la suppression du ch. 9.1.3.2, étant d'avis que la limitation n'a pas de raison d'être. La *SSIM* fait la même demande. Selon elle, il est disproportionné d'exiger que la saisie des données fournies par le patient ne puisse s'effectuer que directement dans le dossier électronique du patient. *BINT* ajoute que le ch. 9.1.3.2 ne saurait servir de règle générale et souhaite également sa suppression. Qu'un document soit téléchargé directement dans le dossier électronique du patient puis transféré vers un autre espace de stockage ou vice-versa n'a aucune importance. *Medgate* signale ici aussi une faute de frappe dans la version allemande : l'ortho-

[143] FR, NE, GE, VS, VD, JU
[144] FR, NE, GE, VS, VD, JU
[145] FR, NE, GE, VS, VD, JU

graphe correcte est « bereitgestellten ». Pour *privatim* se pose ici la question de savoir comment procéder avec des données qui doivent être transférées dans le dossier électronique du patient au moyen d'applis de santé. Ils demandent comment s'assurer que ces données ne véhiculent pas un logiciel malveillant ou autre menace potentielle. *OFAC* signale à propos du ch. 9.1.3.3 qu'il contredit les chiffres 3.5.1.3 et 9.5.1.3 qui, eux, autorisent le « bulk download ». Au ch. 9.1.3.3, six cantons[146] ne comprennent pas le sens de la phrase et demandent de préciser ce que l'on entend par « domaines fonctionnels ». La *SSIM* rappelle que le patient peut contrôler la retransmission des données par l'octroi des autorisations d'accès. Une retransmission implicite des données saisies peut fort bien être dans l'intérêt du patient. Ces cantons demandent donc la suppression du ch. 9.1.3.3. La *FMH* demande un examen critique de la disposition au ch. 9.1.3.3 sous l'angle de l'utilité thérapeutique et de la sécurité du patient.

9.2 Présentation

Douze participants[147] réitèrent pour le ch. 9.2.1.3 leurs commentaires relatifs au ch. 3.2.1.3. *BFH* ne voit pas clairement de différence entre les ch. 9.2.1.1 et 9.2.1.2. *Medgate* signale deux fautes de frappe dans la version allemande : il faut lire « Gesundheitsfachperson » au lieu de « Gesundheitsfachpersonen » au ch. 9.2.1.1 et « Zugriffsrechte » au lieu de « Zugriffsrechten » au ch. 9.2.1.5.

9.3 Accessibilité

VAKA, *K3* et *VZK* observent que la notion d'accessibilité au ch. 9.3.1.1 fait référence aux personnes ayant un handicap et non aux personnes âgées. Ils suggèrent de remplacer aussi la désignation « patients handicapés » (« behinderte Patientinnen und Patienten ») par « personnes ayant un handicap » (« Menschen mit Behinderung ») dans la version allemande. Ils proposent concrètement de biffer les termes « âgés ou ayant un handicap » de cette disposition. Six cantons[148] renvoient pour le ch. 9.3 à leurs prises de position sur le sujet au ch. 3. *SBV* réitère pour le ch. 9.3.1.2 sa prise de position sur le ch. 3.3.1.2. *VGIch* fait valoir qu'il faut régler les grandes lignes de l'exigence dès le stade de l'ordonnance, sans attendre l'ODEP-DFI. On contrevient ici au principe de légalité.

9.4 Formats de fichiers : mise à disposition

Six cantons[149] renvoient pour le ch. 9.4 à leurs prises de position sur le sujet au ch. 4. *ZH, K3, VZK ZAD* font valoir que les dispositions du ch. 9.4 découlent déjà de celles de la LDEP et de l'ODEP ou qu'elles vont de soi et qu'on peut dès lors les supprimer. *K3*, *VZK*, *ZH* et ZG réitèrent pour le ch. 9.4 leur prise de position sur le ch. 3.4, tandis que *K3* et *VZK* renvoient, pour le ch. 9.4.1.2, à leur commentaire relatif au ch. 3.4.1.2. *La Poste* observe que l'ODEP-DFI définit l'annexe 4 comme sa source pour les formats des fichiers tandis que les CTO se réfèrent à l'annexe 3 (métadonnées), ce qui nécessite une mise au point. Il n'est d'ailleurs pas question que l'ordonnance rabaisse le dossier électronique du patient au rang d'un convertisseur de documents. Convertir des documents au format PDF ne pose plus de problème aujourd'hui à l'utilisateur ni aux systèmes primaires. *La Poste* est d'avis qu'aucune conversion de documents ne devrait être requise et demande de supprimer cette exigence.

9.5 Formats de fichiers : requête

ZH, *K3*, *VZK* et *ZAD* réitèrent ici la position déjà prise au sujet du ch. 9.4. Six cantons[150] renvoient pour le ch. 9.5 à leurs prises de position sur le sujet au ch. 5. *BFH* demande pourquoi le portail d'accès doit offrir la fonction de téléchargement vers un système primaire, puisque les professionnels de la santé disposent de leur propre accès. Il faut envisager de supprimer le ch. 9.5.1.2. *SCH* rappelle à propos de ce chiffre que le patient ne dispose pas d'un système primaire. *Medgate* se demande également ce qu'un « système primaire » vient faire ici et suppose qu'il s'agit là d'une erreur à corriger. *La Poste* ne

146 FR, NE, GE, VS, VD, JU
147 FR, BL, CDS, GL, LU, OW, UR, SBC, NW, SZ, TG, VGIch
148 FR, NE, GE, VS, VD, JU
149 FR, NE, GE, VS, VD, JU
150 FR, NE, GE, VS, VD, JU

voit pas la raison d'être de la disposition au ch. 9.5.1.3. La manière dont fonctionnent les interfaces au sein des communautés est hors de propos de la LDEP et les solutions utilisées entre communautés sont de type XCA (ou XCF). Une telle exigence n'aurait de sens que si l'on entreprenait aussi de normaliser la façon d'effectuer un « bulk download ». *La Poste* demande que cette disposition soit supprimée. Elle rappelle par ailleurs que les « rate limits » et « use cases » doivent être définis en détail pour éviter des discussions interminables. On souhaite là aussi la suppression de cette exigence.

9.6 Données historisées (let. c)

ZH, *K3*, *VZK* et *ZAD* réitèrent ici les positions déjà prises au sujet des ch. 9.4. et 9.5. *BFH* demande ce que l'on entend par « forme lisible » et propose un autre terme comme variante : « […] consulter, sous forme d'un contenu clair qu'ils puissent aisément suivre et comprendre, les données historisées de toutes les communautés […] ». Chez privatim, on regrette que cette formulation ne dise pas dans quelle mesure un patient peut établir un aperçu global de toutes les données historisées des communautés et des communautés de référence. Ce serait pourtant important pour assurer un contrôle efficace. Il faudra examiner s'il est possible de préciser l'énoncé en ce sens.

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

10.1 Stockage des documents de patients

10.1.1/10.1.2 : *HIN* part de l'hypothèse qu'au ch. 10.1.1, le mot « spéciaux » utilisé pour désigner les lieux de stockage internes ne veut pas dire « physiquement séparés ». Une séparation logique suffit amplement. On propose de compléter l'énoncé comme suit : « […] lieux de stockage internes spéciaux logiquement séparés des lieux de stockage de documents pour professionnels de la santé et institutions de santé […] ». La *CCM*, *BüAeV*, *GAeSO*, *KAeG* et *SG* estiment que le lieu de stockage de documents saisis par le patient lui-même doit absolument être tenu séparé du lieu de stockage de documents pour professionnels de la santé et institutions de santé afin que l'on puisse d'emblée distinguer clairement les documents sur la base du lieu de stockage et garantir la sécurité du traitement. Ils demandent comme *HIN* que le ch. 10.1.1 soit complété en ce sens : « […] lieux de stockage internes spéciaux séparés des lieux de stockage de documents pour professionnels de la santé et institutions de santé […] ». *KSSG* fait remarquer qu'une séparation de ces référentiels de données (repositories) entre les documents établis par le patient et ceux établis par les professionnels de la santé double les frais de maintenance, de licence et d'exploitation d'un référentiel de données. Une séparation peut aussi s'effectuer au niveau logique. D'où leur demande de supprimer le ch. 10.1.1. Six cantons[151] trouvent imparfaite la traduction française du ch. 10.1.1 et demandent que son énoncé soit corrigé en « […] des lieux de stockage dédiés […] ». Ces cantons demandent en outre que le ch. 10.1.2 soit adapté comme suit : « […] à aucun effacement ». *OFAC* demande à propos du ch. 10.1.2 pourquoi des données non consultées depuis plus de 10 ans ne seraient pas soumises aux mêmes règles que celles visées au ch. 2.1.1.1. La conservation abusive expose à des risques inutiles et enfreint le principe de proportionnalité de la LPD.

10.1.3/10.1.4 : Au sujet du ch. 10.1.3, *BFH* relève que deux giga-octets représentent beaucoup d'espace de stockage pour des documents texte, mais bien moins pour la saisie des données vitales et plus rien du tout s'il s'agit de télécharger des images. En fait de 2 Go, l'espace de stockage couramment mis à disposition aujourd'hui se situe plutôt vers 10 Go, si bien qu'il faudrait plutôt parler d'un espace de stockage correspondant aux conditions usuelles du marché, mais au minimum de 10 Go. *PharmaSuisse* est d'avis qu'un espace de stockage de 2 Go est insuffisant et recommande de l'augmenter à 5 Go au moins, comme le proposent la plupart des services Cloud gratuits. De l'avis de 17 participants[152], la taille de 2 Go exigée pour l'espace de stockage est purement arbitraire et cette disposition peut donc être supprimée. Il serait préférable d'inclure dans l'ODEP une disposition générale et abstraite qui préciserait que le dossier électronique du patient doit offrir suffisamment d'espace de stockage pour que

[151] FR, NE, GE, VS, VD, JU
[152] CDS, BL, GL, LU, OW, UR, ZG, ZH, SZ, TG, AR, NW, K3, VZK, SSIM, FMH, ZAD

les patients puissent y enregistrer tous leurs documents importants. Six cantons[153] observent qu'une capacité de stockage de 2 Go est loin de couvrir les besoins de certains patients et demandent par conséquent de reformuler ainsi le ch. 10.1.3 : « Les communautés doivent garantir et s'organiser pour fournir un espace de stockage correspondant au besoin ». Ils demandent aussi la suppression du ch. 10.1.4.

10.2 Archivage hors ligne des documents et des métadonnées

La Poste et *VAKA* font valoir que les règles de réimportation de documents, qui ne semblent pas constituer un véritable « use case », engageront pourtant des frais relativement importants parce que la technologie nécessaire, qui de surcroît n'est pas encore disponible, sera sans doute très coûteuse. Ils demandent la suppression pure et simple du ch. 10.2. *OFAC* demande entre autres à quoi serviront ces dispositions et si ce sera gratuit. Elle se demande si l'on ne s'exposera pas à des risques inutiles si un patient mal sensibilisé archive ses données hors ligne sur un cloud proposé sur le marché.

La Poste fait valoir que l'exigence d'interopérabilité suppose que l'on spécifie aussi les formats à utiliser. Le ch. 10.2.1 doit être supprimé ou complété des spécifications nécessaires. *BFH* demande si le terme de « données concernant les patients » désigne seulement les données administratives ou si les données concernant le traitement médical en font également partie. Il rappelle que le législateur n'a encore spécifié aucun format interopérable, du moins si l'on suppose que le terme d'« interopérabilité » ne vise pas le format PDF. Il convient donc de préciser de quelles « données concernant les patients » il est question ici. *Economiesuisse* et *SBC* proposent que le ch. 10.2.1 s'applique à toutes les données du patient, et pas seulement aux données saisies par le patient qui font l'objet du ch. 10. Au besoin, le titre du ch. 10 devra être modifié comme suit : « […] enregistrées par les patients et les professionnels de la santé ». *HIN* déclare tenir pour acquis, par analogie au ch. 3.4.1.2, que l'exigence visée au ch. 10.2.1 est largement remplie si le système empêche d'emblée le paramétrage des formats non acceptés.

SCH relève que l'ordonnance ne prescrit pas de formats ni de transactions spécifiques et laisse de ce fait une grande liberté d'action à des implémentations propriétaires, ce qui peut nécessiter l'engagement de frais impossibles à estimer à ce stade pour garantir un processus d'importation cohérent. IHE définit déjà dans le cadre technique (ITI-32 Portable Media Creator et Importer) les acteurs, les transactions, ainsi que les formats d'importation et d'exportation des données et documents depuis le registry et les référentiels de données (repositories) dans les communautés conformes IHE. Cette spécification se réfère aux « use cases » correspondants du domaine DICOM et renvoie pour les points essentiels au standard DICOM. La spécification IHE décrit déjà aussi le calcul des valeurs de hachage des données et documents pour en sécuriser l'intégrité et l'état original. *SCH* demande que les trois points du ch. 10.2 soient remaniés en deux chiffres ci-après : « 10.2.1 Les communautés doivent offrir aux patients la possibilité d'exporter ou d'importer les données et documents de leur dossier électronique du patient dans un format électronique interopérable selon la norme IHE ITI-32 ; 10.2.2 Les communautés de référence doivent garantir au moyen des procédés définis dans la norme IHE ITI-32 que les données destinées à être remises à disposition dans le dossier électronique du patient resteront inchangées. ».

