Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP
Unità di direzione politica della sanità

Rapporto sui risultati dell'indagine

Ordinanza sulla cartella informatizzata del paziente (OCIP)

Ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI)

22 marzo 2017

Indice

1. Situazione iniziale

Il 19 giugno 2015 il Parlamento ha adottato la legge federale sulla cartella informatizzata del paziente (LCIP; RS 816.1) che entrerà in vigore nel 2017. Il 22 marzo 2016 il Dipartimento federale dell'interno (DFI) ha avviato l'indagine conoscitiva sul diritto d'esecuzione della LCIP. L'indagine conoscitiva, che si è conclusa il 29 giugno 2016, verteva su tre ordinanze: l'ordinanza sulla cartella informatizzata del paziente (OCIP), l'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI) e l'ordinanza sugli aiuti finanziari per la cartella informatizzata del paziente (OFCIP). L'OCIP disciplina i gradi di riservatezza e i diritti d'accesso (capitolo 1), le disposizioni sull'attribuzione e la gestione del numero d'identificazione del paziente (capitolo 2), le prescrizioni per le comunità e le comunità di riferimento (condizioni di certificazione; capitolo 3), gli strumenti d'identificazione (capitolo 4), l'accreditamento (capitolo 5), la certificazione (capitolo 6) e i servizi di ricerca di dati (capitolo 7). L'OCIP-DFI concretizza l'OCIP. Costituita da 9 articoli con 8 allegati, questa ordinanza disciplina esclusivamente alcuni aspetti molto tecnici della cartella informatizzata del paziente (CIP). L'OFCIP concretizza le prescrizioni degli articoli 20 - 23 LCIP, che disciplinano gli aiuti finanziari a livello di legge.

Il presente rapporto contiene esclusivamente le risposte all'indagine conoscitiva sull'OCIP e l'OCIP-DFI. I risultati dell'indagine conoscitiva sull'OFCIP sono raccolti in un rapporto separato.

2. Procedura di indagine conoscitiva e principi di valutazione

Questo capitolo contiene una tabella, che indica il numero dei pareri pervenuti dai diversi partecipanti, e illustra i principi di valutazione applicati al capitolo 3 (pareri sulle singole disposizioni dell'OCIP e dell'OCIP-DFI).

2.1 Procedura di indagine conoscitiva

Tabella 1: panoramica delle risposte pervenute

Categoria	Cantoni, CDS	Partiti	Associazioni mantello svizzere dell'economia	Altre organizzazioni	Organizzazioni non interpellate e privati	**Totale**
Numero / categoria	27	3	3	30*	74**	137

*curafutura, SVV e **VKZS hanno espressamente rinunciato a esprimere il loro parere

2.2 Principi di valutazione

Al fine di offrire un quadro generale il più completo possibile, il presente rapporto riassume e riporta con accuratezza i pareri, che sono stati numerosi e svariati nel loro contenuto. I pareri dettagliati pervenuti nell'ambito dell'indagine conoscitiva sono disponibili al seguente indirizzo:

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

I pareri relativi ai singoli articoli dei testi sono riportati nel capitolo 3.

3. Pareri sulle singole disposizioni dell'OCIP / OCIP-DFI[1]

Questo capitolo presenta i pareri sui singoli articoli del testo. Nei limiti del possibile, le diverse proposte di modifica sono state riportate alla lettera. In caso di richieste di integrazione del testo di un atto normativo, l'aggiunta è stata sottolineata per motivi di trasparenza. Le richieste generali di modifica, di stralcio e di aggiunta concernenti altri atti normativi sono menzionate, ma non espressamente contrassegnate.

3.1 OCIP

3.1.1 Capitolo 1: Vertraulichkeitsstufen und Zugriffsrechte

CMC, *BüAeV*, *GAeSO*, *KAeG SG* e *HIN* ritengono opportuno completare il capitolo 1 «Gradi di riservatezza e diritti di accesso» con una disposizione aggiuntiva. Propongono un nuovo articolo «Registrazione dei propri dati», con la seguente formulazione: «Von der Patientin oder dem Patient selber erfasste Daten werden im elektronischen Patientendossier in einem separaten Ordner abgelegt. Nimmt die Patientin oder der Patient keine Zuordnung vor, so wird den von ihm eingestellten Daten die Vertraulichkeitsstufe „sensible Daten" zugewiesen und es gilt das Zugriffsrecht „erweitert"». *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* chiedono inoltre di cambiare il titolo del capitolo 1 in: «Gradi di riservatezza e diritti di accesso alla cartella informatizzata del paziente».

Art. 1 Vertraulichkeitsstufen

[1] Die Patientin oder der Patient kann die Daten des elektronischen Patientendossiers einer der folgenden vier Vertraulichkeitsstufen zuordnen:

a. Vertraulichkeitsstufe «nützliche Daten»;

b. Vertraulichkeitsstufe «medizinische Daten»;

c. Vertraulichkeitsstufe «sensible Daten»;

d. Vertraulichkeitsstufe «geheime Daten».

[2] Nimmt die Patientin oder der Patient keine Zuordnung vor, so wird neu eingestellten Daten die Vertraulichkeitsstufe «medizinische Daten» zugewiesen.

[3] In Abweichung von Absatz 2 kann eine Gesundheitsfachperson neu eingestellten Daten die Vertraulichkeitsstufe «sensible Daten» zuweisen.

SSIM raccomanda di nominare un responsabile della protezione dei dati e propone di applicare le prescrizioni della legge sulla protezione dei dati. Chiede altresì di evitare una regolamentazione eccessiva. *FMH* segnala che di solito sono i medici ad aiutare i pazienti ad aprire una cartella informatizzata del paziente e a consigliarli in materia. Questo lavoro dovrebbe ricevere un compenso finanziario. A tale proposito *FMH* ricorda inoltre che la cartella informatizzata del paziente dovrebbe semplificare la comunicazione fra paziente e professionista della salute, e non ostacolarla. eHealth e quindi anche la cartella informatizzata del paziente dovrebbe accompagnare il paziente nel suo percorso medico, accelerare lo scambio di informazioni, rafforzare la sicurezza del paziente e rafforzare la coesione fra paziente e professionista della salute. Concretamente si chiede la costituzione di organismi incaricati di aprire le cartelle informatizzate e di informare i pazienti.

Capoverso 1: 7 partecipanti[2] ritengono insufficiente, dal punto di vista della protezione dei dati, illustrare le diverse tipologie di dati solo nel rapporto esplicativo. Chiedono invece che nell'ordinanza vengano presentanti degli esempi sui tipi di dati che rientrano nei vari gradi di riservatezza. Avanzano anche una proposta concreta per la formulazione di un capoverso aggiuntivo all'articolo 1. Analogamente anche *FSAS*, *SWOR*, *Physioswiss* e *ASI* segnalano che è necessario introdurre nell'ordinanza le spiegazioni

[1] Visto che gli avamprogetti non sono stati tradotti in italiano, il presente rapporto riporta le due versioni disponibili al momento della consultazione, cioè tedesco e francese, nonché le richieste di modifica in versione originale.

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

sui gradi di riservatezza contenute nel rapporto esplicativo, affinché l'attribuzione sia chiara sia per i professionisti della salute che per i pazienti. Anche il Cantone *TG* auspica una breve spiegazione dei gradi di riservatezza. *FMH* fa notare diversi problemi di terminologia e traduzione nelle denominazioni dei gradi di riservatezza e chiede una denominazione precisa e una definizione dei gradi di riservatezza. Il Cantone *TI* auspica una definizione precisa delle tipologie di dato. Gli esempi del rapporto esplicativo non sono esaustivi e la definizione dovrebbe essere inserita nel testo dell'ordinanza. Sulla stessa falsariga altri 6 Cantoni[3], sottolineano che diversi termini richiedono un chiarimento e soprattutto degli esempi.

FSAS, *SWOR*, *Physioswiss* e *ASI* sono favorevoli allo scaglionamento proposto con i 4 gradi di riservatezza; anche *H+* e *senesuisse* apprezzano la limitazione a 4 gradi di riservatezza. *K3* e *VZK* temono che i gradi di riservatezza, i ruoli e i diritti di accesso siano troppo complessi per i normali cittadini e raccomandano di semplificare i diritti di accesso e i gradi di riservatezza. Anche 6 Cantoni[4] chiedono una semplificazione per evitare una confusione che possa scoraggiare i pazienti. 6 partecipanti[5] sono del parere che non è opportuno distinguere fra «dati utilitari» e «dati medici» perché questi termini non sono degli attributi di riservatezza. Sul piano internazionale è più diffusa la distinzione in 3 gradi di riservatezza. Questi partecipanti chiedono pertanto di prevedere 3 livelli: «normal» (consultabile da tutto il personale curante), «restricted» (dati sensibili, consultabili solo dal personale curante che ha un diritto di accesso ampliato) e «very restricted» (dati segreti, consultabili solo dal paziente ed eventuali rappresentanti). Anche *Tessaris* preconizza una limitazione a 3 gradi di riservatezza, che chiama «open = free access», «limited access» e «secret = excluded access». L'abbandono della distinzione fra dati utilitari e medici è chiesta anche dal Cantone *ZH*. *STSAG* propone a sua volta una riduzione a 3 gradi con le denominazioni «utilitari/amministrativi», «medici» e «segreti». Anche *ÄTG* e *HÄ CH* ritengono opportuno vagliare una possibile riduzione da 4 a 3 gradi di riservatezza. Scrivono che in linea di massima già oggi tutti i dati medici sono da considerare sensibili, per cui le categorie delle lettere b e c si fondono in una sola. Anche il Cantone *TI* ritiene che i dati medici sono di principio già considerati dati sensibili e propone di modificare l'espressione «dati sensibili» con «dati stigmatizzanti» (o «dati particolarmente sensibili»). Altri 6 Cantoni[6] segnalano che bisogna distinguere fra le categorie di dati (amministrativi, utilitari, medici) e i gradi di riservatezza (normali, stigmatizzanti, segreti). Inoltre secondo l'art. 3 lettera c della legge federale sulla protezione dei dati, i dati sanitari personali rientrano già fra i «dati sensibili». La distinzione fatta nell'avamprogetto fra dati sensibili e dati medici è incomprensibile ed errata. Deve essere quindi corretta. Bisogna poi precisare che i dati amministrativi sono potenzialmente accessibili a tutti i professionisti della salute.

Tessaris scrive che i «dati medici» corrispondono al grado «open – free access» e propone di prevedere solo i gradi di riservatezza «dati medici» (nuova lettera a), «dati sensibili» (nuova lettera b) e «dati segreti» (nuova lettera c). *VGIch* e *SUVA* avvertono che il grado di riservatezza «dati segreti» è in contraddizione con il fine e lo scopo della cartella informatizzata del paziente e che la lettera d deve essere di conseguenza stralciata. *Senesuisse* e *H+* chiedono di verificare, dopo circa 3-5 anni dall'introduzione, se il grado 4 è effettivamente necessario. Mentre *senesuisse* obietta che questo grado non porta un valore aggiunto agli obiettivi della strategia eHealth, *H+* evidenzia che la tutela della confidenzialità e della protezione dei dati nell'interesse del paziente deve avere la precedenza sul libero scambio dei dati. *IG eHealth* e *PH CH* fanno notare di aver sostenuto i 5 gradi di riservatezza raccomandati da eHealth Suisse e avvertono che la soppressione della categoria «dati amministrativi» crea un vuoto, perché impedisce di disciplinare l'accesso a informazioni degne di protezione nel MPI. *IG eHealth* aggiunge che potrebbe appoggiare anche i 4 gradi di riservatezza scelti, purché si definisca come gestire i dati sensibili del MPI. Assieme a *PH CH* propone di introdurre una nuova lettera al capoverso 1 per disciplinare l'impiego dei dati amministrativi sensibili. Il Cantone *TI* chiede di aggiungere il grado di riservatezza «dati amministrativi», per i quali bisognerebbe poi specificare il diritto di accesso nell'art. 2 capoverso 1.

---

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

IG eHealth, *PH CH*, il Cantone *ZG* e *Posta* chiedono una definizione conclusiva del termine «dati». *Posta* raccomanda altresì di raccogliere i termini e le definizioni in un glossario. Anche il Cantone *NE* sottolinea la necessità di chiarire la terminologia per assicurare la certezza del diritto. Secondo 7 partecipanti[7] i diritti di accesso devono essere esercitati solo fino a livello di documento. *IG eHealth* e *PH CH* propongono una formulazione alternativa per il capoverso 1: «[…] die Daten, die in einem Dokument zusammengefasst sind, einer der […]». Anche *Integic* auspica un chiarimento del termine «dati» e rimanda all'allegato 3 – OCIP-DFI: Metadati, Capitolo 1.12 «Tipo di documento». *VGIch* desidera una precisazione del termine «dati medici» oppure la scelta di un termine meno restrittivo. Il Cantone *TI* chiede di aggiungere direttamente nel testo dell'OCIP la definizione di dati e documenti relativi ai vari livelli di riservatezza.