K3 et *VZK* objectent que les exigences des ch. 10.2.2 et 10.2.3 sont pratiquement impossibles à remplir dans leur intégralité, vu que les patients ont toute liberté pour télécharger leurs documents, les effacer ou les renvoyer dans l'espace de stockage après modification. Il convient dès lors de supprimer ces deux chiffres. Toujours à propos de ces mêmes chiffres, six cantons[154] observent qu'à moins de disposer d'un système qui génère un historique complet pour chaque document, il sera impossible de déterminer si des données ont été modifiées. Ils souhaitent également la suppression des ch. 10.2.2 et 10.2.3. *Integic* appelle à préciser les points du ch. 10.2 car ils prêtent actuellement à confusion. Selon les résultats de l'imagerie (DICOM), par exemple, la disposition au ch. 10.2.3 en particulier pourrait éventuellement poser problème. En effet, l'archivage hors ligne doit toujours se rapporter à l'intégralité du dossier. Lorsqu'un participant quitte une communauté, cela ne devrait pas inquiéter le patient. Au

[153] FR, NE, GE, VS, VD, JU
[154] FR, NE, GE, VS, VD, JU

besoin, la communauté de référence reprendra les données qui y sont archivées. *KSSG* regrette qu'une telle vérification ne puisse pas être effectuée sur les profils IHE existants. Lorsqu'un document est enregistré à nouveau, un nouvel ID unique de document est généré et enregistré avec lui. La duplication d'un document (vérification du hachage, etc.) n'est pas une fonctionnalité IHE. *KSSG* demande la suppression du ch. 10.2.3. *OFAC* s'interroge sur la signification de ce « mises à disposition une nouvelle fois dans le dossier électronique du patient ».

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

La *CCM*, *BüAeV*, *GAeSO* et *KAeG SG* saluent la mise en place d'un service-desk pour les patients. Cependant, aucune règle n'a encore été instaurée qui définisse qui doit assumer les frais de ce service. Cette lacune doit être comblée. Le service d'assistance destiné aux professionnels de la santé ne devrait pas leur occasionner de frais supplémentaires, vu que l'introduction du dossier électronique du patient leur coûte déjà très cher. *VGIch* déclare à propos du ch. 11.1.1 que l'historisation est soumise aux mêmes règles que pour les services d'assistance pour professionnels de la santé. Or, on constate ici des lacunes dans l'ordonnance ou des imprécisions dans le rapport explicatif. La cohérence de ces dispositions doit être garantie. Tous les utilisateurs doivent consigner leurs accès dans un journal. *VGIch* tient par ailleurs à préciser que l'obligation de garder le secret médical est une disposition du Code pénal dont on ne saurait faire une « obligation analogue » telle qu'évoquée au ch. 11.1.2.2. *VGIch* demande en outre la correction suivante dans le texte allemand du ch. 11.1.2.4 : « […] Einwilligung der jeweiligen Patienten erfolgen können […] ». *Medgate* rapporte la même erreur et demande qu'on la corrige comme suit : « […] Einwilligung der jeweiligen Patientin oder des jeweiligen Patienten erfolgen können […] ». Chez *privatim*, on comprend mal pourquoi un professionnel de la santé doit donner son accord à des accès à distance depuis les terminaux du patient. L'accord du patient devrait amplement suffire à ce genre d'accès. *BFH* demande pourquoi il faut informer un professionnel de la santé de l'existence d'un accès à distance à des fins d'assistance et pourquoi l'on ne devrait pas également en avertir au moins le patient. Le rôle d'assistant (« supporter ») devrait également figurer dans les métadonnées.

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

OFAC déclare au sujet du ch. 12.1.1 qu'un dossier électronique du patient ne doit être supprimé qu'en cas de révocation du consentement ou de décès. En cas de non-utilisation, on n'efface que les documents, mais non pas le dossier électronique du patient, ni le NIP, ni non plus les données saisies par le patient qui ne sont pas assujetties à un délai d'effacement visé par les dispositions du ch. 10.1.2.

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

K3 et *VZK* observent que la réglementation énoncée au ch. 12.2 figure déjà dans l'ODEP et qu'elle n'a donc pas lieu d'être ici. *ZH* et *ZAD* font la même remarque pour le ch. 12.2, dont ils demandent également la suppression. Six cantons[155] réitèrent leur prise de position relative à l'art. 20 ODEP et demandent la suppression du ch. 12.2.1.2. *SBC* demande à propos du ch. 12.2.1.3 si le processus se déclenche aussi quand le patient fait don de ses données à la recherche ou qu'il les transmet à ses héritiers. Sur ce même sujet, *economiesuisse* est d'avis que les données de patients décédés devraient pouvoir être exportées pour servir par ex. à la recherche médicale, mais qu'il faut pour cela le consentement du patient (par une disposition anticipée) ou de ses survivants. La *SSIM* fait valoir qu'un dossier électronique du patient ne peut être supprimé immédiatement après un décès, car un accès à ces données pourrait éventuellement être nécessaire pour des raisons médico-légales. La *SSIM* propose que l'on ne puisse procéder à sa suppression qu'au terme d'un délai d'attente, par ex. de 360 jours.

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

K3, *VZK*, *ZH* et *ZAD* réitèrent pour le ch. 12.3 leurs prises de position sur le ch. 12.2. *K3* et *VZK* ajoutent

[155] FR, NE, GE, VS, VD, JU

que la suppression du dossier électronique du patient ne saurait relever uniquement de la responsabilité des communautés de référence, mais nécessite que l'on définisse des règles dans l'espace de confiance du dossier électronique du patient. Six cantons[156] estiment qu'en cas de suppression du dossier électronique du patient en application de l'art. 20 ODEP, ces données ne doivent pas être supprimées immédiatement, mais doivent être masquées et rendues inaccessibles. Leur suppression effective interviendra au bout de 10 ans. Le ch. 12.3 doit être adapté en conséquence et suivi d'un chiffre supplémentaire intitulé « Masquage du dossier électronique du patient ». *USB* est pour que l'on examine si la suppression ne devrait pas intervenir qu'après une période transitoire. Il est en outre souhaitable que le sens des termes de suppression/destruction/effacement soit précisé et au besoin expliqué pour tous les textes d'ordonnance. D'après *VGIch*, l'idée et le but de l'obligation d'informer toutes les communautés en vertu du ch. 12.3.1.4 restent obscurs. La CdC pourrait par exemple être chargée d'informer – éventuellement sur un mode automatique – les autres communautés si nécessaire. En outre, une révocation devrait toujours être valable avec effet immédiat. Il s'agit également de définir comment interpréter la notion de délai approprié visée à l'art. 20 ODEP. Cette notion est répétée dans les Critères techniques et organisationnels. Or, leur rôle est de décrire les critères techniques et organisationnels de certification et non d'interpréter l'ordonnance. *VGIch* conseille de fixer un délai (par ex. d'un mois) dans l'ODEP. *SBC* demande qui informera toutes les communautés et communautés de référence. *KSSG* pose la question des modalités d'une telle suppression dans toutes les communautés affiliées et préconise la création d'une information technique et donc automatisée à cet effet. Il propose d'élaborer un profil IHE correspondant.

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

Six cantons[157] déplorent que le processus de révocation par le patient lui-même au travers du portail patient ne soit pas décrit au ch. 12.4.1 Ils souhaitent que cette description soit ajoutée au texte. *La Poste* relève à propos du ch. 12.4.1.2 que la révocation peut aussi se faire par voie électronique et demande comment il faut s'y prendre. Elle demande que la disposition soit adaptée à cette fin. À propos du ch. 12.4.2.1.2, *La Poste* demande également si un patient doit se présenter personnellement pour faire supprimer son dossier électronique du patient lorsqu'il ne peut plus utiliser son MID. Là aussi, la disposition doit être adaptée. Une révocation écrite doit suffire.

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

Six cantons[158] renvoient à leur commentaire sur l'art. 20 ODEP et demandent la suppression du ch. 12.5. *SBC* demande à qui revient le rôle de détecter les inutilisations visées au ch. 12.5.1. *VGIch* se prononce pour que le ch. 12.5.1.1 soit complété comme suit : « le patient est clairement informé de la suppression […] ».

3.2.3 Art. 3 Métadonnées (annexe 3)

Art. 3 Métadonnées
Les métadonnées visées à l'art. 9, al. 3, let. b, ODEP figurent à l'annexe 3.

Art. 3 : Six cantons[159] demandent quel est le lien avec la liste des métadonnées établie par eHealth-Suisse en collaboration avec les cantons. Ils donnent comme exemple la liste des documents classés selon les codes LOINC. Ils souhaitent la réintroduction de la liste LOINC, déjà traduite, qui est utilisée par les cantons depuis plusieurs années et harmonisée avec les pratiques internationales.

Annexe 3

1.1 Rôle de l'auteur : *BFH* est d'avis que si le code 40999 « Other » (Autres) est un « fourre-tout » pratique, il importe tout de même de bien réfléchir au rôle joué par les administrateurs système, les

[156] FR, NE, GE, VS, VD, JU
[157] FR, NE, GE, VS, VD, JU
[158] FR, NE, GE, VS, VD, JU
[159] FR, NE, GE, VS, VD, JU

collaborateurs de l'assistance utilisateurs ou d'autres prestataires appelés peut-être à ouvrir un jour des dossiers hors d'un parcours thérapeutique concret pour permettre à des concitoyens d'y enregistrer des données sur leur style de vie ou des documents plus anciens. *ChiroSuisse* signale une erreur dans la désignation allemande du code national 40003 et demande qu'elle soit reformulée en « Chiropraktor » (et non « Chiropraktiker »). L'*ASI*, *SWOR* et *FSAS* trouvent un peu court que l'on se serve du terme générique « Therapeutin/Therapeut » (« Other Therapist ») (code national 40011) pour désigner différentes professions. Les noms des professions doivent être mentionnés dans leur intégralité. Selon la *FMH*, la traduction allemande de « Social Worker » (code national 40010) est fausse. Ils demandent que l'on reprenne la désignation professionnelle correcte de « Sozialarbeiter FH ». Par ailleurs, le terme de « Complementary therapist » (code national 40006) ne désigne pas les médecins pratiquant la médecine complémentaire. Il faut utiliser les dénominations professionnelles reconnues en Suisse par l'OrTra-MA et l'OrTra-TC. *BS* demande si le « Case Manager » (homme ou femme) est compris dans les « Social Workers » (code national 40010). Les métadonnées devraient indiquer de quel domaine de la santé le ou la « Case Manager » fait partie. *ZH* et *pharmaSuisse* s'accordent à dire que le rôle de « Pharmacist » (code national 40001) doit être subdivisé en « Retail pharmacist » et en « Hospital pharmacist » conformément aux codes 50045/50046 du ch. 1.2, vu que ces deux professions sont clairement distinctes.

1.2 Discipline médicale de l'auteur : *KSSG* signale l'omission de la discipline « Oncologie », à rajouter dans le tableau. La radio-oncologie n'est pas la même chose. *HÄ CH* et *ÄTG* critiquent le caractère trop différencié de cette classification, qui comprend six options possibles rien que pour le personnel soignant. Ils demandent qu'elle soit simplifiée. *SMCF* fait valoir que la liste des disciplines médicales devrait se fonder sur l'annexe 1 de l'ordonnance sur les professions médicales (OPMéd) et qu'il faut lui ajouter celle de « médecin praticien ». *PharmaSuisse* signale que le terme anglais « Pharmacologist » (code national : 50040) signifie littéralement « pharmacologue ». Or il existe des médecins pharmacologues et des pharmaciens pharmacologues. Si ce code doit être réservé exclusivement aux médecins, il est recommandé de modifier la désignation anglaise par exemple en « Medical Pharmacologist ». De plus, les désignations actuelles des codes 50045 et 50046 doivent être modifiées en « Retail pharmacist FPH » (pharmacien FPH en pharmacie d'officine) et en « Hospital pharmacist FPH » (pharmacien FPH en pharmacie hospitalière), respectivement. Il est en outre recommandé d'ajouter à la liste les professions de « Clinical Pharmacist FPH » (pharmacien FPH en pharmacie clinique) et « Pharmaceutical administrative assistant » (assistant-e de gestion en pharmacie). *BS* signale que certains termes anglais (par exemple « Allergist ») sont inusités dans cette langue et propose que les désignations de ces disciplines soient dûment revues et corrigées. Une autre discipline absente de cette liste est la médecine de laboratoire ; il convient donc d'examiner s'il ne faut pas y inclure le titre de « Specialist for laboratory medicine » (« spécialiste FMH en médecine de laboratoire »). Une autre question qui se pose est de savoir si les formations infirmières spécialisées (« Specialized nurse », code national 50065) ne devraient pas être spécifiées plus en détail et si la profession d'infirmière spécialisée ne devrait pas constituer une discipline en soi. L'*ASI*, *SWOR* et *FSAS* demandent une formulation neutre des disciplines médicales qui s'abstienne de toute combinaison savante entre le nom de la profession et celui de la spécialité (p. ex. rôle : médecin, spécialité : gynécologie). Ils souhaitent en outre que les noms des professions infirmières (codes nationaux 50062 à 50068) soient mentionnés sous ce rôle.