Capoverso 2: *KDSBSON* fa notare che, in linea di massima, le misure di protezione e sicurezza dei dati non dovrebbero essere semplicemente raccomandate, bensì prestabilite con delle preimpostazioni tecniche. A partire da questo approccio «privacy by default», le impostazioni di base dovrebbero essere definite in modo più restrittivo. Concretamente, l'articolo 1 capoverso 2 dovrebbe stabilire che i nuovi dati registrati siano attribuiti ai «dati sensibili» e l'articolo 2 capoverso 2 che senza istruzioni specifiche del paziente si applichi il diritto di accesso «limitato». Anche *DSBAG* avanza le stesse proposte e ne chiede un esame. *Privatim* obietta che dal punto di vista della protezione dei dati è insoddisfacente che senza un intervento del paziente praticamente «tutto sia accessibile a tutti» e chiede pertanto di operare una distinzione secondo l'approccio «privacy by default». A livello concreto propone due piste di soluzione, che includono anche l'assegnazione automatica dei nuovi dati al grado di riservatezza «dati sensibili». Analogamente *Integic* e *BINT* raccomandano di attribuire ai nuovi dati registrati il grado di riservatezza «restricted» se il paziente non stabilisce altrimenti. Il paziente potrebbe inoltre scegliere l'opzione che sia il professionista della salute a determinare il grado di riservatezza. Se ciò non avviene si applica automaticamente il livello «restricted». Il Cantone *TG* scrive che come impostazione standard bisognerebbe definire il grado di riservatezza «dati sensibili» o «dati segreti». Secondo *FMH* l'impostazione standard dovrebbe essere scelta in modo tale da tenere meglio conto delle esigenze della maggioranza dei pazienti. *Tessaris* propone che al momento della registrazione nella cartella informatizzata del paziente i dati siano classificati con il grado di riservatezza «dati sensibili».

Secondo il Cantone *BS*, il tema «privacy by default» solleva l'interrogativo se non sia più opportuno rinunciare completamente a un'impostazione default per la registrazione dei dati. Lasciando al professionista della salute o alla struttura sanitaria la possibilità di scegliere il grado di riservatezza e rinunciando a un'impostazione generale come «dati sensibili» si potrebbe evitare che molti professionisti della salute con diritto di accesso «normale» vadano a consultare la cartella informatizzata del paziente senza trovarvi dei dati. Il Cantone *FR* avverte che il principio «privacy by default» può contrastare con gli obiettivi della cartella informatizzata del paziente e chiede pertanto di soppesare gli interessi. 10 partecipanti[8] respingono il principio «privacy by default» perché non permette di raggiungere gli obiettivi preconizzati. Il Cantone *SO* parte dal presupposto che l'informazione adeguata prevista dall'articolo 3 includa anche il grado di riservatezza standard (e i diritti di accesso standard secondo l'art. 2 cpv. 2 OCIP). Il Cantone *AR* scrive di non essere contrario al «privacy by default». 10 partecipanti[9] ritengono che la maggior parte dei pazienti non voglia gestire da sola i gradi di riservatezza e chiedono di dare la possibilità ai professionisti della salute di attribuire ai dati il grado di riservatezza «dati utilitari». Secondo 9 partecipanti[10] sarebbe utile verificare se sia possibile anche a livello di documenti scegliere un'attribuzione standard diversa del grado di riservatezza, che avverrebbe automaticamente al momento dell'upload sulla base dei metadati contenuti nel documento. *HÄ CH* e *ÄTG* considerano problematica la possibilità prevista nel capoverso 2 del rapporto esplicativo di attribuire per default ai nuovi dati registrati il grado di riservatezza «dati sensibili». Ciò potrebbe anche involontariamente privare i professionisti della salute di gran parte delle informazioni mediche; l'attribuzione di questo grado di riservatezza

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

dovrebbe avvenire manualmente, caso per caso. *Santésuisse* obietta che la possibilità data al paziente di attribuire ogni grado di riservatezza a ogni tipo di documento può ostacolare una visione d'insieme. Attribuire a informazioni importanti un grado di riservatezza privo di diritto di accesso potrebbe condurre a situazioni critiche dal punto di vista medico. Tali situazioni potrebbero essere eventualmente evitate introducendo un rimando, visibile a tutti i professionisti della salute autorizzati, all'eventuale esistenza di ulteriori informazioni. Il Cantone *FR* propone di aggiungere un capoverso per assicurare l'informazione dei pazienti e controllare che abbiano capito l'importanza dei gradi di riservatezza.

Posta e *IG eHealth* temono che il meccanismo descritto nel capoverso 2 non sia attuabile. Ogni documento deve essere esaminato prima di essere attribuito a un grado di riservatezza. *Posta* aggiunge che i professionisti della salute possono memorizzare in pochi secondi un nuovo documento nel loro sistema locale senza che il paziente possa impedirlo nel processo manuale. L'obiettivo dovrebbe essere invece che i professionisti della salute conoscano in anticipo il grado di riservatezza da attribuire ai documenti. *Posta* e *IG eHealth* avanzano la seguente proposta di formulazione per il capoverso 2: «Ohne andere Anweisungen der Patientin oder des Patienten, publizieren Gesundheitsfachpersonen Dokumente mit der Vertraulichkeitsstufe "medizinische Daten"». *PH CH* propone una formulazione alternativa: «Neu eingestellte Daten werden, sofern die Gesundheitsfachperson nicht anderes zuweist, mit der Vertraulichkeitsstufe „medizinische Daten" gespeichert».

VAKA chiede di dare la possibilità ai pazienti di scegliere un'impostazione attraverso la quale possano accordare a tutti i professionisti della salute registrati il livello di accesso «normale» e attribuire a tutti i nuovi documenti come default il grado di riservatezza «dati medici». Per i pazienti che lo desiderano va mantenuta tuttavia la possibilità di amministrare i diritti di accesso in modo particolareggiato. Una possibile misura di sicurezza potrebbe consistere, secondo *VAKA*, nell'inviare periodicamente ai pazienti un elenco di tutte le persone che hanno accesso alla loro cartella informatizzata. *Tessaris* propone che alla fine di un trattamento il paziente possa stabilire il tipo e l'entità dei nuovi dati da inserire nella cartella informatizzata. Il consenso all'inserimento dei dati terapeutici nella cartella informatizzata del paziente dovrebbe essere accordato per iscritto e firmato dal paziente. I dati inseriti dovrebbero essere rigorosamente criptati secondo lo stato della tecnica. Inoltre dovrebbe essere possibile chiedere che anche i dati di trattamenti precedenti vengano inseriti nella cartella informatizzata del paziente. Il Cantone *ZH* lamenta la mancanza di una regolamentazione dei casi di incapacità di discernimento. Questi casi devono essere disciplinati nel diritto d'esecuzione o quantomeno discussi nel rispettivo rapporto esplicativo. Sarebbe altrettanto importante disciplinare la gestione della cartella informatizzata di adolescenti / giovani adulti, in particolare il momento e le modalità del passaggio del controllo dai genitori ai giovani.

Capoverso 3: *Integic*, *HL7* e *IHE* criticano questo capoverso perché viola la decisione del paziente. Questi partecipanti, nonché *Bleuer* e *Tessaris* ne chiedono lo stralcio. Se il capoverso 3 non viene stralciato, *Integic* propone un'aggiunta secondo la quale il paziente deve essere informato di nuovi dati «very restricted». *SPO* e *FRC* sottolineano l'importanza del consenso del paziente. *SPO* propone la seguente formulazione: «[…] kann eine Gesundheitsfachperson im Einverständnis der Patientin oder des Patienten neu eingestellte […]». *FRC* propone la seguente aggiunta: «[…] le dossier électronique du patient peut, avec l'accord du patient, leur attribuer le niveau de confidentialité «données sensibles». Sulla stessa falsariga *pharmaSuisse* propone: «[…] eine Gesundheitsfachperson im Auftrag einer Patientin oder eines Patienten neu eingestellte […]» per sottolineare che il professionista della salute agisce su incarico del paziente. Ciò potrebbe avvenire per esempio nell'ambito del consenso alla gestione di una cartella informatizzata del paziente secondo l'articolo 15. *K3* e *VZK* fanno notare che in ambito ospedaliero sarà impossibile che i singoli professionisti della salute registrino i dati o i documenti e chiedono pertanto di aggiungere i gruppi di professionisti della salute al capoverso 2 con la seguente formulazione: «[…] eine Gesundheitsfachperson oder eine Gruppe von Gesundheitsfachpersonen neu eingestellte Daten […]». *PKS* scrive che un ospedale deve essere in grado di attribuire automaticamente i gradi di riservatezza ai documenti attraverso un'applicazione e incaricarne diversi professionisti della salute o il loro personale ausiliario. Questi partecipanti, assieme a *UDC*, chiedono lo stralcio della limitazione per l'assegnazione al livello «dati sensibili». *Tessaris* propone un nuovo articolo: «Die Patientin oder der Patient kann die Vertraulichkeitsstufe für Daten im elektronischen Patientendossier jederzeit

ändern. Die Änderung wird der für die betreffende Behandlung zuständigen Gesundheitsfachpersonen automatisch angezeigt.»

Anticipando l'articolo 2, *H+* e *senesuisse* dichiarano di approvare il principio secondo cui, in assenza di istruzioni specifiche del paziente, l'impostazione di base prevede il diritto di accesso «normale». Per assicurare una gestione semplice, respingono l'introduzione di ulteriori livelli. Anche *HIN* si esprime già in questa sede sull'articolo 2 e propone la seguente aggiunta: «Nimmt die Patientin oder der Patient keine weitere Einschränkung vor, kann die Gesundheitsfachperson die ihr zugewiesenen Zugriffsrechte an Hilfspersonen delegieren, sofern deren Zugehörigkeit zur Gesundheitsfachperson gemeinschaftsintern verwaltet wird». A complemento dell'articolo 3 propone di aggiungere: «Die Patientin oder der Patient kann: einzelnen Gesundheitsfachpersonen untersagen, die Zugriffsrechte an Hilfspersonen zu delegieren.»

Art. 2 Zugriffsrechte

[1] Die Patientin oder der Patient kann Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen folgende Zugriffsrechte zuweisen:

a. «eingeschränkt»: Zugriff auf die Vertraulichkeitsstufe «nützliche Daten»;

b. «normal»: Zugriff auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten»;

c. «erweitert»: Zugriff auf die Vertraulichkeitsstufen «nützliche Daten», «medizinische Daten» und «sensible Daten».

[2] Nimmt die Patientin oder der Patient keine Zuweisung vor, so gilt das Zugriffsrecht «normal».

[3] Die Zugriffsrechte gelten bis zum Entzug durch die Patientin oder den Patienten.

[4] Tritt eine Gesundheitsfachperson einer Gruppe von Gesundheitsfachpersonen bei, so erhält sie das mit dieser Gruppe verbundene Zugriffsrecht. Verlässt eine Gesundheitsfachperson eine Gruppe, so wird ihr das mit der Gruppe verbundene Zugriffsrecht entzogen.

[5] In medizinischen Notfallsituationen können Gesundheitsfachpersonen auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten» zugreifen. Sie müssen einen solchen Zugriff vorgängig begründen.

HIN e *santésuisse* ripetono le loro osservazioni sull'articolo 1, mentre *FMH* reitera il suo commento introduttivo sull'articolo 1. *PH CH* e *IG eHealth* desiderano un capoverso 6 con il seguente contenuto: «Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft sind ermächtigt, im Namen der Patientin oder des Patienten Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen; dabei können diese höchstens die Zugriffsrechte zuweisen, die sie selber besitzen.» *CMC*, *BüAeV* e *GAeSO* propongono di aggiungere all'articolo 2 il seguente capoverso: «Nimmt die Patientin oder der Patient keine weitere Einschränkung vor, kann die Gesundheitsfachperson die ihr zugewiesenen Zugriffsrechte an Hilfspersonen delegieren, sofern deren Zugehörigkeit zur Gesundheitsfachperson gemeinschaftsintern verwaltet wird». *SPO* chiede di aggiungere i seguenti capoversi: capoverso 6: «Der Patientin und dem Patienten ist jederzeit Einblick auf das Zugriffsprotokoll gemäss Artikel 8 Absatz 1 EPDG zu ermöglichen». Capoverso 7: «Im Streitfall muss der Nachweis für den rechtmässigen Zugriff von der Gesundheitsfachperson erbracht werden». *Physioswiss* approva esplicitamente i capoversi da 1 a 4. Il Cantone *TI* fa notare che è indispensabile regolamentare l'accesso a un singolo documento da parte dell'autore che non ha diritto di accedere alla cartella informatizzata del paziente e che l'autore deve essere comunque in grado di modificare questo documento in caso di errore. *SSIM* obietta che con questa regolamentazione il paziente assume la responsabilità delle informazioni non messe a disposizione, che potrebbero pregiudicare la sicurezza del trattamento. Analogamente *STSAG* chiede di definire in un capoverso separato le responsabilità nel caso in cui i pazienti classifichino dei dati come segreti. In situazioni di emergenza ritiene che debba essere autorizzato anche l'accesso a informazioni segrete.

14 partecipanti[11] criticano la mancanza di disposizioni sui minori e sulle persone incapaci di discernimento e chiedono di colmare questa lacuna. Secondo 9[12] di questi partecipanti, il diritto di esecuzione finora non si è occupato della questione se, e a quali condizioni, i diritti di amministrazione della cartella

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

[12] BL, CDS, GL, OW, UR, VAKA, NW, BE, TG

informatizzata possano essere esercitati da un rappresentante di cui all'articolo 3 lettera g anche senza il consenso o contro la volontà del paziente. *K3*, *VZK*, il Cantone *ZG* e *ZAD* auspicano che l'ordinanza disciplini anche l'impiego della cartella informatizzata di pazienti deceduti. Per *K3* e *VZK* si pone inoltre la questione se verrà allestita una cartella per i sans-papiers.

Capoverso 1: *Insel* obietta che la creazione di tre livelli di diritto di accesso è inutilmente complicata. Un paziente che vuole impedire la consultazione di dati sensibili da parte di terzi eviterà di caricarli nella cartella. Bisogna poi considerare che le strutture sanitarie saranno poco propensi a ricorrere alla cartella elettronica del paziente se questa è lacunosa, e preferiranno i loro sistemi primari. *Insel* chiede pertanto lo stralcio della lettera a del capoverso 1. *HÄ CH* e *ÄTG* ricordano che, seguendo la loro proposta di riunire le lettere b e c dell'articolo 1 capoverso 1, nell'articolo 2 capoverso 1 rimarrebbero solo due possibilità di scelta. Fanno notare che l'attribuzione dei diritti di accesso nella forma prevista rappresenta un processo che potrebbe essere troppo complesso e difficile per i pazienti. Chiedono quindi una semplificazione. *PharmaSuisse* e il Cantone *ZH* raccomandano che un fornitore di prestazioni sia informato se ha solo un accesso limitato a determinati dati e debba sapere soprattutto a quali contenuti non ha accesso. Secondo *pharmaSuisse* dovrebbe essere inoltre possibile risalire, tramite dei logfile, alle informazioni che un fornitore di prestazioni aveva a disposizione in un determinato momento. *Integic* chiede di adottare i 3 gradi di riservatezza diffusi a livello internazionale (EPSOS). Propone pertanto di riformulare le lettere da a a c del capoverso 1 come segue: «a. «limitato»: accesso al grado di riservatezza «normal»; b. «normale»: accesso ai gradi di riservatezza «normal» e «restricted»; c. «ampliato»: accesso ai gradi di riservatezza «normal», «restricted» e «very restricted». *PH CH* obietta che l'introduzione di nuove nozioni per i diritti di accesso non ha senso e propone il seguente testo alternativo per il capoverso 1: «[…] von Gesundheitsfachpersonen wahlweise den Zugriff auf nur nützliche Daten, nützliche und medizinische Daten oder auf nützliche, medizinische und sensible Daten gewähren». Le lettere da a a c verrebbero stralciate così come il capoverso 3, che verrebbe integrato nel capoverso 2. *Tessaris* propone che tutti i professionisti della salute coinvolti nel trattamento di un paziente possano accedere ai «dati medici», a condizione che il paziente non lo abbia previamente negato a tutti o a un determinato professionista della salute. Inoltre il professionista curante dovrebbe poter accedere anche ai «dati sensibili» o ai «dati segreti», se il paziente ha previamente autorizzato l'accesso. *KAeG SG* avverte che alcune iscrizioni non possono più avvenire in modo professionale se il paziente vi può accedere. Inoltre si chiede come sia possibile accedere ai dati in caso di smarrimento della tessera e se la memorizzazione avviene in un sistema cloud.

11 partecipanti[13] considerano complesso e oneroso il costrutto «gruppi di professionisti della salute». 9 di questi partecipanti[14] chiedono di vagliare una possibilità di semplificazione, mentre il Cantone *ZH* e *ZAD* propongono di sopprimere l'intero costrutto. Il Cantone *ZH* avanza una proposta alternativa per il capoverso 1: «Die Patientin oder der Patient kann Leistungserbringern und Gesundheitsfachpersonen folgende Zugriffsrechte zuweisen: […]». Secondo il Cantone *TI* è necessario definire la nozione di «gruppo di professionisti della salute» e rendere comprensibile al paziente l'utilizzo di questa funzionalità. Anche altri 6 Cantoni[15] chiedono una precisazione della nozione di «gruppo». A loro avviso, il fatto che un paziente non possa accordare diritti di accesso a una struttura, ma solo a dei gruppi di dimensioni ragionevoli pone dei problemi di fattibilità negli ospedali. Chiedono pertanto di aggiungere gli istituti al capoverso 1: «Le patient peut accorder à des institutions, des professionnels […]» e al capoverso 4: «[…] un groupe ou une institution reçoit les droits d'accès accordés à ce groupe ou à l'institution.»

I capoversi da 1 a 4 devono essere completati in modo tale che le disposizioni si applichino sia ai gruppi che ale strutture sanitarie. *SMCF* ritiene che per motivi pratici si dovrebbe rinunciare ad accordare diritti di accesso individuali all'interno di un determinato gruppo di professionisti. Per il Cantone *AG* i diritti di accesso di gruppo sono molto importanti nella pratica. Dal punto di vista della protezione dei dati, la ricerca di dati sulla composizione dei gruppi sembra conforme alle norme sulla protezione dei dati, ma potrebbe provocare un onere supplementare per la comunità. Secondo *PKS* le disposizioni sui diritti di

[13] BL, GL, LU, OW, UR, ZG, SZ, NW, CDS, ZH, ZAD
[14] BL, GL, LU, OW, UR, ZG, SZ, NW, CDS
[15] GE, VS, VD, JU, FR, NE

accesso non vengono incontro alle esigenze terapeutiche dei pazienti né consentono processi adeguati e pratici negli ospedali. Propone di introdurre come impostazione standard il pieno accesso a tutti i dati medici, con la possibilità per i pazienti di limitarlo. La limitazione temporanea anche ai dati sensibili e il dovere di motivazione ostacola inutilmente la raccolta di informazioni in caso di emergenza.

Capoverso 2: *KDSBSON*, *DSBAG*, *privatim* e il Cantone *FR* ripetono in questa sede i commenti fatti sull'articolo 1 capoverso 2 riguardo al tema «privacy by default».

FSAS, *Physioswiss*, *SWOR*, *ASI* e *H+* sono favorevoli all'impostazione standard «normale» per i diritti di accesso. *Posta* chiede invece che, senza precise istruzioni, si applichi automaticamente il diritto di accesso «limitato». *Tessaris* scrive che questo capoverso potrebbe essere stralciato, poiché l'accesso limitato al grado di riservatezza «dati sensibili» è già implicito nella sua proposta sull'articolo 1 capoverso 2. *FMH* reitera a questo proposito la posizione espressa sull'articolo 1 capoverso 2.

Capoverso 3: *KDSBSON*, *DSBAG*, *privatim* e il Cantone *ZG* segnalano che la concessione dei diritti di accesso dovrebbe avere una durata limitata. Sarebbe opportuno vagliare la possibilità di inviare una comunicazione ai pazienti prima della scadenza dei diritti di accesso. I suddetti partecipanti propongono il seguente adeguamento dell'articolo 3 lettera a: «Die Zugriffsrechte werden den einzelnen Gesundheitsfachpersonen für längstens zwei Jahre eingeräumt». Anche il Cantone *TG* è favorevole a una limitazione della durata massima dei diritti di accesso. *Tessaris* auspica lo stralcio di questo capoverso poiché la sua proposta sull'articolo 1 capoverso 3 prevede già una modifica dei gradi di riservatezza e quindi dei diritti di accesso e della loro revoca. Il capoverso 3 dell'articolo 2 potrebbe recitare come segue: «Die Patientin oder der Patient kann eine namentlich bezeichnete Gesundheitsfachperson oder eine Gruppe von Gesundheitsfachpersonen zeitweilig oder dauernd vom Zugriff auf ihr oder sein elektronisches Patientendossier ausschliessen».

Capoverso 4: *Privatim*, *KDSBSON* e *DSBAG* fanno notare che se le autorizzazioni di gruppo vengono mantenute bisognerebbe lasciare ad ogni costo anche la possibilità di un «opt-out» secondo l'articolo 3 lettera f. Il Cantone *TG* ritiene che l'assegnazione automatica ai gruppi e la conseguente assunzione di diritti potrebbe essere problematica per il segreto professionale e cita un esempio a tale proposito. Chiede di trovare una soluzione che garantisca in ogni caso il segreto professionale.

KSSG obietta che in una grande organizzazione non è possibile fornire un quadro chiaro di tutti i professionisti della salute e dei gruppi di professionisti della salute. Inoltre il frequente avvicendamento di personale fa sì che i pazienti riceverebbero troppe informazioni. Propone pertanto di aggiungere una lettera all'articolo 8 per specificare che l'UFSP può autorizzare le comunità, su loro richiesta, a comunicare ai pazienti solo una parte dei professionisti della salute. Inoltre, riguardo al dovere di informazione di cui all'articolo 8 lettera f, si pone la questione per l'articolo 2 capoverso 4 se i diritti debbano essere concessi immediatamente o meno. *KSSG* propone la seguente aggiunta al capoverso 4: «[…] verbundene Zugriffsrecht, ohne besondere Bestätigung durch die Patientin oder den Patienten. Verlässt eine […]». *VGIch* segnala che un professionista della salute, se riceve automaticamente il diritto di accesso del gruppo, ha abbastanza tempo per caricare le informazioni di un paziente sul sistema primario prima che il paziente abbia la possibilità di escluderlo dal diritto di accesso. Propone la creazione di veri gruppi collettivi. Il paziente dovrebbe in tal caso decidere se accettarli oppure no. *ISSS* propone di formulare un nuovo capoverso, secondo il quale le comunità devono fornire su richiesta un elenco del personale ai pazienti, affinché questi ultimi possano decidere sull'attribuzione dei diritti di accesso dei professionisti della salute o di gruppi. *PH CH* e *IG eHealth* criticano il fatto che l'impostazione di base preveda l'informazione dei pazienti su tutti i cambiamenti in seno al gruppo, ma non sugli accessi in caso di emergenza. Ne risulta un profluvio di informazioni per i pazienti e allo stesso tempo una trasparenza sui trasferimenti dei professionisti della salute, che viola i diritti della personalità di questi ultimi. *Lovis* è contraria a una «lista nera» di singole persone che vengono escluse.
K3 e *VZK* segnalano che non è chiaro se i professionisti della salute possano appartenere contemporaneamente a vari gruppi e chiedono che ciò sia possibile (con uno strumento d'identificazione). Per gli ospedali è importante che l'accesso alla cartella informatizzata del paziente venga concesso all'intero ospedale, a un gruppo all'interno dell'ospedale e ai singoli professionisti della salute, e che in caso

normale l'impostazione standard preveda il diritto di accesso per tutto l'ospedale. A questo proposito i due partecipanti puntualizzano che i diritti di accesso devono valere anche per il personale ausiliario. Questa disposizione deve essere inserita nell'ordinanza perché finora è citata solo nell'allegato 2 numero 1.3 (RTO) dell'OCIP-DFI. È altresì necessario assicurare che i reparti del personale degli ospedali possano svolgere facilmente delle verifiche dell'identità (art. 23 OCIP) e rilasciare adeguati strumenti d'identificazione (art. 22 OCIP) nonché rinnovarli (art. 25 OCIP).