1.3 Statut de disponibilité du document : *BINT* et *Integic* regrettent qu'aucun renseignement n'ait été inscrit dans les documents sur leur cycle de vie ni sur les corrections apportées au dossier électronique du patient. De telles indications seraient pourtant souhaitables. *ZH* souhaite voir compléter les classes supplémentaires « Patient Medication » pour les e-documents de l'e-médication et de la « Vaccination Information » pour les données du dossier électronique de vaccination. Pour ce qui est du statut de disponibilité du document, *BS* fait valoir que le terme de « deprecated » est très inusité et incompris des non-initiés. Le contraire d'« approved » est « denied ». Il convient donc d'examiner si l'on ne peut pas utiliser un terme plus compréhensible. *VGIch* précise qu'il faut assurer une gestion des versions pour chaque document et que l'on parle de documents « valides » ou « annulés ». Par ailleurs, il est dit que selon les métadonnées, un document peut présenter un état de disponibilité « autorisé » ou « refusé ».

VGIch propose d'expliquer et au besoin d'unifier cette terminologie pour assurer une meilleure compréhension.

1.4 Classification du document : KSSG fait savoir qu'on utilise à nouveau des codes nationaux, contrairement à ce qui a été publié jusqu'ici. La classe de document doit être rattachée à une norme internationale (ISO 13606). De l'avis de *LUKS*, les différenciations (par ex. 70006 et 70010) ne sont pas clairement désignées. On demande un guide de l'utilisateur rédigé indépendamment du droit d'exécution. *BINT* et *Integic* attirent l'attention sur la nécessité d'attribuer les constellations/intersections possibles en fonction des classes/types de documents, qui devront être complétés et restructurés. À propos des classes de documents, *HÄ CH* et *ÄTG* sont d'avis que les documents et formats d'échange en relation avec l'e-médication, l'e-vaccination et eTOC (transition des soins), actuellement en phase de développement, doivent être intégrés dans cette liste et adaptés au fur et à mesure aux progrès de l'implémentation. *PharmaSuisse* recommande de compléter les classes de « Patient Medication » pour les e-documents de l'e-médication et de « Vaccination Information » pour les données du dossier électronique des vaccinations. La *FMH* suggère que les classes 70001 et 70002 peuvent être regroupées en une seule : 70007/2 « Progress Notes ». De plus, la délimitation entre 70009 et 70013 n'est pas claire. Au besoin, ces classes pourraient également être regroupées sous la désignation commune « Avertissements/alertes ». *BFH* demande si le plan de médication (60005) tombe dans la classe 70012. Quelques explications seraient utiles ici, tout comme l'on pourrait envisager de mettre à jour la liste des documents CDA présents dans le biotope du dossier électronique du patient et de mentionner à quelle classe/quel type (ch. 1.12) ces documents sont attribués.

1.5 Niveau de confidentialité : *SQS* observe que la classe désignée sous le code 30002 devrait avoir un niveau de confidentialité énoncé en termes équivalents en anglais et en allemand, ce qui n'est pas le cas actuellement. À propos du niveau de confidentialité du code 30005, *BS* fait remarquer que le terme « secret » utilisé en anglais (et en français) veut dire « Geheimnis » en allemand et qu'il vaudrait peut-être mieux utiliser le terme « protected data ».

1.6 Format du document : Sept participants[160] se demandent si la liste est complète. Il n'est guère concevable que le dossier électronique du patient ne contienne que ces trois types de documents. Ils demandent que le système prenne en charge au moins les formats d'échange officiels. Pour un résultat de laboratoire dans le cadre d'une procédure de transplantation, celui-ci serait par ex. urn:che:epd:2.16.756.5.30.1.1.1.1.3.4.1. Par ailleurs, ces participants demandent que l'OFSP continue d'entretenir la liste des types de documents sans qu'il faille édicter une nouvelle ordonnance. Les formats d'échange pour le plan de médication ou le rapport de sortie sont déjà prévus et il s'agit maintenant de les faire intégrer rapidement dans le texte de l'ordonnance. *IG eHealth* et *La Poste* font remarquer qu'en français, le terme « format du document » se réfère à la forme du document et non à son contenu. Cette signification du mot « format » a été particulièrement utilisée dans l'annexe 6, §3 (indicateurs) et au ch. 2.2.1.3 des CTO. Les deux intervenants demandent que l'on utilise une terminologie appropriée (par ex. format d'échange) et qu'une fois cette terminologie définie, l'on s'y tienne systématiquement dans tous les textes. *HÄ CH* et *ÄTG* demandent à propos du format des documents si l'on ne devrait pas y intégrer aussi les documents relatifs à l'e-médication et à l'eTOC. La *SSIM* et *LUKS* proposent d'y intégrer encore d'autres types de documents (par ex. les résultats de laboratoire d'une procédure de transplantation).

1.7 Type de l'institution de santé : *Medgate* déplore le manque de clarté dans l'attribution des prestataires de télémédecine et demande que l'on crée un code pour les institutions de télémédecine. *PharmaSuisse* recommande la traduction allemande « Öffentliche Apotheke » pour le code 20009 « Pharmacy ». *BS* est d'avis que le qualificatif anglais « private » pour le code 20004 « private home-based care » suggère une forme précise de financement et ne devrait donc pas figurer dans ce contexte. Il souhaite que l'on se contente de « home-based care ». Par ailleurs, le terme de « nursing home » (code 20008) désigne un établissement médico-social. Il serait souhaitable d'examiner si la désignation française ne pourrait pas trouver une traduction plus fidèle en anglais. *SCH* propose l'adoption du nouvel

[160] IG eHealth, KSSG, medshare, Integic, HL7, IHE, BINT

OID national de « Télémédecine ». La *FMH* fait les suggestions suivantes : code 20001 : dresser une liste systématique des centres de diagnostic, ou alors utiliser le terme général « diagnostische Institute » (centres de diagnostic) ; code 20002 : à traduire par « Notfallstation » (service d'urgences) ; code 20004 : la désignation est « Spitex » ; code 20010 : préciser si médical/non médical ; code 20012 : mauvaise traduction allemande.

1.8 Langue du document : *HÄ CH* et *ÄTG* rappellent que les cabinets des médecins de famille reçoivent régulièrement des documents des pays d'origine de leurs patients, par ex. de Turquie, et qu'il faudrait que la liste comporte au moins un groupe supplémentaire intitulé « Other » (autres). *HL7*, *IHE* et *BINT* font valoir que l'on devrait également admettre les codes « de », « fr », « it » (sans –CH) et « en » (sans –US). Il est conseillé d'omettre les extensions de pays ou au moins d'admettre les codes de langue sans ces extensions. *IG eHealth* et *La Poste* déconseillent de présenter cette liste comme exhaustive, car cela pourrait poser des problèmes pratiques. Ils demandent comment procéder lorsqu'un patient souhaite télécharger un document dans une autre langue. La liste peut se définir comme un exemple ou comme un relevé de spécifications minimales. La liste suivante est utilisée dans le secteur de la santé : Référence à l'OID 1.0.639.1[161]. *La Poste* ajoute à ce propos que tous les codes de langue ISO devraient être admis.

1.9 MIME Type du document : Quatorze participants[162] signalent que la liste contient des doublons et, partant, des données redondantes qu'il s'agit d'épurer. *HL7*, *IHE*, *medshare* et *Integic* soulignent la nécessité de préciser sous « application/pdf » que le format requis est PDF/A. Ils renvoient à ce sujet aux directives des Archives fédérales[163] et de l'ELGA[164] et précisent que tous les fichiers PDF incorporés dans des documents CDA de l'ELGA-doivent répondre à la norme PDF/A-1a (selon « ISO 19005-1:2005 Level A conformance ») *IG eHealth* et *La Poste* qualifient la liste des formats de documents de très restrictive, et signalent même qu'il y manque plusieurs formats pourtant d'usage courant (par ex. PNG). De plus, la définition des formats est très imprécise. Le format TIFF est pris en charge, sans toutefois que l'on sache de quelle extension TIFF il s'agit. Ils demandent que les formats de documents admis soient spécifiés sous forme d'une liste d'exigences minimales. *ZH* plaide pour que l'on complète la liste des formats admis. *BFH* demande pourquoi seul le niveau CDA 1 est pris en compte. Dans ses commentaires, *USB* mentionne notamment le format de données STL et demande l'admission de ce type de document dans le tableau MIME.

1.10 Discipline médicale des données saisies dans le document : *KSSG* réitère ici sa prise de position relative au ch. 1.2 « Discipline médicale de l'auteur ». *ChiroSuisse* signale une erreur dans la désignation anglaise du code 10007 et demande son remplacement par « Chiropractic ». *PharmaSuisse* et *ZH* recommandent d'ajouter « Pharmacotherapy » (pharmacothérapie) et « Patient Care » (soins aux malades chroniques) à la liste des disciplines médicales. La *SSIM*, *LUKS* et la *FMH* font valoir qu'en combinant la discipline médicale et le type de document, on obtient davantage de degrés de liberté et une meilleure représentation de l'intégrité référentielle. Les ch. 1.10 et 1.12 doivent être remaniés dans cette optique.

1.11 Sexe du patient : *PharmaSuisse* est d'avis que l'indication du sexe du patient n'est pas nécessaire pour chercher et trouver un document et qu'il n'y a donc pas besoin de faire figurer ce renseignement dans les métadonnées, sans parler du risque d'utilisation abusive d'une telle fonction de recherche. Cette association propose dès lors de supprimer le ch. 1.11.

1.12 Type du document : *GE*, *VD*, *VS*, *JU* et *FR* réitèrent ici leur prise de position relative à l'art. 3 ODEP-DFI. *BFH*, *BINT* et *Integic* renvoient à leurs commentaires sur le ch. 1.4 et la *SSIM*, la *FMH* et *LUKS* réitèrent ici leur prise de position relative au ch. 1.10. KSSG fait savoir qu'on utilise à nouveau

[161] http://www.hl7.org/oid/index.cfm?Comp_OID=1.0.639.1
[162] BFH, HIN, HL7, IHE, medshare, Integic, K3, VZK, PharmaSuisse, ZH, SQS, LUKS, SSIM, FMH
[163] https://www.bar.admin.ch/bar/de/home/archivierung/ablieferung/digitale-unterlagen.html
[164] https://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/CDA/Implementierungsleitfaden_2.06.1/HL7_Implementation_Guide_for_CDA_R2_-_Allgemeiner_Implementierungsleitfaden_fuer_ELGA_CDA_Dokumente_V2.06.1.pdf

des codes nationaux, contrairement à ce qui a été publié jusqu'ici. La classe de document doit être rattachée aux codes internationaux LOINC. Rappelant sa prise de position sur l'art. 4/annexe 4, *PharmaSuisse* recommande d'ajouter les types de documents suivants à la liste des formats admis : Rapport d'e-dispensation/d'utilisation (Dispensation Record), Commentaire sur l'e-médication (eMedication comment) et Résultats de laboratoire (Laboratory data). *La Poste* rapporte que selon la recommandation d'eHealth Suisse, chaque type de document doit être attribué à une seule classe de documents, mais malheureusement cette attribution est libre (pas de consigne ni de recommandation). Dès lors, si chaque communauté, voire chaque professionnel de la santé entreprenait d'attribuer les documents selon ses propres critères, il en résulterait des incohérences au niveau des échanges intra- ou intercommunautaires. *La Poste* demande par conséquent des consignes prescrivant comment attribuer un type de document à une classe de documents précise. *STSAG* critique le fait que le terme allemand « Kurve » au code 60037 n'est pas une bonne traduction de l'anglais « Progress Note » et propose de la remplacer par « Verlaufsbericht Intensivstation » (rapport d'évolution en unité de soins intensifs). *BS* propose la nouvelle désignation anglaise « Electronic prescription » pour le code 60006. *BS* signale encore que l'expression anglaise correspondant au code 60027 est erronée. Histologie se dit « histology » et les examens histologiques ne s'effectuent pas tous sur une biopsie. La cytologie ne figure nulle part et doit encore être ajoutée.