Capoverso 5: *BRH* ritiene complesso e nebuloso l'accesso nelle situazioni di emergenza e auspica una descrizione più concreta degli elementi di sicurezza. Inoltre chiede di indicare il tempo necessario durante le emergenze per superare tali barriere di sicurezza. *VAKA*[16] è del parere che nei casi di emergenza dovrebbero essere disponibili automaticamente anche i dati sensibili. S*enesuisse* osserva che il testo non è formulato in modo abbastanza chiaro da disciplinare esattamente i diritti dei professionisti della salute. Mentre il capoverso 5 prevede solo l'accesso ai dati «utilitari» e «medici», secondo l'articolo 3 lettera b la decisione sul diritto di accesso spetta unicamente al paziente anche in caso di emergenza. Sarebbe preferibile una disposizione che sia adeguata alle emergenze mediche. Il Cantone *ZG* chiede un chiarimento nel rapporto esplicativo per specificare che, in caso di accesso durante un'emergenza medica, l'articolo 24 LCIP si applica solo se è evidente che non si tratta di una situazione di emergenza.

VAKA scrive che per un accesso in caso di emergenza occorre una nuova registrazione. Un'ulteriore motivazione le sembra obsoleta, per cui la frase: «Sie müssen einen solchen Zugriff vorgängig begründen» può essere stralciata. La soppressione della motivazione per gli accessi in caso di emergenza è auspicata anche da *K3*, *VZK*, il Cantone *ZH* e *ZAD*. *ASPS*, *Spitex* e *BINT* sostengono che l'ostacolo della motivazione deve essere mantenuto basso in modo da consentire un accesso tempestivo. I modelli di motivazione strutturati sono più facili da gestire e valutare. Come *BINT* propongono una motivazione semplice in caso di emergenza oppure la possibilità di una motivazione a posteriori. Analogamente, anche *FMH* e *Physioswiss* sono contrari alla previa motivazione di un accesso in caso di emergenza. Un'informazione sistematica successiva e un'eventuale motivazione in caso di sospetto di accesso abusivo dovrebbero essere sufficienti. 6 Cantoni[17] chiedono inoltre di sopprimere nel capoverso 5 il termine «vorgängig» risp. «au préalable». Il Cantone *ZG* auspica una conferma che non vengano introdotti requisiti più severi riguardo al contenuto e all'entità della motivazione. Altrimenti sussiste il rischio che in caso di dubbio i professionisti della salute non facciano ricorso alla cartella informatizzata del paziente. Per evitare un impiego irregolare della motivazione di un intervento di emergenza, *HL7*, *IHE* e *Integic* auspicano delle istruzioni sulla forma e il grado di dettaglio della documentazione. Come anche *SSIM*, questi partecipanti ipotizzano come alternativa alla motivazione anticipata una breve conferma dell'emergenza (1 click) e una giustificazione dettagliata solo in un secondo momento. *Posta* chiede di sostituire la motivazione, che giudica insensata, con un'informazione automatica al medico di fiducia e al paziente. In caso di emergenza bisognerebbe confermare la volontà che sia svolto un accesso di emergenza con notifica (spuntare e premere «OK»). Il Cantone *AG* sottolinea la necessità di trovare una soluzione tecnicamente semplice per l'accesso in caso di emergenza. Il Cantone *TI* dubita che il requisito di motivazione scritta ed eventuali barriere con password e codici di un accesso in modalità d'urgenza sia praticabile. Sarebbe più sensato utilizzare una risposta standard da confermare, posticipando la motivazione scritta al termine della presa a carico. Mentre anche *LUKS* preconizza una motivazione a posteriori e non a priori e *Insel* chiede concretamente di depennare la parola «vorgängig», *SPO* è favorevole a una previa motivazione dell'accesso in caso di emergenza medica con un'interazione manuale a titolo di garanzia. Analogamente a *SPO, FRC* ritiene necessario motivare in anticipo, seppure brevemente, ogni accesso di emergenza.

SMCF avanza una proposta concreta su come formulare il capoverso 5: «En cas d'urgence médicale, […] Ils doivent pouvoir motiver cet accès a posteriori». *Tessaris* propone la seguente formulazione: «[…] auf die Vertraulichkeitsstufen „medizinische Daten" und „sensible Daten" zugreifen. Sie müssen die Begründung für einen solchen Zugriff im elektronischen Patientendossier in textlicher Form festhalten». *IG*

[16] Senza Bethesda

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

eHealth e *PH CH* preferirebbero la seguente formulazione per il capoverso 5: «In medizinischen Notfallsituationen können Ärzte auf die die Vertraulichkeitsstufe „medizinische Daten“ zugreifen. Sie müssen einen solchen Zugriff vorgängig durch eine Willensbekundung bestätigen. Die Willensbekundung muss den Hinweis enthalten, dass der Zugriff nur in einer medizinischen Notfallsituation des Patienten durchgeführt werde darf. Der Patient und sein Hausarzt sind über diesen Notfallzugriff zu informieren». Anche *Pharmasuisse* avanza una proposta concreta: «[…] Gesundheitsfachpersonen auf sämtliche Vertraulichkeitsstufen zugreifen, sofern sie vom Patienten nicht generell vom Zugriff ausgeschlossen wurden. Sie müssen […]». *CURAVIVA* e *Insos* segnalano un'incongruenza fra il capoverso 5 e l'articolo 3 lettera b in fine OCIP e la mancanza di un ordine di priorità. Propongono pertanto di aggiungere una frase alla fine del capoverso 5: «Artikel 3 Buchstabe b in fine bleibt vorbehalten». *VLSS* raccomanda al capoverso 5 di estendere l'accesso di emergenza anche ai «dati sensibili», a meno che il paziente in questione non lo abbia limitato ai «dati medici» o ai «dati utilitari» secondo l'articolo 3 lettera c. *KAeG SG*, *BüAeV*, *GAeSO* e *CMC* propongono la seguente aggiunta al capoverso 5: «Die Stammgemeinschaft stellt sicher, dass die Information über den Zugriff der Patientin oder dem Patienten auf der von ihr bzw. ihm vorgängig gewählten Zustellungsart erfolgt. Hat die Patientin oder der Patient keine Zustellungsart gewählt, erfolgt die Mitteilung der Information per Einschreiben». *BüAeV*, *GAeSO* e *CMC* chiedono una definizione più precisa delle emergenze mediche e propongono di aggiungere un capoverso all'articolo 5 con il seguente contenuto: «Medizinische Notfälle sind Fälle, bei welchen die Patientin oder der Patient infolge eines Unfalls oder infolge einer Krankheit dringend medizinischer Hilfe bedarf».

Art. 3 Optionen der Patientinnen und Patienten

Die Patientin oder der Patient kann:

a. festlegen, dass die Zugriffsrechte nach Artikel 2 Absatz 1 nach sechs Monaten erlöschen;

b. das Zugriffsrecht für medizinische Notfallsituationen auf die Vertraulichkeitsstufe «nützliche Daten» einschränken, um die Vertraulichkeitsstufe «sensible Daten» erweitern oder vollständig ausschliessen;

c. festlegen, welche Vertraulichkeitsstufe neu eingestellten Daten zugewiesen wird;

d. einzelne Gesundheitsfachpersonen vom Zugriff auf ihr oder sein elektronisches Patientendossier ausschliessen;

e. die Information nach Artikel 8 Buchstabe f deaktivieren;

f. festlegen, dass Gesundheitsfachpersonen, die in eine Gruppe von Gesundheitsfachpersonen eintreten, nicht automatisch das mit der Gruppe verbundene Zugriffsrecht erhalten;

g. eine Stellvertretung benennen;

h. Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft dazu ermächtigen in ihrem oder seinem Namen Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen; dabei können diese höchstens die Zugriffsrechte zuweisen, die sie selber besitzen.

HIN ripete le sue osservazioni sull'articolo 1. 9 partecipanti[18] reiterano la loro richiesta, avanzata a proposito dell'articolo 2, di introdurre una disposizione sui minori e sulle persone incapaci di discernimento. A questa rivendicazione si associa anche il Cantone *SZ*. Il Cantone *BE* appoggia la richiesta relativa alle persone incapaci di discernimento. Il Cantone *ZG* e *ZAD* segnalano, come già all'articolo 2, che è necessaria una disposizione sulle persone decedute. *FMH* ripete la sua posizione introduttiva espressa sugli articoli 1 e 2.

FRC approva espressamente le lettere da d a h. 6 Cantoni[19] chiedono di aggiungere una lettera i per introdurre la nozione di delega temporanea da un professionista della salute a un altro (in caso di assenza), senza che il paziente debba aggiungere questo professionista nei diritti di accesso. Questa modalità sarebbe attivata di default, ma il paziente avrebbe la possibilità di disattivare la funzione di delega da un professionista dalla salute all'altro. *ASPS* e *Spitex* propongono in questa sede di creare una sorta di indice di tutti i documenti memorizzati nella cartella informatizzata del paziente, affinché il paziente sia informato se per un determinato trattamento sono rilevanti altri documenti. *KAeG SG*,

[18] CDS, BL, GL, LU, OW, UR, NW, ZG, ZAD

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

BüAeV, *GAeSO CMC* fanno notare che se viene accolta la loro proposta di inserire un nuovo articolo sulla registrazione dei propri dati, l'articolo 3 dovrebbe essere modificato come segue: «[…] Vertraulichkeitsstufe die von ihr oder ihm selber erfassten Daten zugewiesen wird und/oder welches Zugriffsrecht gelten soll oder aber das Zugriffsrecht vollständig ausschliessen». Tenuto conto delle osservazioni sul rapporto esplicativo e sulla scia dell'adeguamento dell'articolo 2 si rende inoltre necessaria la seguente modifica dell'articolo 3: «[…] einzelnen Gesundheitsfachpersonen untersagen, die Zugriffsrechte an Hilfspersonen zu delegieren». Di conseguenza bisognerebbe anche estendere o completare il numero 6 RTO. *PKS* fa notare che l'opzione di concedere o revocare i diritti di accesso comporta un notevole onere amministrativo per le comunità e che le liste nere di singoli professionisti non sono conformi all'odierna prassi nel settore sanitario. *SMCF* avverte che la molteplicità e la complessità delle opzioni offerte al paziente annullano i vantaggi della cartella informatizzata. I diritti di accesso dovrebbero essere gestiti in maniera globale per l'intera cartella informatizzata del paziente, senza possibilità di differenziazione.

Lettera a: *privatim*, *DSBAG*, *KDSBSON* e il Cantone *FR* scrivono che per motivi di «privacy by default» l'impostazione di base non dovrebbe prevedere un accesso a tempo indeterminato. Analogamente al Cantone *ZG*, propongono la seguente formulazione per l'articolo 3 lettera a: «a. einzelnen Gesundheitsfachpersonen unbefristete Zugriffsrechte einräumen». Il Cantone *ZG* chiede di verificare la possibilità di limitare la durata dell'autorizzazione di accesso nell'impostazione di base. Secondo *K3*, *VZK* e *VAKA* una restrizione temporale non ha senso ed è difficile da gestire: l'accesso viene o concesso o negato. Come *Integic*, chiedono di stralciare la lettera a. In alternativa allo stralcio, *Integic* vede tuttavia la possibilità di introdurre limitazioni a intervalli temporali diversi. Nella forma attuale le lettere a e f sono difficili da attuare anche per i produttori di sistemi. *VGIch* non capisce perché il limite opzionale per i diritti di accesso sia fissato solo a 6 mesi. Anche *H+* e *Insel* auspicano una maggiore flessibilità affinché il paziente possa stabilire liberamente la durata dei diritti di accesso. *IG eHealth*, *PH CH* e *Posta* considerano troppo rigida la durata fissa di 6 mesi. Fanno notare che il paziente vuole eventualmente accordare a un professionista della salute il diritto di accesso solo per una consultazione, e raccomandano la seguente aggiunta alla lettera a: «[…] Artikel 2 Absatz 1 nach maximal 6 Monaten erlöschen;». 10 partecipanti[20] rilevano che la determinazione delle scadenze dovrebbe essere affidata ai produttori di soluzioni per la cartella informatizzata del paziente e propongono di riformulare la lettera a come segue: «[…] Artikel 2 Absatz 1 befristet gelten;». Il Cantone *TI* fa notare che non è chiaro se il paziente possa far estinguere i diritti di accesso concessi anche con scadenze diverse dai sei mesi e chiede di chiarire questo punto. *Tessaris* considera eccessiva la scadenza di sei mesi e propone che i diritti di accesso di cui all'articolo 2 scadano dopo una durata stabilita dal paziente durante la consultazione. Il Cantone *FR* evidenzia che il paziente dovrebbe ricevere un preavviso sulla scadenza del termine e le sue conseguenze, e chiede pertanto di aggiungere un capoverso o un articolo per ricordare al paziente i suoi diritti e le possibilità di modifica.

FRC ritiene eccellente la possibilità del paziente di annullare automaticamente l'autorizzazione dopo sei mesi.