3.2.4 Art. 4 Formats d'échange (annexe 4)

Art. 4 Formats d'échange
Les formats d'échange visés à l'art. 9, al. 3, let. c, ODEP figurent à l'annexe 4.

Art. 4 : *BRH* rappelle que les formats d'échange de fichiers médicaux contiennent les données qui constituent le véritable enjeu du dossier électronique du patient et sont au centre du processus d'échange de données médicales. Aux termes du rapport explicatif, ces formats devraient être élaborés dans le contexte des processus multi-acteurs et ne font donc pas partie du droit d'exécution. Cet organisme propose que l'on définisse les formats d'échange (tout au moins le data set minimal) au début de l'ODEP-DFI. La *SSIM* constate que l'on ne dispose pas encore des formats d'échange, ceux-ci étant en cours d'élaboration dans des processus multi-acteurs selon l'OFSP. Elle demande l'intégration la plus rapide possible de ces multi-acteurs pour permettre la mise en place d'un processus efficace et efficient qui donne des résultats durables. *PharmaSuisse* regrette que l'annexe 4 n'existe pas encore et souligne que les formats d'échange servent à l'échange d'informations entre les professionnels de la santé. Plus les professionnels de la santé disposeront d'informations, mieux ils pourront optimiser le traitement d'un patient, ce qui augmente la sécurité des patients. L'association salue vivement le fait que le patient contrôle exclusivement le paramétrage des droits d'accès, qui définit les documents qu'un professionnel de la santé peut consulter et grâce auquel tous les professionnels de la santé, quel que soit leur groupe, disposent en principe de toutes les informations dont ils ont besoin. Elle salue également le fait que l'annexe 4 sera élaborée dans le cadre de processus multi-acteurs et qu'elle pourra figurer dans le droit d'exécution à la faveur des révisions futures. L'annexe 4 doit être rédigée le plus rapidement possible et devra correspondre aux délibérations du groupe de travail interprofessionnel (IPAG). *HL7* et *IHE* relèvent que seuls quatre formats d'échange ont été définis et que les objets d'information ont ici une influence décisive. À l'instar de *Bleuer*, ces organismes annoncent qu'avec les résultats du diagnostic par imagerie, les « use case » suivants seront courants dans un avenir proche : les images, les rapports d'examen, etc. seront remis au patient sur CD/DVD avec un afficheur (viewer). Certains de ces viewers sont des systèmes propriétaires, ce qui signifie que même des données au format DICOM ne sont pas compatibles avec tous les viewers. Il faut par conséquent se réserver la possibilité d'enregistrer des CD/DVD contenant des images, des rapports d'examens, etc. dans le dossier électronique du patient avec les viewers compatibles, par ex. sous forme de fichiers ZIP. Le format ZIP doit aussi être soutenu parce qu'il est admis dans DICOM (pour les détails, v. DICOM PS3.12). L'*AMDHS* regrette que la consultation sur l'ODEP mais aussi sur l'ODEP-DFI ait lieu avant que l'on se soit concerté sur les formats d'échange. Étant donné que ces formats ne sont même pas vraiment traités dans le projet soumis, il est demandé aux milieux médicaux d'avaliser ces ordonnances en l'état, ce qui revient quasiment à « acheter » cette pièce maîtresse « les yeux fermés ». L'*AMDHS* connaît fort bien ce « cas de figure interprofessionnel » pour se l'être fait présenter lors de la consultation interne menée par la FMH, mais s'étonne vivement du degré de détail des formats d'échanges prévus. Au lieu de se limiter à ce qui est nécessaire

et utile, ces recommandations prescrivent qu'en plus de la partie médicale, tous les professionnels de la santé participant à la chaîne de traitement apportent au dossier électronique du patient des historiques médicaux complets ayant pour thèmes les problèmes, l'anamnèse, les traitements et l'évolution de l'état du patient. Cette démarche est irréaliste et inadaptée à son objet. Elle fait perdre de vue l'essentiel et contribue à la création d'immenses cimetières de données que l'OFSP, bien que légalement mandaté pour le faire, ne pourra pas évaluer parce que trop peu de patients voudront avoir un dossier électronique.

3.2.5 Art. 5 Profil d'intégration (annexe 5)

Art. 5	Profils d'intégration
L'annexe 5 définit, en application de l'art. 9, al. 3, let. d et e, ODEP:	
a.	les profils d'intégration;
b.	les adaptations nationales des profils d'intégration;
c.	les profils d'intégration nationaux.

Art. 5 : *NE* se rallie ici au commentaire de *FR* relatif à l'art. 1, ODEP-DFI. *H+* salue la décision du DFI de faire appel à des normes techniques internationalement reconnues et bien établies en Suisse. Il importe que les communautés et les communautés de référence ne soient pas privées par leur statut juridique de la possibilité de coopérer avec les plateformes existantes d'échanges de données du eGouvernement.

Annexe 5a

GE, *VS*, *VD*, *JU* et *FR* se déclarent incompétents pour commenter cette annexe et estiment qu'elle doit être validée par IHE Suisse. *OFAC* fait confiance à IHE Suisse pour ce qui est de la standardisation et de la documentation des profils d'intégration. Il en va de même pour *KSSG* qui se fie à la prise de position d'IHE Suisse et HL7. *SG* renvoie à l'examen fait par IHE Suisse et HL7 et ajoute qu'il manque des profils d'intégration définissant la suppression au-delà des communautés. *LUKS* estime qu'il importe que le droit d'exécution de la LDEP évolue au rythme du progrès technique. Il convient notamment de prendre en compte et d'admettre les futures évolutions du standard HL7 FIHR. IHE Suisse et HL7 doivent être intégrés dans la suite du processus d'évaluation et de remaniement. *IG eHealth* et *La Poste* sont d'avis qu'en l'état, cette prescription est dénuée de sens. Les profils IHE définis sont prévus en partie pour l'utilisation au sein d'un domaine d'affinité et en partie pour l'action intercommunautaire. Le législateur a déterminé que la présente loi s'appliquait au domaine intercommunautaire. Il est donc inutile de vouloir définir des profils exclusivement prévus pour un usage au sein des domaines d'affinité. D'ailleurs, on n'est pas au clair sur la manière d'interpréter cette liste de profils. Ces profils doivent-ils être pris en charge par tous les systèmes qui veulent participer à la communauté ? En d'autres termes, est-il interdit d'intégrer une solution qui transmet des messages HL7 par File Transfer ? Ces prescriptions pourraient être confiées à un examen par des auditeurs, ce qui occasionne des frais qu'il vaut mieux éviter. *IG eHealth* et *La Poste* proposent une formulation spécifique qui distingue entre les profils MUST (impératif) et SHOULD (souhaitable) *Integic* dit à propos de « 1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption » : RESTful-ATNA est un nouveau « Supplement for Trial Implementation » qu'il faudrait intégrer (Add RESTful Query to ATNA - Published 2015-08-07)[165]. Outre la solution proposée qui utilise National Extention, une autre solution est d'ailleurs disponible avec IHE RESTful-ATNA. La *SSIM* et *SBC* pensent que les fournisseurs de composants informatiques devraient la faire homologuer. En outre, l'enregistrement de systèmes informatiques devrait être totalement séparé de la certification des communautés. Cela permettrait de faire des économies significatives lors de la certification des communautés individuelles, étant donné que les composants techniques seront déjà enregistrés ; on aurait ainsi une répartition claire des attributions entre les fournisseurs de composants informatiques et la communauté ; il y aurait un marché public pour les composants techniques ; le processus d'approvisionnement des communautés pourrait être simplifié et il y aurait un support pour une infrastructure « best of breed » qui ne représenterait pas un écosystème fermé d'un fournisseur ; on

[165] http://wiki.ihe.net/index.php/ATNA_Repository_RESTful_Access
http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

attendrait dès lors une stimulation de la part de l'industrie. La *SSIM* et *SBC* proposent que la certification d'une communauté faisant intervenir des composants homologués puisse se faire sans répéter toute la procédure d'enregistrement de l'infrastructure technique, la communauté pouvant se contenter de faire certifier les processus organisationnels et les mesures de protection des données. La *SSIM* ajoute que les demandes d'IHE Suisse sont supportées. *HIN* trouve très utiles l'aperçu et le tableau descriptif succinct, tandis que *medshare* salue vivement la voie choisie des profils d'intégration. La *FMH* demande par contre la suppression de cette disposition, étant opposée à la réglementation à l'échelon de l'ordonnance.

Annexe 5b

1.1 Definitions of terms

La Poste et *IG eHealth* observent à propos du ch. 1.1 :

1.1.1 : - La formulation anglaise « may » est contraire à l'obligation de documenter des professionnels de la santé et il faut lui préférer la formulation suivante : « Healthcare professionals must save this data ».
- À propos de l'élément de phrase « must join a certified community » : The emphasis seems incorrect. Not only must the join a certified community. Such HP must ensure that they are certifiable themselves. De faux espoirs peuvent engendrer des problèmes massifs. Demande : Clarify the formulation and make sure that the proper emphasis is made.
- À propos de l'élément de phrase « view their data » : The emphasis could be improved. Demande : Instead of "their data" you should write "their own data".

1.1.2 : - Why is this called community portal index? The index lists many more informations apart from the portals. Community service index would be more appropriate since this service will provide information on all the services the community provides to third parties. Demande : change the terminology.
- À propos de la figure 1 : Why is this called "Unique person identification"? Clarify terminology

1.1.3 : - The term "base community" was introduced (and translated to Stammgemeinschaft) already 3 or 4 years ago. It is unclear, why the term reference community is now used. Question: why is the term reference chosen? What does the community reference to? Clarify terminology.

1.1.4 : - CCO is the only institution which is allowed to correlate the Social Security Number (AVN13) with the electronic patient dossier-PID. This statement is unclear. The community must provide the AHVN13 to the ZAS (EPDV Art 5.2.e). When this happens the community is able to correlate the two identifiers. Further: there are cantonal laws that allow the use of the AHVN13 for patient matching. Demande : delete this statement or clarify the statement so that it complies with the laws. Cette mise au point a une répercussion directe sur la mise en œuvre.
- À propos de l'élément de phrase « the gateways may correlate » : Why is it not must? Some transactions like patient discovery mandate the use of the electronic patient dossier-PID as the only identifier. Demande : remplacer « may » par « must ». L'omission de changer ce terme pourrait créer des problèmes de compatibilité.

HIN déclare à propos de l'élément de phrase « Primary Systems may correlate their local patient identifier with the MPI-PID » que le terme « Primary Systems » désigne sans doute les systèmes primaires des institutions de santé. Si cette hypothèse est juste : au ch. 2.11.1 de l'annexe 2 (CTO), il est dit notamment que le NIP n'est pas directement et durablement associé aux documents du patient dans les systèmes primaires. Cet énoncé des CTO et les présentes déclarations dénotent des contradictions qui doivent être résolues. En outre, le terme « HIS » n'est pas défini. Il faut lire probablement « Hospital Information System ». Ce terme doit être ajouté au glossaire.

1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption

BINT et *medshare* rappellent qu'à part la solution proposée par National Extention, une autre solution est disponible : IHE RESTful-ATNA. RESTful-ATNA est un nouveau « Supplement for Trial Implemen-

tation » qu'il faut intégrer. On indique d'ailleurs un lien Wiki[166] dans ce contexte. Tandis que *BINT* renvoie à un document du 07.08.2015[167] relatif à RESTful-ATNA, *medshare* se réfère à un document portant la date du 27.05.2016[168]. *La Poste* ajoute à ce propos : The underlying concept seems to be to expose ATNA logs to end users. This concept has been tried in Austria and it has later been changed to support a more human interpretable event log. Since this has already been proven to be a less than ideal solution this should be replaced with a two tiered approach of ATNA logs for legal purposes and some higher abstraction level of event logging for end users.