Lettera b: *CURAVIVA* e *Insos* ripetono la loro posizione sull'articolo 2 capoverso 5. *PharmaSuisse* raccomanda – a condizione che la sua proposta sull'articolo 2 capoverso 5 venga accolta – di modificare l'articolo 3 lettera b come segue: «[…] medizinische Notfallsituationen generell auszuschliessen». Nel caso in cui la sua proposta di formulazione dell'articolo 2 capoverso 5 venga respinta, l'articolo 3 lettera b dovrebbe essere modificato come segue: «[…] medizinische Notfallsituationen nach entsprechender Aufklärung des Patienten durch eine Gesundheitsfachperson auf die Vertraulichkeitsstufe […]». Secondo *Spitex* e *ASPS* i pazienti dovrebbero essere tenuti a confermare attivamente la volontà che i dati sensibili non siano visualizzati in caso di emergenza. L'impostazione standard dovrebbe quindi mantenere i «dati sensibili». Inoltre sarebbe opportuna una notifica automatica dell'avvenuto accesso in caso di emergenza. *Tessaris* scrive che l'articolo 3 lettera b dovrebbe essere stralciato se viene accolta la sua proposta di formulazione dell'articolo 5 capoverso 2. *FRC* obietta che potrebbe essere pericoloso escludere completamente il diritto di accesso in caso di emergenza medica. Il Cantone *AG* considera

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

delicato consentire l'esclusione del diritto di accesso se il paziente al momento dell'impostazione non fosse capace di discernimento. È importante che il rapporto esplicativo faccia riferimento al diritto di protezione dei minori e degli adulti. *HÄ CH* e *ÄTG* non vedono il senso della lettera b e ne chiedono lo stralcio. Secondo *STSAG* bisognerebbe chiarire che il paziente si assume la responsabilità delle conseguenze terapeutiche della mancata disponibilità di informazioni. Come alternativa, le impostazioni di base della cartella informatizzata del paziente dovrebbero prevedere la possibilità di accedere a tutte le informazioni in caso di emergenza.

Lettera c: *Tessaris* chiede lo stralcio dell'articolo 3 lettera c, come risulta dall'introduzione proposta per l'articolo 1. *HÄ CH* e *ÄTG* ritengono problematica questa disposizione e preferiscono che non venga lasciata una possibilità di scelta. In riferimento al loro commento sull'articolo 1 chiedono l'attribuzione per default ai dati medici.

Lettera d: Secondo *H+*, *HÄ CH* e *ÄTG* dovrebbe essere possibile accordare l'accesso in caso di emergenza a un professionista della salute nonostante il blocco generale del paziente. Analogamente anche *VGIch* ritiene che il paziente dovrebbe avere la possibilità di escludere un professionista della salute, ma allo stesso tempo concedergli l'accesso in caso di emergenza. Questa opinione è condivisa anche dal Cantone *BS*, che propone di aggiungere alla fine della frase: «[…] ausschliessen. Sie oder er kann ausgeschlossenen Gesundheitsfachpersonen das Zugriffsrecht für medizinische Notfallsituationen erteilen». *KSSG* è del parere che la lettera d sia in contraddizione con affermazioni orali, secondo le quali non sarebbe necessario presentare ai pazienti tutti i professionisti della salute. Se effettivamente dovesse essere possibile limitare i professionisti presentati all'esterno, la lettera d dovrebbe essere precisata come segue: «d. einzelne der nach aussen sichtbaren Gesundheitsfachpersonen […]». *Tessaris* auspica lo stralcio dell'articolo 3 lettera d e rimanda al suo parere sull'articolo 2 capoverso 3.

Lettera e: *VAKA* scrive che nella lettera e, come nell'articolo 2, bisognerebbe partire da uno standard e consentire solo deroghe effettive. Propone modifiche in base al valore degli standard e delle deroghe. Vista la loro richiesta di stralciare la lettera f dell'articolo 8, 6 Cantoni[21] chiedono che di conseguenza venga soppressa anche la lettera e dell'articolo 3. *IG eHealth* e *PH CH* avvertono che con l'attuale disposizione alcuni pazienti riceverebbero un profluvio di informazioni inutili. Di conseguenza chiedono di modificare come segue la lettera e: «e. kann jederzeit die aktuelle Zusammensetzung einer Gruppe von Gesundheitsfachpersonen abrufen». Anche *Posta* ritiene eccessiva la grande quantità di notifiche dovute ai costanti cambiamenti di personale e chiede, come anche il Cantone *ZG*, di passare da «opt-out» a «opt-in». Sulla stessa falsariga, *Tessaris* desidera che debbano essere i pazienti a chiedere di essere informati di entrate e uscite di professionisti della salute da un gruppo di professionisti della salute. Anche *Spitex* e *ASPS* chiedono che i pazienti debbano confermare attivamente di voler essere informati di nuove entrate di professionisti della salute. Nella lettera e la parola «deaktivieren» dovrebbe essere pertanto sostituita con «aktivieren». *K3* e *VZK* ritengono inaccettabile per motivi di protezione dei dati che i pazienti, attraverso la loro cartella informatizzata, possano raccogliere dati sui tutti i professionisti della salute di una struttura sanitaria, anche se questi professionisti non hanno accesso alla cartella informatizzata del paziente. Chiedono pertanto lo stralcio della lettera e.

Lettera f: *VGIch* ripete il suo commento sull'articolo 2 capoverso 4 riguardo ai gruppi, mentre *KDSBSON*, *DSBAG* e *privatim* reiterano la loro posizione sulla possibilità di «opt-out». *ASI*, *FSAS* e *SWOR* temono che questa disposizione sia difficile da attuare in grandi organizzazioni, ma precisano che questo diritto debba essere concesso ugualmente ai pazienti.

6 Cantoni[22] ritengono che, a parte l'esclusione di un professionista della salute («lista nera») un paziente non dovrebbe avere la possibilità di modificare i diritti che un professionista della salute ha «ereditato» al suo ingresso in un gruppo. *Insel* obietta che l'esclusione di singole persone all'interno di un ospedale è infattibile e praticamente impossibile da attuare nei sistemi primari. Se si tratta di un accesso neces-

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

sario in caso di emergenza non è neppure nell'interesse del paziente. Anche *K3* e *VZK* criticano l'impraticabilità negli ospedali. Come *Posta* segnalano che i diritti di accesso devono valere per interi gruppi oppure limitarsi a uno o più singoli professionisti della salute. Altre soluzioni non sono possibili negli ospedali e provocherebbero situazioni pericolose. Bisogna inoltre assicurare che i professionisti della salute possano accertarsi in qualsiasi momento se hanno un accesso limitato o illimitato a una cartella informatizzata del cliente. Per *USB,* la possibilità del paziente di escludere in generale dall'accesso i nuovi professionisti della salute entrati in un gruppo è un compito troppo complesso. Sarebbe sufficiente inserire determinati professionisti della salute nella lista delle esclusioni. I Cantoni *ZH*, *NW* e *ZG* nonché *ZAD* considerano inattuabile la lettera f per i grandi fornitori di prestazioni. Tutti i membri di un gruppo devono avere accesso alla cartella, altrimenti possono verificarsi situazioni estremamente pericolose. *KSSG* auspica che i nuovi professionisti della salute entrati in un gruppo e il personale ausiliario ricevano automaticamente l'autorizzazione del gruppo, mentre *LUKS*, *Integic*, *HL7*, *IHE* e *medshare* obiettano che la lettera f è troppo complessa da attuare dal punto di vista tecnico e organizzativo. *Integic* scrive inoltre che non è chiaro se il paziente viene informato attivamente quando un professionista della salute trasmette dei diritti di accesso. *IG eHealth*, *PH CH* e *Posta* osservano che un paziente deve aver fiducia nell'organizzazione e nella sua capacità di auto-organizzarsi oppure nei singoli individui. *SBC* auspica in generale una riduzione della complessità. *VAKA* chiede che sia possibile «ereditare» i diritti di accesso e raccomanda di rafforzare l'uso di esclusioni primarie e diritti di accesso individuali invece di volere gestire le dinamiche dei gruppi.

24 partecipanti[23] chiedono lo stralcio dell'articolo 3 lettera f. *Posta* avanza la stessa proposta, ma come alternativa potrebbe immaginarsi che i portali debbano offrire al paziente la possibilità di accordare l'autorizzazione a un gruppo oppure copiare i membri di un gruppo. In questo modo il paziente sa sempre se ha autorizzato singoli individui o un intero gruppo. *IG eHealth* e *PH CH* propongono di riformulare la lettera f come segue: «f. festlegen, dass keine Zugriffsrechte an Gruppen erteilt werden». *Tessaris* chiede che i professionisti della salute che entrano in un gruppo ricevano il diritto di accesso assegnato a questo gruppo solo dopo l'avvenuta comunicazione al paziente. *SPO* chiede se eventuali rappresentanti agiscono con la propria identità e auspica una formulazione più chiara a tale proposito.

Lettera g: *K3* e *VZK* ricordano che i casi di rappresentanza saranno molto frequenti e che l'ordinanza dovrebbe stabilire soprattutto l'età a partire dalla quale un minore può aprire da solo una cartella informatizzata del paziente ed assumerne la piena responsabilità. Analogamente *VGIch* segnala che rimangono da chiarire lo status dei minori e i diritti di accesso nel contesto del diritto di affidamento. Secondo *IG eHealth*, *PH CH*, i Cantone *ZG* e *Posta* questa disposizione è troppo riduttiva. Mentre *IG eHealth* e *PH CH* chiedono un chiarimento su come procedere in caso di perdita di incapacità di discernimento, il Cantone *ZG* e *Posta* desiderano una precisazione sull'impiego degli strumenti d'identificazione, le procure e le revoche.

Il Cantone *TI* chiede di definire la figura del «rappresentante» oppure indicare che si fa riferimento al «rappresentante terapeutico» o alla persona con «diritto di rappresentarla in caso di provvedimenti medici» di cui all'art. 377 del Codice civile svizzero. *Senesuisse* considera inutile e inappropriata la disposizione sui diritti dei rappresentanti. Questo punto è disciplinato in modo molto più chiaro e completo nell'articolo 377 lettera f CC. Si potrebbe quindi inserire un rinvio o un complemento in questo senso. *CURAVIVA* e *Insos* fanno notare che nel caso di pazienti incapaci di discernimento, il loro rappresentante è abilitato a prendere decisioni in tutti gli ambiti nei quali il paziente potrebbe decidere lui stesso se fosse capace di discernimento, in particolare per quanto riguarda i trattamenti medici. Dopo un'adeguata informazione da parte del medico e del personale curante, il rappresentante può approvare o rifiutare un trattamento e, a fortiori, l'apertura di una cartella informatizzata del paziente. Il rappresentante viene attivato unicamente se il paziente incapace di discernimento non ha dato indicazioni precedentemente sulla decisione da prendere attraverso le direttive anticipate del paziente (articoli 377 e 378 CC). Questa regolamentazione è chiara ed esaustiva; consolida armoniosamente quella concernente

[23] 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

la cartella informatizzata del paziente. In questo senso, l'articolo 3 lettera g OCIP è superfluo e incompleto. Tuttavia, visto che non contraddice la legislazione sulla protezione delle persone incapaci di discernimento, può essere lasciato invariato. *HÄ CH* e *ÄTG* rilevano che la lettera g è stata formulata per i pazienti e auspicano che la regolamentazione delle rappresentanze sia estesa anche ai professionisti della salute, in particolare ai medici di base con rappresentanza regionale (in caso di emergenza) o ad ambulatori di gruppo.

Lettera h: *KDSBSON*, *DSBAG*, *privatim* e i Cantoni *FR* e *AG* chiedono se è giusto e voluto che i diritti di accesso possano essere trasferiti solo ai professionisti della salute all'interno della stessa comunità di riferimento, ma non ai professionisti della salute di altre comunità e comunità di riferimento. Se non è così, bisognerebbe modificare il testo dell'ordinanza. Inoltre propongono, come anche il Cantone *ZG*, che la lettera h sia formulata come segue: «h. Gesundheitsfachpersonen dazu ermächtigen, in ihrem Namen Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen. Eine Gesundheitsfachperson kann höchstens jene Zugriffsrechte zuweisen, die sie selber besitzt. Die Gesundheitsfachperson hat die Patientin oder den Patienten über entsprechende Zuweisungen zu informieren». Il Cantone *BE* propone invece la seguente aggiunta: «Die Gesundheitsfachperson hat die Patientin oder den Patienten über entsprechende Zuweisungen zu informieren». *IG eHealth*, *PH CH* e *Posta* chiedono che la trasmissione dei diritti in caso di delega sia impostata come default. Secondo *IG eHealth* e *PH CH* il paziente dovrebbe avere la possibilità di limitare il trasferimento, mentre *Posta* raccomanda di chiarire fino a che punto arriva la catena delle autorizzazioni. *IG eHealth* e *PH CH* avanzano la seguente proposta concreta: «h. kann die Weitergabe von Rechten an weitere Gesundheitsfachpersonen seiner Stammgemeinschaft verbieten oder auf die Weitergabe an maximal eine weitere Gesundheitsfachperson oder Gruppe einschränken». *Tessaris* propone la seguente formulazione della lettera h: «[…] Zugriffsrechte weiteren ihr oder ihm bekannt gegebenen Gesundheitsfachpersonen […]». *VGIch* lamenta una mancanza di chiarezza sullo scopo, la necessità, esempi concreti e iter per l'autorizzazione alla trasmissione dei diritti di accesso. Chiede pertanto di stralciare la lettera h oppure di chiarirla meglio. Il Cantone *AG* è favorevole all'autorizzazione di un professionista della salute a trasferire il suo diritto di accesso ad altri professionisti della salute. Intravede però un certo pericolo per il paziente e chiede pertanto degli esempi. *HÄ CH* e *ÄTG* desidera che siano disciplinati i trattamenti al di fuori della propria comunità di riferimento.

3.1.2 Capitolo 2: Patientenidentifikationsnummer

Art. 4 Format der Patientenidentifikationsnummer

[1] Die Patientenidentifikationsnummer ist elfstellig. Sie setzt sich zusammen aus einer Kontrollziffer und einer zehnstelligen Nummer. Diese darf für eine bestimmte, im Register der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) nach Artikel 71 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG) verzeichnete Person verwendet werden, jedoch keinerlei Rückschlüsse auf diese Person zulassen.

[2] Die Patientenidentifikationsnummer darf nur manuell erfasst werden, wenn eine Kontrollzifferprüfung durchgeführt wird. Das Eidgenössische Departement des Innern (EDI) legt die Vorgaben für den Aufbau der Patientenidentifikationsnummer und die Kontrollzifferprüfung fest.

Secondo *Insel*, è difficile capire dal punto di vista di un ospedale perché non si possa utilizzare il numero AVS per identificare il paziente e perché l'Ufficio centrale di compensazione (UCC) debba generare invece un numero separato. Alla luce delle soluzioni eHealth già affermate all'estero, la prassi scelta per la Svizzera risulta opinabile e costosa. *STSAG* chiede di stabilire che ogni paziente può ricevere un unico numero d'identificazione (NIP). *Bethesda* e *RPB* desiderano che sia disciplinato il momento a partire dal quale un neonato riceve un proprio NIP per la cartella informatizzata del paziente. Propongono che la cartella informatizzata possa essere aperta al più presto possibile e gestita dalla madre o dal padre come rappresentante.

Capoverso 1: *DSBAG*, *privatim* e i Cantoni *ZG* e *SZ* scrivono che dal punto di vista della protezione dei dati è positivo che il NIP non permetta di risalire alla persona. *CMC*, e *BüAeV*, *GAeSO* e *KAeG SG* si associano a questa posizione. Per loro si pone però la questione del se e perché il NIP debba essere

memorizzato presso l'UCC. Bisognerebbe inoltre evitare che l'UCC possa attribuire un NIP a una determinata persona. 7 partecipanti[24] dichiarano che sarebbe preferibile adottare gli standard internazionali, come GS1-GSRN, piuttosto che una soluzione svizzera isolata. *ICTS*, *IG eHealth* e *PH CH* avanzano la seguente proposta di formulazione per l'articolo 4 capoverso 1: «Die PID ist nach internationalen Standards für PID aufgebaut. Diese darf […]». *Stiftung refdata*, *GS1* e *SSIM* scrivono che la cifra di controllo del GS1-GSRN è calcolata sulla base dell'algoritmo Modulo-10, lo stesso di quello proposto nell'attuale progetto per il calcolo della cifra di controllo. Le specifiche tecniche ISO 18530, riprese nel 2015 da CEN, indicano come è composto un tale codice (GSRN) e come può essere utilizzato. Questi partecipanti adducono anche un esempio di struttura del GSRN e rimandano al grafico contenuto nel documento dell'indagine conoscitiva. *Economiesuisse* segnala che la soluzione proposta non permette per esempio ai frontalieri di aprire una cartella informatizzata del paziente e chiede di eliminare questa lacuna.

Art. 5 Antrag auf Zuweisung der Patientenidentifikationsnummer

[1] Die Patientenidentifikationsnummer wird auf Antrag einer Stammgemeinschaft durch die ZAS vergeben.

[2] Die Stammgemeinschaft stellt der ZAS folgende Daten für die Vergabe der Patientenidentifikationsnummer zur Verfügung:

a. den Namen;

b. die Vornamen;

c. das Geschlecht;

d. das Geburtsdatum;

e. die Versichertennummer nach Artikel 50c AHVG

[3] Reichen die gemeldeten Daten für die Vergabe nicht aus, so kann die ZAS bei der Stammgemeinschaft zusätzliche Daten verlangen.

Insel ripete il suo commento sull'articolo 4. *VAKA*[25] propone l'obbligo di comunicare alla comunità di riferimento ogni cambiamento dei dati demografici in modo automatico e per via elettronica. 6 Cantoni[26] chiedono per motivi di sicurezza e costo che sia possibile impiegare il NIP all'interno di una comunità (nei sistemi primari) per accertare in maniera univoca l'identità dei pazienti. I Cantoni *NE*, *GE*, *JU*, *VS* e *VD* si informano sui termini e i costi per la generazione di un NIP e la seguente apertura di una cartella informatizzata del paziente. L'ideale sarebbe un «*mode transactionnel*» per ottenere un NIP e creare una cartella informatizzata del paziente direttamente a partire da un sistema primario. La domanda per la creazione di un NIP deve avvenire per via elettronica ed essere disponibile nel processo di creazione della cartella informatizzata del paziente. Secondo i suddetti Cantoni è necessario poter disporre del NIP immediatamente.

Capoverso 1: *VAKA*, *K3* e *VZK* fanno notare che, secondo il testo in esame, per aprire una cartella informatizzata del paziente bisogna essere assicurati in Svizzera. In tal caso però le persone senza NAVS13 (p. es. turisti, diplomatici, frontalieri ecc.) non possono aprire una cartella. Mentre *K3* e *VZK* chiedono un esame di tale aspetto, *VAKA* e il Cantone *AG* auspicano l'inclusione di tutti i gruppi di persone nell'attribuzione del NIP. Anche *Posta* e *H+* chiedono che il NIP possa essere rilasciato anche a persone che non sono dotate del NAVS13. *H+* desidera inoltre che le comunità di riferimento possano impiegare la piattaforma di trasmissione sedex per domandare l'attribuzione del NIP all'UCC. Solo in questo modo si può garantire un processo di notifica elettronico efficiente e standardizzato. *OFAC* domanda che ne è dei pazienti che desiderano aprire una cartella informatizzata, ma non dispongono del NAVS13. *IG eHealth* e *PH CH* propongono la seguente aggiunta all'articolo 5 capoverso 1: «[...] vergeben. Die ZAS stellt sicher, dass auch nicht obligatorisch Versicherte nach Art. 1 AHVF im zentralen Versichertenregister ohne AHV13 geführt werden können und dass die Stammgemeinschaften für die Personen eine PID beantragen dürfen». *K3* e *VZK* auspicano che il processo di cui al capoverso 1 sia mantenuto il più snello possibile. *ASPS* e *Spitex* propongono il rilascio di un NIP a tutte le persone con

[24] GS1, Stiftung refdata, SSIM, ICTS, IG eHealth, PH CH, economiesuisse

[25] Senza RPB

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

un numero AVS, in modo da facilitare la registrazione. I fornitori di prestazioni che aprono una nuova cartella elettronica del paziente o richiedono un NIP tramite la comunità di riferimento non dovrebbero incorrere in costi aggiuntivi.

Capoverso 2: *Santésuisse* auspica che, oltre alle comunità di riferimento, anche l'Identity-Provider possa trasmettere all'UCC i dati citati nel capoverso 2. *BRH* è del parere che il numero AVS, come parte del NIP, pregiudichi la protezione dei dati e chiede che l'identità del paziente sia separata da quella dell'assicurato. *PharmaSuisse* obietta che secondo l'articolo 4 capoverso 1 il NIP non consente di risalire alla persona, ma che una comunità di riferimento, nel momento in cui chiede l'attribuzione del NIP, potrebbe stabilire un tale collegamento con il numero AVS. Si chiede pertanto se nel dispositivo normativo non sia prevista a tale proposito una clausola di segretezza.

Capoverso 3: *K3* e *VZK* si chiedono se la comunità di riferimento non debba disporre di ulteriori dati sull'utente di una cartella informatizzata del paziente in caso di richiesta di maggiori informazioni. Propongono che l'UCC invii automaticamente alla comunità di riferimento i cambiamenti di indirizzo, nome, ecc. 6 partecipanti[27] desiderano una precisazione su quali sono i dati in questione. *Medshare* chiede in generale una definizione del termine «dati». Questa parola è utilizzata ripetutamente nell'ordinanza, ma certe volte con interpretazioni diverse. *Tessaris* parte dal presupposto che il capoverso 3 includa i casi di persone che si trovano in Svizzera (p. es. come turisti) e non dispongono di un numero di assicurato secondo l'articolo 50c LAVS. *KSSG* fa notare che bisognerebbe descrivere il servizio di raccolta di maggiori informazioni e che una richiesta manuale è troppo onerosa.

Art. 6	Abfrage der Patientenidentifikationsnummer
Gemeinschaften und Stammgemeinschaften können die Patientenidentifikationsnummer bei der ZAS über ein elektronisches Abrufverfahren abfragen.	

ASPS e *Spitex* reiterano il loro parere sull'articolo 5. *HL7*, *IHE* e *Integic* auspicano un chiarimento sui dati necessari per la consultazione e propongono i dati di cui all'articolo 5 capoverso 2. *K3* e *VZK* ritengono che la consultazione dovrebbe essere possibile anche per i fornitori di prestazioni e i professionisti della salute. Altrimenti, in situazioni di emergenza, non si potrebbero reperire i dati necessari a causa del mancato accesso alla cartella informatizzata. *Posta* segnala che il NIP potrebbe esser utilizzato anche per la comunicazione fra i fornitori di prestazioni e il paziente. Il NIP dovrebbe essere valido e rimanere invariato sull'arco di tutta la vita. Chiede inoltre di verificare se il NIP possa essere impiegato anche ad altri scopi e se questi richiedono delle basi giuridiche nell'OCIP.

Art. 7	Annullierung
[1] Wird das elektronische Patientendossier aufgehoben, so wird die Patientenidentifikationsnummer in der Identifikationsdatenbank der ZAS annulliert.	
[2] Eine annullierte Patientenidentifikationsnummer darf nicht erneut vergeben werden.	

KSSG rimanda alla sua osservazione sull'articolo 5, dove chiedeva una descrizione più dettagliata di questo tipo di servizio. *VAKA* appoggia la posizione espressa da *Bethesda* e *RPB* sull'articolo 4. *Lovis* sottolinea la necessità di mantenere il NIP e che l'emittente ne garantisca l'unicità. Analogamente, il Cantone *TI* e *FMH* chiedono di modificare l'art. 7 in modo da poter conservare il NIP anche dopo la chiusura della cartella informatizzata del paziente e riassegnarlo allo stesso paziente in caso di riapertura. Il Cantone *AG* fa notare a proposito degli articoli 5 e 7 che la comunità di riferimento deve accollarsi un notevole onere se deve chiedere l'annullamento del NIP al momento della chiusura della cartella informatizzata del paziente. *Medshare* osserva che la cartella informatizzata appartiene al paziente dal momento dell'apertura fino alla morte. Per questo motivo nessuno ha il diritto di cancellare dei dati. Il NIP deve essere quindi annullato dall'UCC su richiesta del paziente. In tal caso va annullato anche in tutti gli MPI. 6 Cantoni[28] evidenziano che il NIP serve anche alla comunicazione fra le comunità. Un

[27] HL7, IHE, VAKA, Posta, ZG, medshare
[28] FR, GE, VS, VD, JU, NE

paziente che ha traslocato potrebbe essere iscritto presso due comunità di riferimento. Il suo NIP non deve mai essere annullato. Inoltre si perderebbero le corrispondenze fra il MPI della comunità di riferimento e l'MPI di altre comunità. Così come il numero NAVS13 non cambia in linea di massima mai per una persona, anche il NIP deve essere mantenuto dopo la soppressione della cartella informatizzata del paziente. Il suo mantenimento è il presupposto per l'interoperabilità. A un NAVS deve corrispondere un unico NIP. Questi partecipanti propongono la seguente formulazione per l'articolo 7 capoverso 1: «[…] son numéro d'identification est conservé». «En cas de création ultérieure d'un nouveau dossier électronique du patient, le numéro d'identification initial doit être repris».