1.4.2 : *Integic* fait remarquer que l'acteur IHE Document Consumer n'interagit pas avec Audit Record Repository en interrogation, mais seulement en écriture pour la transaction Record Audit Event (ITI-20). Un Audit Record Repository n'est pas un composant acteur qui prend en charge XDS-b. Le workflow sous la forme décrite n'est pas conforme IHE. Une précision ou une exécution de ces résolutions est vivement recommandée, vu qu'une ITI-18 et une ITI-43 subséquente du Doc Consumer à l'ARR ne correspondraient pas aux profils IHE mentionnés. *HL7* et *IHE* déclarent : Registry Stored Query [ITI-18] transaction that uses the parameters described in chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10. Retrieve Document Set [ITI-43] transaction performed against an Audit Record Repository using a document UUID received by a previously executed by a Registry Stored Query mentioned before. Ils en demandent la suppression. *La Poste* et *IG eHealth* consignent les déclarations suivantes à propos du ch. 1.4.2 :
- „Combine all Audit Trail Message entries of all Audit Trail Document entries into one single document of type ATNA Audit Trail Document Format (see chapter 1.4.4.2 on page 23)". This will not scale. The number of audit messages is strictly increasing over time. At a minimum the sorting has to be "newest-first" and the number of returned records should be capped to a reasonable small number. Otherwise the coordinating server, which is in charge of aggregating the result, has increasingly high and non-deterministic memory requirements. Ideally the service should support server-side pagination and server-side search.
- Translate the coded information into the language preferred by the user when provide it to the user through the UI or other results like reports. What is the purpose of this requirement? The average patient will hardly be able to interpret the contents of the ATNA audit log. In Austria the ATNA log is kept separate from a user compatible event log. The ATNA log is required for legal purposes. The event log is used to make events understandable.
IG eHealth ajoute en outre le point suivant : The specifications in EPDV and its appendices seem to prohibit on demand documents as very specific document formats are defined and explicit storage seems to be required. Add the ATNA Document Type to the list of permitted types. En ce qui concerne le ch. 1.4.2.2, *Integic* relève que seul l'acteur Secure Application est mentionné. Ce sont surtout les communautés/fusions de Registry et de Repository qu'il faut clairement exécuter en tant que Secure Node, ou dont il faut compléter l'acteur. *HL7* et *IHE* demandent que le passage « These actors […] ATNA Audit Repositories » au ch. 1.4.2.3 soit reformulé : „If the parameter $XDSDocumentEntryTypeCode contains the value 60049 (Audit trail), the responding gateway must return an UUID for a subsequent retrieval of an On Demand Document returning the audit messages matched by the filter parameters in the query of the corresponding document UUID in the 1.4.4.1 ATNA Audit Message Format. See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10". Ils ajoutent à propos du ch. 1.4.2.4.1 qu'il n'y a pas besoin de prescrire comment réaliser un audit interne à la communauté. Ainsi, il est possible d'utiliser aussi IHE RESTful ATNA à cette fin. Pour ce qui est du ch. 1.4.2.5, ils demandent en outre la suppression du premier, du troisième et du quatrième des quatre points énumérés dans le texte.

1.4.3 : *Integic* signale que ITI-57 ne peut modifier que ConfidentialityCode, ce qui pose question pour la création de plusieurs versions. L'annulation d'un document enregistré dans le dossier électronique du patient et inscrit au Document Registry dans le contexte de l'illustration des cycles de vie de documents (voir ITI-41 RPLC) devrait être autorisée. *IG eHealth* et *La Poste* demandent la correction suivante au

[166] http://wiki.ihe.net/index.php/ATNA_Repository_RESTful_Access
[167] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf
[168] http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA_Rev2.0_PC_ 2016-05-27.pdf

ch. 1.4.3.2 : instead of UUID this should read documentUniqueId. Ils ajoutent à propos du ch. 1.4.3.1.2 : „Cache all audit messages“, this paragraph implies several drawbacks:
- Caching implies that an updated version of the document is not available for another 8 hours. If a user notices that after a log view, subsequent actions (even his own) are no longer presented, he may think that logging is flawed.
- To force a particular implementation makes no sense. It is preferable to specify what the response must contain and maybe allow the option to cache this information for up to 8 hours. The implementation details should be left to the platform.
The method chosen (On demand document) to implement this feature can be discussed. Alternatives would be: - XCF, - Delayed Document Assembly. Improve the requirement for a more sustainable solution. Avoid to limit the freedom of the implementation and standardize the relevant aspect of the interfaces

1.4.4 : En ce qui concerne l'AuditMessage/ActiveParticipant, *Integic* recommande d'introduire non seulement l'UserID, mais aussi un nom lisible de la personne intervenant en tant que 1.1 mandatory Element afin de rendre l'historisation plus facile à suivre pour le patient. *HIN* constate que le GLN au ch. 1.4.4.1.1 est défini comme « MUST » (impératif). Or, le texte de l'ordonnance (art. 24 ODEP) dit « peut transmettre », ce qui en ferait un élément optionnel. Cela paraît contradictoire. Il y a des cas où le GLN n'est pas encore défini. HIN propose de faire du GLN un « MUST » partout. Cela signifie qu'avant de pouvoir entrer dans une communauté, un cabinet médical doit d'abord obtenir un numéro GLN. *La Poste* et *IG eHealth* font l'observation suivante à propos du ch. 1.4.4.1 : Why should the implementer be forced to persist an audit event in any particular format? A canonical format is only relevant for audit message exchange across communities. As long as the implementer can generate and populate the exchange format he should be free to store the data in whatever format deemed most practical. Demande : Remove MUST requirement to store audit event data in a pre-defined format. Ils ajoutent cette réflexion à propos du ch. 1.4.4.1.1 : Which time zone is used in a timestamps string representation is completely irrelevant as long as the time zone is included in the string representation so downstream processes interpret it correctly. Demande : remove the Swiss national extension.

1.5 Requirements on PIXv3 for Patient Identity Feed

La Poste et *IG eHealth* déclarent à propos de OtherIDs : From the documents of EPDV storing the electronic patient dossier-PID in the MPI is a MUST requirement. Why is it a MAY requirement here? Correct the requirement.

1.7 Requirements on PDQv3 Profile for Patient Demographics Query

La Poste et *IG eHealth* ont une incertitude à propos du ch. 1.7.2.1.1 : If there are more than 5 matches zero matches a special handling like in the XCPD transaction (see IHE ITI TF-2b, chapter 3.55.4.2.2.6) is necessary. Clarify this statement

1.8 Requirements on XCPD Profile for Cross-Community Patient Discovery

Dans leur prise de position, *La Poste* et *IG eHealth* prennent l'exemple d'un cas et demandent comment le résoudre. Ils formulent aussi la revendication suivante : An example for patient matching across communities should be provided. Ils ajoutent à propos du ch. 1.8.2 : As the header is a suggestion by the initiating gateway to the responding gateway, i.e. the responding gateway may do whatever, why is there a hard limit of the value that can be recommended? To restrict a non-binding value seems pointless. Remove “This values MUST NOT exceed 3 days”.

1.9 Requirements on HPD Profile for Replication

HIN réitère pour les ch. 1.9.5.1.1 et 1.9.5.1.2 sa prise de position sur le ch. 1.4.4.1.1.

Annexe 5c

1 Introduction

KSSG demande à propos de la mise en œuvre de XDS-I si le service DICOM WADO fait également partie de la certification. Celui-ci serait un élément des systèmes primaires si seul le KOF était enregistré au Repository XDS. Une autre question qui l'intéresse est si les portails d'accès patient doivent supporter un afficheur DICOM compatible avec WADO (acteur Imaging Document Consumer) et si c'est pertinent ou non pour la certification. Le domaine XDS-I pour l'échange d'images a été entièrement ignoré dans les CTO, d'où la nécessité de revoir l'ODEP et les CTO à l'aune des exigences d'IHE XDS-I. À propos de la phrase « It has been specified for the Document Registries to act as Policy Enforcing Service Providers in terms of a XACML PEP », *La Poste* et *IG eHealth* déclarent : Where has this been specified? How do we deal with the situation that someone, who knows all the identifiers relevant to a document can retrieve this document with the REG PEP intercepting this transaction? Example: A primary system that was authorized in the past, stored this information. It can access the document even after the authorization expired.
Ils sont par ailleurs d'avis que de telles consignes réduisent singulièrement les possibilités pour divers fournisseurs d'implémenter leurs propres solutions. *IG eHealth* demande : Do not specify HOW something must be implemented. Specify the desired result instead.

2 Volume 1 – Integration Profiles

IG eHealth et *La Poste* observent à propos du ch. 2.2 :
- Signature: An X.509 signature by a trusted entity (XUA Assertion Provider) to guaranty the confidentiality of the claims being made and unaltered content of the assertion." A digital signature does not provide confidentiality. implying wrong expectation must be avoided. Demande : Remove "confidentiality of the claims being made and".

- Subject: The custodian attribute has to be present in addition to the GLN/ electronic patient dossier-ID. Authorization decisions can only be made for GLN/ electronic patient dossier-IDs because those are the entities that are being authorized by patients. The custodian acts in the name of either one of those entities. In other words, the custodian has an existence dependency to a GLN or electronic patient dossier-ID. Demande : Be more specific about which attributes co-exist on a subject.

- Attribute Statement: organization & organization-id: Carrying organization text and ID attributes for patients makes little sense. Resource-id = electronic patient dossier-PID: This assumes that there will never be any cross-patient use cases. This appears to be not very future proof. Demande : Do not require org text and org ID attributes for patients. Drop electronic patient dossier-PID as resource attribute.

Integic estime que la durée de validité de 10 minutes est beaucoup trop courte pour un cabinet médical. Le délai d'attente doit être relevé à 30 à 60 minutes. *La Poste* et *IG eHealth* relèvent le point suivant concernant le ch. 2.3.2 : XACML 3.0 was published in Jan. 2013. is there a reason to use an outdated version? It should keep up with current standards.

3 Volume 2 – Transactions

IG eHealth et *La Poste* apportent la remarque suivante au sujet du ch. 3.1.10 : „urn:e-health-suisse:2015:error:not-holder-of-patient-policies" is to be set as the result of an "Indeterminate" PDP response. But the PDP will also return this decision value if there was an error during rule evaluation. The two cannot be distinguished based on the XACML response unless one has control over the PDP's workings. Which one normally does not have as it is part of a XACML library. Cela a des effets directs sur l'implémentation et les performances. Demande : Drop the attribute. Leur prise de position pour le ch. 3.1.5 est la suivante : The list should include document access via the repository. Repository access is mentioned towards the end of the document, but really should be mentioned as an event that requires authorization in its own right. Ce qui a aussi des effets directs sur l'implémentation et les performances. Demande : Add trigger event "RetrieveDocumentSetRequest". *Integic* signale à propos du ch. 3.1.6.1

que « ADR due to XDS Register Document Set-b » devrait être le ch. 3.1.6.2. *IG eHealth* et *La Poste* font la remarque suivante au sujet du ch. 3.1.6.1 : The approach of "bulk querying the PDP" does not scale for large responses, neither in terms of memory usage nor runtime. This approach requires the PEP to un-marshal the complete registry response into memory, then determine the document subsets and place requests for the subsets. The response can only be forwarded after all PDP responses are received, lest the document order seen by the client is not guaranteed to be the same as generated by the registry. The PEP must be able to operate on the registry response stream in order to scale. The bulk request approach also does not scale if other document attributes become part of the access decision. The number of combinations to bulk-query for grows exponentially with the number of attributes and their values. The paragraph should be seen as an implementation example for small result sets. But as the size of the result is unknown, unless fully un-marshaled into memory, it is rather useless from an implementation perspective. Another example based on response stream filtering should be added. *Medshare* observe à propos du ch. 3.3 que le format d'échange technique pour la Policy échangée contre CH:PPQ n'est pas mentionné et doit être spécifié. Concernant le ch. 3.3.9, *Integic* propose que l'on remplace « ACMLPolicyQuery Response » par « XACMLPolicyQuery Response ».

3.2.6 Art. 6 Évaluation (annexe 6)

Art. 6	Evaluation
Conformément à l'art. 21, al. 2, ODEP, les communautés et les communautés de ré-férence sont tenues de mettre les données mentionnées à l'annexe 6 à la disposition de l'OFSP pour l'évaluation.	

Art. 6 : Six participants[169] demandent que cet article soit complété par la consigne que les communautés ne doivent fournir ces données à l'OFSP que sous une forme anonymisée. Il découle des données mentionnées à l'annexe 6 que cela suffit pour procéder aux évaluations prévues. Ils demandent donc l'ajout d'un nouvel alinéa 2 : « Les communautés et les communautés de référence sont tenues d'anonymiser ou de faire anonymiser les données avant de les fournir à l'OFSP ». *GE*, *VS*, *VD* et *JU* demandent que l'on précise les indicateurs exigés : – période considérée – globalement ou par patient, – fréquence, – fréquence moyenne, – fréquence médiane, – chiffres absolus, etc. L'établissement de ces indicateurs engendrera des coûts pour les communautés, coûts qui devraient être couverts par la Confédération car c'est elle qui exige ces indicateurs. Il conviendra de compléter ce texte en indiquant le cadre financier. *HL7*, *IHE* et *medshare* demandent que l'on fixe une périodicité et des délais. *HIN* plaide pour que les exigences relatives au reporting restent réalisables. En particulier, le reporting doit se faire sur demande et non par défaut. L'art. 6 doit donc être complété comme suit : « Les communautés et les communautés de référence sont tenues de fournir sur demande à l'OFSP […] ». La *SSIM* demande que les données, respectivement les indicateurs relatifs aux données de base, droits d'accès, fichiers, utilisation et protection des données soient restreints à un strict minimum et ne puissent servir de manière abusive à contrôler les prestataires de services. *Santésuisse* déclare qu'en vue de l'évaluation visée à l'art. 1, al. 3, LDEP, ni la loi ni l'ordonnance ni encore le rapport explicatif n'ont fourni la moindre indication sur le but de l'évaluation, les moyens de l'atteindre et la manière dont elle doit être concrétisée. Les indicateurs mentionnés à l'annexe 6 ne sauraient en aucun cas satisfaire aux exigences d'une évaluation du dossier électronique du patient quant à l'amélioration à apporter à la qualité du traitement médical, aux processus du traitement, à la sécurité du patient, etc.