Capoverso 1: *HL7*, *IHE*, *BINT* e *Integic* fanno notare che il NIP della cartella informatizzata del paziente dovrebbe essere annullato anche in tutti gli MPI. Raccomandano pertanto di stralciare questo articolo. Se questo principio è mantenuto bisognerebbe correggere anche tutti gli MPI, registry e repository. *BINT* e *Integic* chiedono congiuntamente che le comunità di riferimento informino tutte le comunità certificate e l'UCC sulla chiusura di una cartella informatizzata del paziente.

Capoverso 2: *BINT* e *Integic* auspicano che per un periodo limitato le comunità e le comunità di riferimento possano consultare i NIP annullati presso l'UCC attraverso un sistema elettronico di consultazione. *Posta* propone di citare esplicitamente che il capoverso 2 vale anche per lo stesso paziente. *ASPS* e *Spitex* raccomandano invece che in caso di riapertura di una cartella informatizzata del paziente il «vecchio» NIP sia riattivato. *BFH* ritiene opportuno aggiungere un capoverso 3 che specifichi come gestire i numeri nel caso in cui dopo la cancellazione venga riaperta una cartella informatizzata del paziente.

3.1.3 Capitolo 3: Gemeinschaften und Stammgemeinschaften

Sezione 1: Gemeinschaften

Art. 8 Verwaltung

Gemeinschaften müssen die ihnen angehörenden Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen verwalten. Dazu müssen sie insbesondere:

a. deren Eintritt und deren Austritt regeln;

b. die Gesundheitsfachpersonen identifizieren;

c. die Aktualisierung der Daten im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 sicherstellen;

d. sicherstellen, dass Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier nur gültige Identifikationsmittel verwenden, die von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurden;

e. sicherstellen, dass die Zusammensetzung der Gruppen von Gesundheitsfachpersonen für Patientinnen und Patienten jederzeit nachvollziehbar ist;

f. die Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informieren.

VGIch ripete in questa sede il suo commento sull'articolo 2 capoverso 4 e sull'articolo 3 lettera f riguardo alla questione dei gruppi. 16 partecipanti[29] criticano l'elevato onere amministrativo legato alle disposizioni dell'articolo 8. *VAKA* chiede una modifica per ridurre l'onere. *Physioswiss*, *ASI*, *SWOR* e *FSAS* raccomandano di disciplinare per tempo i processi e di implementarli in modo conforme alle esigenze pratiche. Bisognerebbe anche predisporre maggiori risorse. *PharmaSuisse* segnala che il team di una farmacia dovrebbe ricevere, come gruppo, l'autorizzazione del paziente ad accedere alla sua cartella informatizzata, altrimenti anche dei processi banali diventerebbero estremamente complessi. Il Cantone *TI* sottolinea l'importanza della possibilità per il paziente di concedere l'accesso ai propri dati a un gruppo di professionisti della salute che collaborano fra loro e rimanda a questo proposito all'esperienza pratica del progetto «reTIsan».

[29] ASPS, Spitex, Insel, VAKA, RPB, Physioswiss, PKS, UDC, ASI, SWOR, FSAS, Posta, STSAG, HÄ CH, ÄTG

IG eHealth und *PH CH* si chiedono come garantire che il paziente conosca l'identità del personale ausiliario anche in diverse comunità / comunità di riferimento e possa verificare a chi accorda l'accesso. Propongono la seguente formulazione per l'articolo 8: «[…] Gesundheitsfachpersonen, Hilfspersonen und Gruppen von Gesundheitsfachpersonen verwalten. […]». Basandosi sulle affermazioni riportate a pagina 15 del rapporto esplicativo sull'OCIP (versione tedesca) e nel messaggio sull'articolo 3 LCIP, *HIN* parte dal presupposto che un professionista della salute possa delegare il trattamento della cartella informatizzata del paziente al suo personale ausiliario, a meno che il paziente non lo abbia espressamente vietato. Raccomandano che il paziente, al momento dell'autorizzazione alla registrazione dei suoi dati nella cartella informatizzata del paziente, consenta ai professionisti della salute da lui autorizzati di ricorrere a personale ausiliario secondo il loro apprezzamento. *HIN* rimanda alle sue proposte di aggiunta sugli articoli 2 e 3 e, se non verranno accolte, chiede una definizione più precisa di quali professioni / formazioni rientrano nella nozione di «professionista della salute». All'articolo 8 *HIN* propone di aggiungere due nuovi capoversi: «g. sicherstellen, dass die zugeordneten Hilfspersonen von Gesundheitsfachpersonen für Patientinnen und Patienten jederzeit nachvollziehbar sind;» e «h. die Patientinnen und Patienten über das erstmalige Zuordnen von Hilfspersonen von Gesundheitsfachpersonen informieren». Secondo *KSSG* l'articolo 8 deve esser completato in modo che siano soddisfatti i seguenti criteri: l'UFSP definisce le categorie professionali che sono considerate «professionisti della salute»; il Cantone definisce i registri federali o cantonali con i quali deve essere verificata l'abilitazione dei professionisti della salute; tutte le categorie professionali che non sono designate espressamente come professionisti della salute sono da considerarsi personale ausiliario ai sensi del numero 1.3 CTO. Infine bisognerebbe aggiungere una lettera con il seguente tenore: «Das BAG kann Gemeinschaften auf Antrag erlauben, aus Gründen der Übersichtlichkeit für die Patientinnen oder die Patienten nur einen Teil der GFS nach aussen zu publizieren».

STSAG avverte che l'autenticazione a due fattori è difficilmente attuabile. Bisognerebbe verificare l'introduzione di un'infrastruttura simile all'HIN-Access-Gateway come equivalente ammesso per l'accesso autentificato. Riguardo alla gestione dei professionisti della salute, *HÄ CH* e *ÄTG* chiedono una semplificazione. Propongono due modalità di gestione: un «professional-mode» per tutti coloro che vogliono addentrarsi nella materia nonché gestire e impostare tutto da soli, e un «easy-mode» che permetta di gestire con un «click» e per default tutte le impostazioni in un modo ragionevole e piuttosto libero (ancora da discutere).

I Cantoni *NW*, *ZG* e *ZH* nonché *ZAD* ritengono che non si dovrebbero usare disposizioni indirette, bensì disciplinare direttamente cosa devono fare le comunità. I Cantoni *ZG* e *ZH* nonché *ZAD* avanzano le seguenti proposte di formulazione per l'articolo 8, alle quali aggiungono alcune osservazioni: «Gemeinschaften verwalten die ihnen angehörenden Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen. Dabei gelten folgende Grundsätze:
a. Die Gemeinschaft regelt, wie Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen ihr beitreten oder sie verlassen [Cosa devono disciplinare esattamente le comunità? È necessario disciplinare in dettaglio gli ingressi e le uscite? È veramente necessaria questa disposizione?]
b. Die Gemeinschaft identifiziert die Gesundheitsfachpersone [Strumenti d'identificazione? Cosa deve verificare esattamente la comunità? Quando identifica?]
c. Die Gemeinschaft aktualisiert die Daten im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Art. 40.
d. Die Gemeinschaft lässt Zugriffe auf das elektronische Patientendossier nur zu, wenn dafür ein gültiges Identifikationsmittel verwendet wird, das von einem nach Art. 30 zertifizierten Herausgeber stammt.
e. Die Gemeinschaft informiert Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen.»

Lettere b e c: *ASPS* e *Spitex* fanno notare che in Svizzera non esiste finora un registro completo per infermieri diplomati. La legge sulle professioni sanitarie prevede la creazione di un registro nazionale, ma visto che non potrà entrare in vigore all'inizio del 2017, è necessaria una soluzione transitoria. L'OCIP dovrebbe prevedere un registro completo o definire un processo transitorio affinché anche gli

infermieri diplomati possano essere certificati. L'iscrizione nel registro nazionale dovrebbe essere gratuita ed esser gestita da un istituto indipendente. Analogamente anche *ASI*, *FSAS*, *SWOR* e *H+* avvertono che un'identificazione univoca dei professionisti della salute, soprattutto nell'ambito delle cure infermieristiche, rappresenta una grossa sfida per le strutture sanitarie e le comunità. Per questo motivo si rende necessario un registro professionale nazionale e completo per assicurare un'identificazione affidabile. *HL7*, *IHE*, *Integic* e *medshare* propongono la seguente precisazione alla lettera b: «die Gesundheitsfachpersonen authentifizieren und eindeutig identifizieren». Per la lettera c desiderano che sia definita la periodicità. Il Cantone *AG* chiede chiarimenti sull'identificazione del personale ausiliario e una precisazione sul personale ausiliario con diritto di accesso.

Lettera d: *VGIch* e *Insel* obiettano che, secondo questo articolo, un ospedale dovrebbe farsi certificare come emittente di strumenti d'identificazione oppure impiegare firme qualificate per i sistemi primari allacciati. *Insel* chiede lo stralcio della lettera d, mentre *VGIch* osserva che la scelta di procedure adeguate per l'identity management dei collaboratori dell'ospedale spetta in fondo agli ospedali stessi. Secondo *KSSG* bisognerebbe precisare al numero 1.4 CTO, che l'identità dei professionisti della salute e del personale ausiliario può essere archiviata elettronicamente in modo sicuro e potrebbe essere richiamata con una severa autenticazione per l'accesso alla cartella informatizzata del paziente.

HÄ CH e *ÄTG* propongono di mantenere un solo livello per l'accesso al sistema primario, conformemente alla prassi abituale, e di introdurre le caratteristiche di sicurezza certificate a due livelli solo sul piano secondario, quando il sistema primario entra in contatto con la cartella informatizzata del paziente per richiamare o archiviare dati. Sarebbe altresì ipotizzabile che solo determinate postazioni all'interno di un ambulatorio entrino in contatto con la cartella informatizzata del paziente e che solo lì vengano installati i relativi dispositivi di sicurezza.

Lettera e: Secondo 6 Cantoni[30] i pazienti non dovrebbero poter accedere in tempo reale alla composizione dei gruppi, ma conoscere in qualsiasi momento (attraverso i protocolli di accesso) quale professionista della salute appartenente a un gruppo ha avuto accesso ai suoi dati. L'articolo 8 lettera e deve essere stralciato. Anche il Cantone *TI* si esprime contro l'aggiornamento in tempo reale e a favore dello stralcio della lettera e. La stessa richiesta è avanzata anche da *STSAG*, dal Cantone *ZG*, da *K3* e *VZK*. *BFH* propone come priorità assoluta di ridurre i gruppi in modo pragmatico, come avviene già oggi, al medico primario «e il suo team». Come secondo priorità – o se viene mantenuta la lettera e – il paziente dovrebbe essere informato del fatto che anche i professionisti della salute a cui ha negato il diritto di accesso possono prendere visione dei dati attraverso il loro sistema clinico (primario). *KSSG* ritiene che l'esclusione di personale ausiliario impedisce la tracciabilità per i pazienti. Ne consegue una contraddizione con il numero 1.3.2.2 CTO. Se questa disposizione dovesse risultare veramente necessaria, bisognerebbe indicare anche il personale ausiliario nella cartella informatizzata del paziente e sincronizzarlo con i servizi centrali. Ciò non è certamente l'obiettivo. Per questo motivo si chiede una gestione delle autorizzazioni a livello di gruppo o di organizzazione, con la possibilità di escludere esplicitamente singoli professionisti della salute. *ASI*, *FSAS* e *SWOR* criticano la marea di informazioni che risulterebbe se il paziente venisse informato di ogni cambiamento di personale nel team curante. Inoltre questa trasparenza è da considerare critica anche per i professionisti della salute. *VGIch* chiede che vengano citati i criteri per la selezione del gruppo. *HÄ CH* e *ÄTG* considerano troppo complessa la gestione dei professionisti della salute (lett. e ed f). Temono che i pazienti ne vengano scoraggiati e finiscano per non autorizzare l'accesso al medico necessario.