Annexe 6

1. Données de base : *OFAC*écrit qu'il appartient aux hôpitaux et autres institutions concernées par les art. 39 et 49a, LAMal de déclarer leur date d'affiliation, probablement auprès de l'OFSP. Cette information n'a pas sa place dans un indicateur d'évaluation. *HIN* fait remarquer que dans certains cas, la combinaison entre l'âge, le sexe et le domicile ne pourra pas être rendue suffisamment anonyme. L'anonymat des patients doit cependant être garanti. *HIN* propose de reformuler comme suit le second indicateur : « […] selon l'âge, le sexe et le domicile ; un regroupement qui reste à définir doit être appliqué aux groupes de moins de sept membres ». Il demande aussi que l'on précise ce que l'on entend exactement par domicile. *La Poste* fait valoir que l'indicateur contenant la répartition selon l'âge, le sexe et

[169] KDSBSON, DSBAG, privatim, FR, BE, ZG

le domicile figure dans les indicateurs des ch. 1 et 2. Il faut corriger cette erreur et supprimer l'indicateur à un endroit.

2. Droits d'accès : *HIN* et *La Poste* réitèrent leur prise de position à propos du ch. 1. La SSIM et la *FMH* sont d'avis que les droits d'accès n'ont pas de pertinence et sont disproportionnés pour une évaluation. La *SSIM* demande qu'ils soient revus et corrigés. De l'avis de *STSAG*, le nombre et le genre de fichiers par niveau de confidentialité à l'échelon du DFI ne sont pas pertinents et ne sauraient correspondre à une évaluation appropriée des indicateurs. Ces informations sont très peu concluantes et n'augmentent que dans une mesure douteuse la marge de manœuvre. Il faut s'abstenir de collecter des données inutiles et d'augmenter inutilement le nombre des professionnels de la santé affiliés. Cet indicateur doit donc être supprimé. *LUKS* rappelle que les droits d'accès relèvent de la souveraineté décisionnelle des patients. L'ampleur dans laquelle les patients restreignent ou étendent ces droits d'accès n'intervient pas dans l'évaluation. Le patient peut retrouver dans le portail du dossier électronique s'il y a eu un accès en urgence et par qui. Le ch. 2 doit être revu en conséquence. *KSSG* observe que le relevé de tels indicateurs semble être une opération relativement complexe, vu que le ch. 4.14.1.9 des CTO interdit l'enregistrement de données relatives au patient dans l'ATNA, les fichiers log, etc.

3. Fichiers : De l'avis de *LUKS*, le nombre de documents paramétrés ne donne aucun indice de l'utilité du dossier électronique du patient. La *SSIM* et la *FMH* considèrent comme non pertinent et disproportionné le nombre de fichiers destinés à l'évaluation, tandis que *STSAG* atteste que le nombre de fichiers paramétrés en fonction de leur format n'apporte aucune information. *LUKS*, la *SSIM*, la *FMH* et *STSAG* demandent que cet indicateur soit supprimé. *La Poste* attire l'attention sur le fait que le terme de format est réservé à un autre usage et que le terme approprié ici selon l'annexe 3, §1.6, est « Mime Type ».

4. Utilisation : La *FMH*, la *SSIM* et *LUKS* sont d'avis que ces données ne sont pas pertinentes pour l'évaluation et soupçonnent plutôt une intention de contrôle dans ce relevé, raison pour laquelle ils demandent la suppression de cet indicateur. *KSSG* signale que les indicateurs relatifs à l'utilisation ne pourront être fournis qu'en partie, car quelques-uns de ces attributs ne font pas partie des métadonnées. *HIN* prend note de l'introduction des termes « classe de fichiers » et « type de fichier ». Il est présumé que « classe de fichiers » désigne la classe de documents (annexe 3, chap. 1.4) et que « type de fichier » se réfère à « MIME Type du document » (annexe 3, chap. 1.9). Si ce n'était pas le cas, il conviendrait de clarifier cela dans le texte. *La Poste* critique le fait que pour les indicateurs, les notions de « classe de fichiers » et « genre de fichiers » ne soient pas définies et elle demande qu'une définition soit encore fournie ou alors il conviendra d'utiliser les notions apparemment correctes de « classe de documents » et « type de documents » telles qu'elles ressortent de l'annexe 3. Quant à la statistique des suppressions de données, *La Poste* déclare qu'il n'y a pas de possibilité pour le patient de supprimer un document. Le patient peut modifier le niveau de confidentialité. L'article doit donc être supprimé. En outre, *La Poste* signale à propos du dernier indicateur figurant au ch. 4, qu'il convient de définir un nombre par patient. Elle demande quelles données doivent être présentées (NIP, nom, prénom, etc.) ou ce qui doit être anonymisé. Les points peu clairs devront être précisés ou supprimés. De l'avis de *STSAG* il n'y a pas lieu d'enquêter sur le nombre de professionnels de la santé. D'abord, son utilité est dérisoire et, ensuite, pour les établissements plus ou moins grands, sa portée manque de pertinence. Une enquête effectuée par la communauté de référence suffit amplement. Par ailleurs, la classe de fichiers et le type de fichier n'apportent guère d'informations, si bien qu'il convient de les supprimer dans ce contexte. Un listing des accès dans un déroulement chronologique est un processus très long et inutile pour les informations qu'il apporte. Là aussi, une enquête effectuée par la communauté de référence est suffisante. Il en va de même pour les accès des patients (déroulement chronologique, classes de fichiers et type de fichier)

5. Protection des données : *SG* demande ce qu'il faut considérer comme réclamation et souhaite que l'on définisse exactement ce terme.

3.2.7 Art. 7 Exigences minimales applicables au personnel (annexe 7)

Art. 7	Exigences minimales applicables au personnel
Conformément à l'art. 27, al. 4, ODEP, les exigences minimales applicables à la qua-lification du personnel qui réalise les	

certifications sont définies à l'annexe 7.

Art. 7 : La *SSIM* relève que les exigences applicables à la qualification du personnel réalisant les certifications sont très élevées. *SQS* réitère ici sa prise de position relative à l'art. 27, al. 4, ODEP, et demande la suppression pure et simple de l'art. 7.

Annexe 7

SQS observe à propos du ch. 1.1.1 que les critères techniques et organisationnels que doivent remplir les communautés de référence et les communautés ne contiennent a priori pas d'éléments qui requièrent des connaissances spécifiques d'informatique médicale propres à garantir une vérification dans les règles de l'art dans le cadre d'une certification. Ensuite, d'après le rapport explicatif relatif à la LDEP, les critères de compétences applicables à un organisme de certification devraient se fonder sur des principes et des procédés bien étayés sur le plan international. Au cas où l'on opte pour une certification selon les règles de l'OCPD, les exigences minimales du personnel des organismes de certification doivent être déterminées par les dispositions de l'annexe de l'OCPD réglant les exigences minimales applicables à la qualification du personnel des organismes de certification. D'ailleurs, les compétences du personnel sont réglées par la norme ISO/IEC 27006 (pour une certification ISO 27001) ou ISO 17021. *SQS* ajoute à propos du ch. 1.1.5 que la norme ISO/IEC 27006 n'est pertinente que si l'on doit procéder à une certification ISO/IEC 27001. Dans ce cas aussi, les exigences applicables à la qualification du personnel de l'organisme de certification sont données par l'accréditation. Il convient de supprimer purement et simplement les ch. 1.1.1 et 1.1.5. Au sujet des ch. 1.1.1, 1.1.2, 1.1.3, 2.1.1, 2.1.2 et 2.1.3, *HIN* estime qu'en l'absence de formation spécifique, il vaut mieux exiger cinq ans (au lieu de deux ans) d'expérience professionnelle. Deux ans d'expérience suffisent s'ils sont combinés à une formation professionnelle complémentaire. Par ailleurs, d'après *HIN*, il semble que le nombre concret des années d'expérience professionnelle demandées dans les branches en question (informatique médicale, protection des données), soit deux ans d'expérience professionnelle ou une année de formation, se situe à la limite inférieure. De toute évidence, il faut du personnel ayant davantage d'expérience pour assumer des tâches aussi importantes que les certifications dans les domaines sensibles, telles que les données des patients. *HIN* salue néanmoins le choix d'exiger que les éditeurs de MID et les communautés soient certifiés. Pour la *SSIM*, la *FMH* et *LUKS*, les exigences applicables à la qualification du personnel des organismes de certification sont trop élevées, ce qui limitera la concurrence et fera exploser les coûts. Pour autant, ces exigences extrêmes ne devraient pas produire d'améliorations significatives de la sécurité des données dans la pratique quotidienne. L'expérience montre que la sécurité des données dépend davantage du comportement des utilisateurs que des mesures techniques de protection. *Lovis* déclare qu'il faudra en assurer la fiabilité et la responsabilité. *OFAC* signale que le ch. 1.1.2 conduit à une incohérence juridique. Les communautés opérées par les cantons seront, en tant qu'organes cantonaux, soumises au droit de leur canton en matière de protection des données. Des disparités importantes existent : ainsi, aucun canton ne prévoit dans son propre droit de la protection des données la mise en œuvre d'un SGPD (Système de Gestion de la Protection des Données), en contradiction avec la LPD, l'OLPD et la doctrine du PFPDT sur l'autorégulation. Aucun canton ne prévoit, dans son propre droit de la protection des données, de procédure de certification. *OFAC*déclare en outre qu'elle n'est pas directement concernée par cette annexe et elle souhaite que les exigences applicables aux organismes de certification ne divergent pas de celles qui sont déjà en vigueur et gérées par le SAS.

3.2.8 Art. 8 Protection des moyens d'identification (annexe 8)

Art. 8 Protection des moyens d'identification
Conformément à l'art. 30, al. 2, ODEP, les prescriptions relatives à la protection des moyens d'identification sont définies à l'annexe 8.

Art. 8 : *IG eHealth* déclare qu'il convient d'accorder une haute priorité à la simplicité et à la clarté de l'application pour les patients, car si cette dernière est très complexe, elle risque de constituer un obstacle majeur à l'accès au dossier électronique du patient. C'est pourquoi, en sus des exigences relatives à la sécurité des données, il convient également de garantir la convivialité de l'application en veillant à

la simplicité des règles de base et du paramétrage. L'annexe 8 doit donc être remaniée. Pour assurer le succès du dossier électronique du patient, il importe de proposer des MID à la fois sûrs et aisés à manipuler. Comme le montre l'expérience, les smarts cards n'ont guère de chances d'être acceptées et là encore, un défi de taille devrait être relevé non seulement au niveau de la compatibilité avec l'infrastructure informatique existante, mais aussi des processus d'édition. Les systèmes tels que mTAN ou les procédés utilisant des mécanismes biométriques ou comportementaux sont donc exclus de fait. Il convient de garantir que les MID dotés d'un niveau de protection suffisant et acceptés sur le plan cantonal puissent également être utilisés dans les hôpitaux pour l'accès au dossier électronique du patient. Des investissements supplémentaires ne devraient pas être nécessaires. Partout où la loi l'autorise, on évitera d'imposer le recours à une double identification (un MID pour les accès internes des hôpitaux et un autre pour les accès aux dossiers électroniques de patients)

Annexe 8

1.2 TOE Overview

OFAC observe que LDEP a été traduit en anglais par « FLEHR », mais qu'ODEP n'a pas été traduit. Soit l'on s'en tient à la règle stricte de traduire en anglais la terminologie spécifique à la LDEP, soit l'on traduit tous les textes dans nos langues officielles. De plus, les logos et traductions de la Confédération, du DFI et de l'OFSP ne sont pas présents de manière constante dans tout le document. Logos et traductions doivent être homogènes et idéalement traduits dans la langue du document. En ce qui concerne le ch. 1.2.1, *La Poste* fait remarquer que la TOE Definition ne permet d'authentifier ni les procédés biométriques, ni les procédés comportementaux. Or, on ne pourra pas appliquer mTAN sans une adaptation appropriée. *La Poste* demande donc que l'on reprenne les définitions de la norme ISO 29115, chap. 3.3 au lieu d'introduire une définition de « device ». Elle signale en outre, au sujet du ch. 1.2.2, que le choix du terme « identification means » est impropre. Il faut parler d'« authentication means » pour les moyens d'accomplir le processus d'authentification, alors que le terme d'« identification means » désigne les moyens d'identifier une personne. Cette erreur est à corriger. En outre, le terme « holder of the token » implique que les procédés qui se passent de « token » (jeton) sont interdits de facto. Le terme de « token » doit être remplacé par celui d'« authentication factor », issu de la norme ISO 29115. D'autre part, la description du TOE indique que seuls les procédés fondés sur le NIP sont admis, ce qui soulève le problème des procédés qui n'utilisent pas de NIP. Le TOE doit être reformulé de manière à décrire à la fois la procédure d'authentification et celle faisant appel au NIP. Enfin, on note l'introduction du terme de « context ». Celui-ci n'a pourtant rien à faire dans la thématique de l'authentification. L'authentification vise à vérifier si l'identité affirmée par l'usager est correcte. La question du contexte relève plutôt de la procédure d'autorisation. Que l'éditeur du moyen d'identification ait ou non besoin de ce contexte pour sélectionner le procédé d'authentification approprié est une question « hors champ » (out of scope) pour ce document. Les références à ce contexte doivent donc être effacées ou marquées comme facultatives. *SCH* déclare au sujet du ch. 1.2.2 que les explications relatives au workflow d'authentification sont certes très détaillées, mais ne décrivent que la « IdP-Initated Approach ». Le choix du workflow préféré pour l'authentification (IdP-/RP-initiated approach) pour le dossier électronique du patient doit être laissé aux fabricants d'applications. En outre, les protocoles entre Relying Party et NIP, ainsi que les procédures d'authentification, doivent être réglés par le marché. Enfin, il serait plus simple de guider l'utilisateur en l'invitant à se rendre sur le portail du dossier électronique du patient et à s'y connecter avec ses paramètres. C'est en tout cas l'expérience faite par de nombreux utilisateurs. L'acceptation du dossier électronique du patient s'en trouve aussi améliorée. *SCH* demande que l'on supprime l'option de s'authentifier par l'IdP-initiated Workflow. Il faut se contenter de fixer les conditions et les résultats de l'authentification sans prescrire les démarches pour y parvenir. *SCH* fait en outre les propositions suivantes : Electronic identification means comprises one or more token that are secured by a device. Each token may hold a credential, that is used by the IdP to authenticate the user's identity based on possession and control of the corresponding token. An IdP-initiated or SP-initiated approach may be used.

1.5 Assets

Au sujet du tableau 1, *La Poste* signale que les descriptions sont énoncées de telle manière que seules des procédures utilisant la smart card sont possibles. Il faut les modifier pour permettre l'utilisation du mTAN ou d'autres moyens sans recours à une smart card. *La Poste* demande que l'on reprenne les définitions de la norme ISO 29115, chap. 3.3. Elle observe en outre, à propos du ch. 1.5 : - Public keys by definition are public and they need to protection. Si on comprend bien ce que la phrase est censée vouloir dire, la formulation est cependant fautive. Demande : Term to be used here is "private keys".

- The expectation in the example of "identification data" is not tenable. Using a combination of attributes to uniquely identify a user seems like a bad choice. Please note that GLN is an extremely dangerous example: GLN is unique for a person. Unfortunately in the health care system of Switzerland we have quite a number of health care providers that work in different organizations that may or may not be members of different communities. Depending on the context of the person, this person may have different users (at least one in each community). C'est une pure question de terminologie. Demande : use proper terminology. use good examples.

- Table 1: Assertion Data: SAML assertions are the only supported standard to transport claims about the authenticated identity. This is geared towards SOAP web services and not practical for HTTP based services. Faute de modification appropriée, l'intégration de nouveaux profils FHIR IHE et d'applications mobiles posera des problèmes. Demande : Support for HTTP based services should be included.

- There are several references in the document to the purpose of login to a web portal. This precludes purposes like authentication of web services, REST interfaces or mobile applications. Demande : The purpose should be formulated openly. Further references should be avoided.

- Table 1: The following description is not an "English" sentence; "The IdP stores enough information about the authentication means of the user to validate the user". The IdP must ensure that the information stored about the authentication means of the user cannot be used to recover the authentication means itself. Demande : change the formulation.

1.6 External Entities and Subjects

La Poste fait la remarque suivante à propos du tableau 2, ch. 1.6 : - The term "identification token" has not been used before. The term identification means of identification token should not be used. The purpose of this token is to be used in the authentication process and it should be called authentication means. The term means is more generic than token since a means just implies that it can be used for the purpose instead of token, which implies a physical presence.

- We are missing the HelpDesk. This role also requires privileged access to be able to support end users. The terms trusted and privileged should be aligned.

- IdP: This abbreviation is wrongly explained. Dans sa prise de position, *La Poste* cite la page Wikipedia traitant du NIP.

Elle précise que les points soulevés sont une pure question de terminologie et demande pour ces éléments : Use properly defined terms that avoid confusion.

3 Security Problem Definition

La Poste note à propos du tableau 3 : CredentialHandling: The wording is geared towards smart card use. Faute de modification appropriée, l'usage du mTAN ne sera pas possible. Elle demande que l'on reprenne les définitions de la norme ISO 29115, chap. 3.3. *SCH* dit à propos du CredentialHandling que dans le cas où l'utilisateur peut révoquer ses credentials de manière autonome, il n'a pas besoin de communiquer avec le service d'assistance du NIP. La dernière phrase du tableau 3 sous CredentialHandling doit être terminée comme suit : « […] appropriate channels or that the claimant is able to revoke/reset his device/token through appropriate means ». *SCH* souhaite aussi apporter les compléments d'explication suivants à la Policy P.Assertion : „SAMLID-Token has to comply with the specification given in section 6.3 or 6.4. The IdP information processing system shall contain a component to generate unique reference identifiers. A time restricted SAMLID-Token issued […]". Le point suivant doit en outre être précisé au sujet de P.TrustedCommunityEndpoint : "[…] as defined in section 6.3 or 6.4".

4 Security Objectives

Dans le tableau du ch. 4.1, *La Poste* fait les remarques suivantes à propos de l'O.Confidentiality : Please note that all references to public keys in the user data conflict with this requirement. Public keys are made for dissemination. C'est une pure question de terminologie. Demande : modify the definition of user data. Elle fait en outre la remarque suivante au sujet de l'O.Authentication : The explanation in the second paragraph should be aligned with ISO 29115. Ceci a son importance pour l'acceptation du mTAN. Demande : use the term "authentication factor". La Poste écrit à propos du ch. 4.2, OE.User Security Awareness: This paragraph contains references to smart card registration processes. Faute de modification appropriée, l'usage du mTAN ne sera pas possible. *La Poste* demande que l'on reprenne les définitions de la norme ISO 29115, chap. 3.3. *HIN* signale à propos du ch. 4.3.1 que la colonne « OE. SecureAreas and Equipment » n'est associée à aucune ligne. La même remarque vaut pour la ligne « A.Physical ». Ce point doit être corrigé ou complété.

5 Security Requirements

À propos du ch. 5.2.12, FCS_COP.1(1), La Poste écrit : Elliptic Curve keys are way smaller than RSA/DH/EG keys with comparable security[170]. Requiring an elliptic curve keys to be 2k in size makes no sense. Faute de modification appropriée, la sécurité va en souffrir. L'erreur se perpétuera automatiquement par le jeu des références. *La Poste* demande de ne pas définir d'algorithmes, mais de référencer les recommandations du BSI ou du NIST et ajoute : The referenced standard FIPS PUB 180-3 was superseded by FIPS PUB 180-4 in March 2012. Elle se réfère ici aux standards actuels[171].

6 Appendix

OFAC fait savoir à propos du SAML au ch. 6.4 que cette restriction technologique est inacceptable. Le SAML n'est ni universel, ni immortel. Le fonctionnement des NIP et des jetons d'identification doit être décrit en termes d'exigences de principe et non de référence trop précise, trop limitative à des technologies somme toute éphémères. *SCH* signale que les passages du présent document traitant de l'authentification font exclusivement référence au protocole SAML. Or, il existe d'autres protocoles bien établis tels que OpenID Connect, basé sur OAuth 2.0. L'interopérabilité des MID doit se restreindre aux formats des données d'identification des personnes. En outre, les protocoles entre Relying Party et NIP, ainsi que les procédures d'authentification, doivent être réglés par le marché. SCH demande par conséquent qu'en sus de la spécification SAML, on établisse également une spécification OpenID Connect/OAuth 2.0. Les ordonnances/annexes devraient en outre être aménagées de manière à pouvoir rajouter ultérieurement d'autres protocoles. Sa prise de position inclut en outre la proposition suivante : 6.5 OpenID Connect/OATH 2.0 Specification; Note: The specification will be drafted during or subsequently to appraisal.

[170] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Key_sizes
[171] http://csrc.nist.gov/publications/PubsFIPS.html

4. Annexes

4.1 Liste des participants

Cette liste, conforme au tableau 1, comprend tous les participants à l'audition du droit d'exécution de la LDEP.

Abkürzung	Kantone
AG	Staatskanzlei des Kantons Aargau Chancellerie d'Etat du canton d'Argovie Cancelleria dello Stato del Cantone di Argovia
AI	Ratskanzlei des Kantons Appenzell Innerrhoden Chancellerie d'Etat du canton d'Appenzell Rhodes-Intérieures Cancelleria dello Stato del Cantone di Appenzello Interno
AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden Chancellerie d'Etat du canton d'Appenzell Rhodes-Extérieures Cancelleria dello Stato del Cantone di Appenzello Esterno
BE	Staatskanzlei des Kantons Bern Chancellerie d'Etat du canton de Berne Cancelleria dello Stato del Cantone di Berna
BL	Landeskanzlei des Kantons Basel-Landschaft Chancellerie d'Etat du canton de Bâle-Campagne Cancelleria dello Stato del Cantone di Basilea Campagna
BS	Staatskanzlei des Kantons Basel-Stadt Chancellerie d'Etat du canton de Bâle-Ville Cancelleria dello Stato del Cantone di Basilea Città
FR	Staatskanzlei des Kantons Freiburg Chancellerie d'Etat du canton de Fribourg Cancelleria dello Stato del Cantone di Friburgo
GE	Staatskanzlei des Kantons Genf Chancellerie d'Etat du canton de Genève Cancelleria dello Stato del Cantone di Ginevra
GL	Regierungskanzlei des Kantons Glarus Chancellerie d'Etat du canton de Glaris Cancelleria dello Stato del Cantone di Glarona
GR	Standeskanzlei des Kantons Graubünden Chancellerie d'Etat du canton des Grisons Cancelleria dello Stato del Cantone dei Grigioni
JU	Staatskanzlei des Kantons Jura Chancellerie d'Etat du canton du Jura Cancelleria dello Stato del Cantone del Giura
LU	Staatskanzlei des Kantons Luzern Chancellerie d'Etat du canton de Lucerne Cancelleria dello Stato del Cantone di Lucerna
NE	Staatskanzlei des Kantons Neuenburg Chancellerie d'Etat du canton de Neuchâtel Cancelleria dello Stato del Cantone di Neuchâtel
NW	Staatskanzlei des Kantons Nidwalden Chancellerie d'Etat du canton de Nidwald Cancelleria dello Stato del Cantone di Nidvaldo

OW	Staatskanzlei des Kantons Obwalden Chancellerie d'Etat du canton d'Obwald Cancelleria dello Stato del Cantone di Obvaldo
SG	Staatskanzlei des Kantons St. Gallen Chancellerie d'Etat du canton de St-Gall Cancelleria dello Stato del Cantone di San Gallo
SH	Staatskanzlei des Kantons Schaffhausen Chancellerie d'Etat du canton de Schaffhouse Cancelleria dello Stato del Cantone di Sciaffusa
SO	Staatskanzlei des Kantons Solothurn Chancellerie d'Etat du canton de Soleure Cancelleria dello Stato del Cantone di Soletta
SZ	Staatskanzlei des Kantons Schwyz Chancellerie d'Etat du canton de Schwyz Cancelleria dello Stato del Cantone di Svitto
TG	Staatskanzlei des Kantons Thurgau Chancellerie d'Etat du canton de Thurgovie Cancelleria dello Stato del Cantone di Turgovia
TI	Staatskanzlei des Kantons Tessin Chancellerie d'Etat du canton du Tessin Cancelleria dello Stato del Cantone Ticino
UR	Standeskanzlei des Kantons Uri Chancellerie d'Etat du canton d'Uri Cancelleria dello Stato del Cantone di Uri
VD	Staatskanzlei des Kantons Waadt Chancellerie d'Etat du canton de Vaud Cancelleria dello Stato del Cantone di Vaud
VS	Staatskanzlei des Kantons Wallis Chancellerie d'Etat du canton du Valais Cancelleria dello Stato del Cantone del Vallese
ZG	Staatskanzlei des Kantons Zug Chancellerie d'Etat du canton de Zoug Cancelleria dello Stato del Cantone di Zugo
ZH	Staatskanzlei des Kantons Zürich Chancellerie d'Etat du canton de Zurich Cancelleria dello Stato del Cantone di Zurigo
Abkürzung	**Parteien**
FDP PLR PLR	FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali
SPS PSS PSS	Sozialdemokratische Partei der Schweiz Parti socialiste suisse Partito socialista svizzero
SVP UDC UDC	Schweizerische Volkspartei Union démocratique du Centre Unione democratica di Centro
Abkürzung	**Gesamtschweizerische Dachverbände der Wirtschaft**

economiesuisse	Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation
SGB	Schweizerischer Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)
SGV	Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e dei mestieri (USAM)
Abkürzung	**Übrige Organisationen**
CCC	Chaos Computer Club Schweiz
ChiroSuisse	Schweizerischen Chiropraktoren-Gesellschaft ChiroSuisse (SCG) Association suisse des chiropraticiens ChiroSuisse (ASC) Associazione svizzera dei chiropratici ChiroSuisse (ASC)
curafutura	Die innovativen Krankenversicherer Les assureurs-maladie innovants Gli assicuratori-malattia innovativi
CURAVIVA	Verband Heime und Institutionen Schweiz Association des homes et institutions sociales suisses Associazione degli istituti sociali e di cura svizzeri
FMH	Verbindung der Schweizer Ärztinnen und Ärzte (FMH) Fédération des médecins suisses Federazione dei medici svizzeri
FRC	Fédération romande des consommateurs (frc)
GELIKO	Schweizerische Gesundheitsligen-Konferenz Conférence nationale suisse les ligues de la santé Conferenza nazionale svizzera delle leghe per la salute
GDK CDS CDS	Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und Gesundheitsdirektoren (GDK) Conférence suisse des directrices et directeurs cantonaux de la santé (CDS) Conferenza svizzera delle direttrici e dei direttori cantonali della sanità (CDS)
H+	H+ Die Spitäler der Schweiz H+ Les Hôpitaux de Suisse H+ Gli Ospedali Svizzeri
HIN	Health Info Net AG
HL7	HL7 Benutzergruppe Schweiz
IG eHealth	Verein IG eHealth
IHE	IHE Suisse
ISSS	Information Security Society Switzerland
HÄ CH	Hausärzte Schweiz – Berufsverband der Haus- und Kinderärzte Médecins de famille Suisse – Association des médecins de famille et de l'enfance Suisse Medici di famiglia Svizzera – Associazione dei medici di famiglia e dell'infanzia Svizzera
OFAC	Berufsgenossenschaft der Schweizer Apotheker La cooperative professionelle des pharmaciens suisses La cooperativa professionale del farmacisti svizzeri

pharmaSuisse	Schweizerischer Apothekerverband Société suisse des pharmaciens Società svizzera dei farmacisti
PH CH	Public Health Schweiz Santé publique Suisse Salute pubblica Svizzera
Physioswiss	Schweizerischer Physiotherapie-Verband Association suisse de physiothérapie Associazione svizzera di fisioterapia
PKS	Privatkliniken Schweiz Cliniques privées suisses Cliniche private svizzere
privatim	privatim, Die schweizerischen Datenschutzbeauftragten privatim, Les préposé(e)s suisses à la protection des données privatim, Gli incaricati svizzeri della protezione dei dati
santésuisse	Verband der Schweizer Krankenversicherer Les assureurs-maladie suisses
SBK	Schweizerischer Berufsverband der Pflegefachfrauen und Pflegefachmänner (SBK) Association suisse des infirmières et infirmiers (ASI) Associazione svizzera delle infermiere e degli infermieri (ASI)
SGMI	Schweizerische Gesellschaft für Medizinische Informatik Société Suisse d'Informatique Medicale (SSIM) Società Svizzera d'Informatica Medica (SSIM)
Spitex	Spitex Verband Schweiz Association suisse des services d'aide et de soins à domicile Associazione svizzera dei servizi di assistenza e cura a domicilio
SPO	Stiftung SPO Patientenschutz (SPO) Fondation Organisation suisse des patients (OSP) Fondazione Organizzazione svizzera dei pazienti (OSP)
Stiftung refdata	Stiftung refdata Fondation refdata Fondazione refdata
SUVA	Schweizerische Unfallversicherungsanstalt (Suva) Caisse nationale suisse d'assurance en cas d'accidents Istituto nazionale svizzero di assicurazione contro gli infortuni
SVBG	Schweizerischer Verband der Berufsorganisationen im Gesundheitswesen (SVBG) Fédération suisse des associations professionnelles du domaine de la santé (FSAS) Federazione Svizzera delle Associazioni professionali Sanitari (FSAS)
SVV	Schweizerischer Versicherungsverband (SVV) Association suisse d'assurances (ASA) Associazione svizzera d'assicurazioni (ASA)
VGIch	Vereinigung Gesundheitsinformatik Schweiz
Abkürzung	**Nicht begrüsste Organisationen und Privatpersonen**
ahdis	ahdis gmbh
AHE	Altersheimverein Eigenamt
ALM	Alterszentrum Moosmatt
APP	Alters- und Pflegeheim Pfauen
ASG	Alterszentrum Schiffländi Gränichen

ASPS	Association Spitex privée Suisse
ÄTG	Ärztegesellschaft Thurgau
AZB	Alterszentrum Blumenheim
AZK	Alterszentrum Sunnmatte
AZSH	Alterszentrum Suhrhard AG
BEKAG	Ärztegesellschaft des Kantons Bern Société des médecins du canton de Berne (SMCB) Società dei medici del Cantone di Berna (SMCB)
Bethesda	Bethesda Alterszentren AG
BFG	Bündnis Freiheitliches Gesundheitswesen Entente Système de santé libéral
BFH	Berner Fachhochschule – Institute for Medical Informatics / Spitalzentrum Biel
BINT	BINT GmbH
Bleuer	Juerg P. Bleuer
BRH	Berner Reha Zentrum AG Heiligenschwendi
BüAeV	Bündner Ärzteverein BüAeV
DSBAG	Beauftragte für Öffentlichkeit und Datenschutz des Kantons Aargau
DSF	Datenschutz-Forum Schweiz
EHS	Verein eHealth Südost
FAAG	Asana Gruppe AG, Altersresidenz Falkenstein
FER	Fédération des entreprises romandes
GAeSO	Gesellschaft der Ärztinnen und Ärzte des Kantons Solothurn
GS1	GS1 Schweiz
HospizAG	Hospiz Aargau
ICTS	ICT Switzerland
Insel	Inselspital Universitätsspital Bern Hôpital universitaire de l'Ile, Berne Inselspital Ospedale universitario di Berna
Insos	Nationaler Branchenverband der Institutionen für Menschen mit Behinderung Association de branche nationale des institutions pour personnes avec handicap
Integic	Integic AG
K3	Konferenz Kantonale Krankenhausverbände
KAeG SG	Ärztegesellschaft des Kantons St. Gallen
KBAG	Klinik Barmelweid AG
KDSBSON	Datenschutzbeauftragter der Kantone Schwyz, Ob- und Nidwalden
KFSAG	Klinik für Schlafmedizin AG
KKA	Konferenz der kantonalen Ärztegesellschaften (KKA) Conférence des sociétés cantonales de médecine (CCM) Conferenza delle società mediche cantonali (CMC)
KMUF	KMU-Forum
KSOW	Kantonsspital Obwalden
KSSG	Kantonsspital St.Gallen
LEUG	Asana Gruppe AG, Spital Leuggern
Lovis	Christian Lovis
LUKS	Luzerner Kantonsspital
Medgate	Medgate AG
medshare	medshare GmbH
MENZ	Asana Gruppe AG, Spital Menziken
Moeri	Thomas Moeri
PINK	Schweizerische Schwulenorganisation PINK CROSS

Post	Post CH AG Poste CH SA Posta CH SA
PSV	Pflegeheim Sennhof AG
RCA	RehaClinic AG
RPB	Regionales Pflegezentrum Baden AG
RZPB	Reusspark Zentrum für Pflege und Betreuung
SBC	Serge Bignens Consulting
SBV	Schweizerischer Blinden- und Sehbehindertenverband Fédération Suisse des aveugle et malvoyants
SCH	Swisscom Health
SDG	Schweizerische Diabetesgesellschaft (SDG) Association suisse du diabète (ASD) Associazione svizzera per il diabete (ASD)
senesuisse	Verband wirtschaftlich unabhängiger Alters- und Pflegeeinrichtungen Association d'établissements économiquement indépendants pour personnes âgées
SMAG	Salina Medizin AG
SMCF	Société de Médecine du Canton de Fribourg
SQS	Schweizerische Vereinigung für Qualitäts- und Management Systeme (SQS) Association suisse pour systèmes de qualité et de management (SQS) Associazione svizzera per sistemi di qualità e di Management (SQS)
SteHAG	Verein der Stammgemeinschaft des Kanton Aargau
STSAG	Spital STS AG
SWICO	SWICO
SW!SS REHA	Vereinigung der Rehabilitationskliniken der Schweiz
SWOR	Swiss Orthoptics
SZW	Seniorenzentrum Wasserflue
Tessaris	Tessaris Integrated Security AG
USB	Universitätsspital Basel
VAKA	Verband Aargauische Spitäler, Kliniken und Pflegeinstitutionen
VDPS	Vereinigung der Direktoren der Psychiatrischen Kliniken und Dienste der Schweiz Association des directeurs de cliniques et hôpitaux psychiatriques en Suisse
VKZS	Vereinigung der Kantonsärzte und Kantonsärztinnen der Schweiz (VKZS) Association des médecins dentistes cantonaux de Suisse (AMDCS) Associazione dei medici dentisti cantonali della Svizzera (AMDCS)
VLSS	Verein der Leitenden Spitalärztinnen und -ärzte der Schweiz (VLSS) Association des médecins dirigeants d'hôpitaux de Suisse (AMDHS) Associazione medici dirigenti ospedalieri svizzeri (AMDOS)
VZK	Verband Zürcher Krankenhäuser
ZAD	Verein Trägerschaft ZAD

4.2 Autres abréviations et notions

Abkürzung	Titel
AHVN13	Die 13-stellige AHV-Nummer
ATP	Attributeprovider
BAG OFSP UFSP	Bundesamt für Gesundheit Office fédéral de la santé publique Ufficio federale della sanità pubblica
(D)DoS-Angriffe	(Distributed) Denial-of-Service-Angriffe
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDI DFI DFI	Eidgenössisches Departement des Innern Département fédéral de l'intérieur Dipartimento federale dell'interno
GLN	Global Location Number
HPD	Health Provider Directory
IDM	Identifikationsmittel
IDP	Identifikationsprovider
IHE	Integrating the Healthcare Enterprise
IPAG EPD	Interprofessionelle Arbeitsgruppe Elektronisches Patientendossier
ISMS	Informationssicherheits-Managementsystem
KIS	Klinikinformationssystem
LOINC	Logical Observation Identifiers Names and Codes
MedReg	Register über die universitären Medizinalberufe
MPI	Master Patient Index
PID	Patientenidentifikationsnummer
PSP	Personensicherheitsprüfung
SaaS	Software as a Service
SIEM	Security Information and Event Management System
STL	Standard Transformation Language
STS	Secure Token Service
TOZ	Technische & organisatorische Zertifizierungsvoraussetzungen
WAF	Web-Application-Firewall
WZW	wirksam, zweckmässig und wirtschaftlich
XUA	Cross-Enterprise User Authentication
ZAS	Zentrale Ausgleichsstelle

4.3 Organisations dont la prise de position est identique à celle du Verband Aargauische Spitäler, Kliniken und Pflegeinstitutionen (VAKA)

An sämtlichen Stellen dieses Berichtes, an denen die nachfolgenden Organisationen nicht explizit aufgeführt sind, entsprechen deren Stellungnahmen derjenigen der VAKA	
Abkürzung	**Name**
AHE	Altersheimverein Eigenamt
ALM	Alterszentrum Moosmatt
APP	Alters- und Pflegeheim Pfauen
ASG	Alterszentrum Schiffländi Gränichen
AZB	Alterszentrum Blumenheim
AZK	Alterszentrum Sunnmatte
AZSH	Alterszentrum Suhrhard AG
Bethesda	Bethesda Alterszentren AG
FAAG	Asana Gruppe AG, Altersresidenz Falkenstein
HospizAG	Hospiz Aargau
KBAG	Klinik Barmelweid AG
KFSAG	Klinik für Schlafmedizin AG
LEUG	Asana Gruppe AG, Spital Leuggern
MENZ	Asana Gruppe AG, Spital Menziken
PSV	Pflegeheim Sennhof AG
RCA	RehaClinic AG
RPB	Regionales Pflegezentrum Baden AG
RZPB	Reusspark Zentrum für Pflege und Betreuung
SMAG	Salina Medizin AG
SteHAG	Verein der Stammgemeinschaft des Kanton Aargau
SZW	Seniorenzentrum Wasserflue