Lettera f: 16 partecipanti[31] avvertono che un'informazione attiva sui cambiamenti dei professionisti della salute all'interno di gruppi, soprattutto di grandi strutture, genera un'inutile marea di informazioni. 16 partecipanti[32] chiedono pertanto lo stralcio della lettera f. *Insel*, *K3, VZK* e *LUKS* adducono come motivo anche il conflitto con la protezione dei dati del personale ospedaliero. *KSSG*, *SSIM*, *FMH* e *LUKS* chiedono la soppressione del dovere di informazione attiva. Secondo *Insel* è sufficiente che il paziente possa

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

accedere a queste informazioni in caso di bisogno. *SCH* propone di aggiungere l'opzione «opt-in» con il seguente complemento alla lettera f: «die Patientinnen und Patienten mittels einer Opt-in-Option über die Eintritte […]». Anche *Economiesuisse*, i Cantoni *ZG*, *NW* e *ZH* nonché *ZAD* sono a favore di una limitazione dell'informazione mediante la soluzione «opt-in». *HL7*, *IHE* e *Integic* scrivono che gli ingressi e le uscite di professionisti della salute devono essere notificati solo quando riguardano i gruppi ai quali il paziente ha concesso il diritto di accesso. Sono del parere che un «muting» delle notifiche potrebbe rendere questo sistema molto più accettabile. *Integic* raccomanda inoltre di concretizzare la conservazione dei protocolli dopo l'uscita. Per *PKS* e *UDC* è sufficiente che i pazienti possano rintracciare in qualsiasi momento gli accessi effettivi alla loro cartella informatizzata. L'intero ospedale dovrebbe riceve l'autorizzazione come gruppo. *VGIch* scrive che il processo «ingresso di professionisti della salute» dovrebbe essere attivato per tutti i professionisti della salute che entrano in una struttura sanitaria. Secondo il rapporto esplicativo è possibile delegare il processo di ingresso alle strutture sanitarie. Questa disposizione dovrebbe essere interpretata in modo tale da permettere alle strutture sanitarie di determinare da sole chi entra attivamente. Le CTO dovrebbero essere modificate di conseguenza.

Art. 9 Datenhaltung und Datenübertragung

[1] Gemeinschaften müssen sicherstellen, dass:

a. die von den Gesundheitsfachpersonen im elektronischen Patientendossier erfassten Daten nach 10 Jahren vernichtet werden;

b. bei einer Aufhebung des elektronischen Patientendossiers nach Artikel 20 Absatz 1 sämtliche Daten vernichtet werden;

c. Daten des elektronischen Patientendossiers nur in Ablagen gespeichert werden, die ausschliesslich dafür vorgesehen sind.

[2] Sie haben auf Verlangen der Patientin oder des Patienten:

a. bestimmte auf diese oder diesen bezogene Daten im elektronischen Patientendossier nicht zu erfassen;

b. Daten nach Absatz 1 weitere 10 Jahre verfügbar zu machen;

c. bestimmte auf diese oder diesen bezogene Daten aus dem elektronischen Patientendossier zu vernichten.

[3] Das EDI legt die weiteren Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers fest. Es regelt insbesondere:

die Umsetzung der Artikel 1 und 2 Absatz 5;

a. die zu verwendenden Metadaten;

b. die zu verwendenden Austauschformate;

c. die zu verwendenden Integrationsprofile;

d. die Vorgaben betreffend die Protokolldaten.

[4] Das EDI kann bestimmen, dass die Vorgaben nach Absatz 3 in der Originalsprache veröffentlicht werden und auf eine Übersetzung in die Amtssprachen verzichtet wird.

[5] Das Bundesamt für Gesundheit (BAG) kann die Vorgaben nach Absatz 3 dem Stand der Technik anpassen.

HÄ CH e *ÄTG* chiedono se possono essere adite le vie legali anche in caso di non-accesso alla cartella informatizzata (p. es. per omissione) e desiderano che venga elaborata una perizia legale per chiarire i punti ancora in sospeso dal punto di vista dei pazienti e dei professionisti della salute. *PKS* e *UDC* criticano che le disposizioni riguardanti la memorizzazione dei dati sono dispendiose da applicare perché non corrispondono ai processi in uso negli ospedali. In particolare la memorizzazione separata dei dati non offre alcun valore aggiunto ai pazienti, mentre causa notevoli costi supplementari alle comunità.

Capoverso 1: *IG eHealth* e *PH CH* osservano che i termini e le definizioni utilizzati nell'articolo 9 sono imprecisi. Chiedono inoltre di aggiungere una lettera del seguente tenore: «Daten im elektronischen Patientendossier einen, von den Gesundheitsfachpersonen erfassten Primärdaten unabhängigen Lebenszyklus haben». Riguardo al capoverso 1 lettera c, *ISSS* propone l'aggiunta di una lettera d, poiché l'attuale testo non formula dei requisiti sulla tenuta regolare dei dati né esige una prova dell'integrità,

mentre altre leggi contengono prescrizioni concrete a tale proposito (p. es. ordinanza sui libri di commercio [Olc], art. 3). L'ordinanza dovrebbe prevedere che i dati della cartella informatizzata del paziente siano conservati in modo da consentire una prova di integrità, cioè permettere di constatare una successiva modifica (p. es. modifica da parte dell'utente, disfunzione tecnica o abuso/cyber-attacco).

Capoverso 1 lettera a: *CDS* e 18 Cantoni[33] sono del parere che la cancellazione per default dei dati medici dopo 10 anni non sia nell'interesse del paziente né abbia un senso dal punto di vista dei processi medico-terapeutici. *CDS* e 8 Cantoni[34] desiderano dare la possibilità ai pazienti di stabilire una durata di conservazione dei dati superiore a 10 anni. Il Cantone *ZH* e *ZAD* chiedono di rielaborare le disposizioni sulla durata della conservazione dei dati. Il termine di conservazione dovrebbe essere molto più lungo (p. es. a vita). 8 partecipanti[35] segnalano che occorre chiarire il momento da cui decorre il termine di 10 anni. Oltre alla questione della decorrenza, il Cantone *ZG*, *KDSBSON*, e *DSBAG* e *privatim* sostengono che la lettera a dovrebbe disciplinare anche l'informazione dei pazienti prima della cancellazione dei dati. Secondo *HÄ CH* e *ÄTG* anche il medico curante (di base) dovrebbe essere informato per tempo prima della prevista cancellazione. 6 Cantoni[36] osservano che il testo proposto non rispetta l'articolo 40 capoverso 1 della legge sugli agenti terapeutici (LATer) nella revisione approvata dal Parlamento il 18 marzo 2016, secondo la quale i dati sul trattamento del sangue e dei suoi derivati devono essere conservati per 30 anni.

11 partecipanti[37] chiedono lo stralcio della lettera a. *VAKA* aggiunge che devono essere soppressi anche i relativi commenti nel rapporto esplicativo e tutte le altre indicazioni di scadenze fisse per la conservazione di documenti. *Economiesuisse* scrive che nella cartella informatizzata del paziente devono essere registrati, senza eccezioni, tutti i dati rilevanti per la salute e la sicurezza. *Insel* ritiene che il termine massimo di 10 anni non sia opportuno e ricorda che i termini di conservazione cantonali sono diversi. Anche *BRH* rimanda alle disposizioni cantonali e chiede che, analogamente alla legislazione bernese, la durata di conservazione sia estesa a 10 anni dopo l'ultima consultazione. *K3* e *VZK* segnalano che questa disposizione è in contraddizione anche con le norme vigenti nel Cantone di Zurigo. Il Cantone *AG* evidenzia che il termine di 10 anni per la conservazione dei dati rilevanti per il trattamento nella cartella informatizzata del paziente (sistema secondario) è compatibile con la legge argoviese sulla sanità, la quale prevede un termine di 10 anni per la conservazione della cartella clinica. *Posta* chiede infine che il paziente possa decidere sulla cancellazione e che non si prendano come riferimento i termini di conservazione dei Cantoni. Il Cantone *NW* obietta che la conservazione separata dei dati è inutile perché i dati degni di particolare protezione vengono già archiviati nel SIC dai grandi fornitori di prestazioni. La conservazione separata dei dati deve essere sostituita da prescrizioni di sicurezza tecniche. *K3* e *VZK* sono contrari alla cancellazione dei dati dopo 10 anni perché la cartella informatizzata del paziente dovrebbe funzionare possibilmente per tutta la vita. Anche *H+*, *ASI*, *FSAS* e *SWOR* ritengono che una cartella debba restare a disposizione dei cittadini per tutta la vita, nel caso in cui vogliano riattivarla. Come alternativa propongono che i dati vengano distrutti dietro preavviso solo se per 10 anni non c'è stato alcun accesso alla cartella informatizzata del paziente, oppure in caso di chiusura della cartella o di decesso. Questa disposizione dovrebbe essere impostata come l'articolo 20 per l'intera cartella informatizzata del paziente. *STSAG* chiede che la cancellazione e la soppressione dei dati siano decise unicamente dal paziente, oppure che avvengano automaticamente dopo 10 anni di inattività. *Santésuisse* avverte che stabilire un limite temporale può provocare una perdita di dati con possibili conseguenze negative dal punto di vista medico. *KSOW* segnala che i dati registrati dai pazienti vengono cancellati dopo 10 anni e s'informa se vengono registrati anche altri dati. I dati sanitari soggetti a scadenze più lunghe non dovrebbero essere cancellati dopo 10 anni (p. es. malattie croniche). Il termine di conservazione dei dati rilevanti dovrebbe essere stabilito caso per caso.

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

6 Cantoni[38] avanzano la seguente proposta di formulazione per la lettera 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* e *ÄTG* desiderano un prolungamento del termine da 10 ad almeno 15 o più anni. *IG eHealth* e *PH CH* propongono la seguente formulazione della lettera a: «dass der Patient informiert wird, wenn von einer Gesundheitsfachperson im elektronischen Patientendossier erfasste Daten 10 Jahre nicht mehr abgerufen wurden». *PharmaSuisse* raccomanda di trattare alla stessa stregua tutti i dati della cartella informatizzata del paziente e di completare pertanto la lettera a come segue: «[…] vernichtet werden, sofern diese Möglichkeit nicht vom Patienten ausgeschlossen wurde». Per coerenza, questa possibilità dovrebbe essere inserita fra le opzioni dell'articolo 3: «i. Die automatische Vernichtung der im elektronischen Patientendossier erfassten Daten nach 10 Jahren (gemäss Art. 9, Abs. 1, Bst. a) auszuschliessen». *SCH* propone la seguente aggiunta: «[…] nach 10 Jahren vernichtet werden können». *Moeri* chiede di evitare la distruzione automatica dopo 10 anni e di applicare invece una cancellazione implicita secondo l'articolo 20 capoverso 1. Questa scadenza dovrebbe valere solo per il sistema primario, come auspica anche il Cantone *BE*. *HL7*, *IHE*, *BINT*, *Bleuer* e il Cantone *SG* scrivono che la cancellazione deve essere lasciata alla discrezione del paziente. In base al paradigma della totale sovranità sui dati, la cancellazione automatica da parte dei gestori dopo 10 anni è inammissibile. Secondo il Cantone *SG* le comunità devono garantire che i dati registrati nella cartella informatizzata del paziente siano cancellati allo scadere di un termine scelto liberamente dal paziente. Quest'ultimo può anche decidere che i dati siano memorizzati a tempo indeterminato / per tutta la vita. *Posta* propone la possibilità di una cancellazione manuale di documenti che non sono più rilevanti (da parte del paziente o del medico di base). Come alternativa si potrebbe considerare anche una memorizzazione permanente con diverse opzioni di configurazione per il periodo di scadenza. *Physioswiss* ricorda che i dati medici importanti devono restare a disposizione finché il paziente non ne consente la cancellazione. Al momento dell'apertura della cartella informatizzata, il paziente dovrebbe avere la possibilità di scegliere un termine di conservazione. La conservazione dei dati dovrebbe altresì essere assicurata anche al di là dell'esistenza di una comunità, una richiesta avanzata anche da *FMH*. *LUKS* chiede che, salvo istruzioni contrarie del paziente, i documenti siano mantenuti nella cartella informatizzata del paziente fino alla sua morte. *Tessaris* scrive che i dati registrati dai professionisti della salute nella cartella informatizzata del paziente siano cancellati o il loro accesso bloccato permanentemente allo scadere di un termine stabilito dal professionista curante in accordo con il paziente. *FMH* osserva che la disposizione della lettera a contrasta con lo scopo della cartella informatizzata del paziente e propone che il paziente debba essere consultato prima di un'eventuale cancellazione di dati. Una cancellazione dovrebbe essere possibile solo se il paziente vi acconsente o sopprime la cartella. Sulla stessa falsariga, *VGIch* ritiene che l'obbligo di conservazione cessi solo al momento della soppressione della cartella su richiesta del paziente oppure alla morte di quest'ultimo. Secondo il Cantone *TI* la lettera a dovrebbe essere modificata indicando che i dati registrati siano conservati fino alla soppressione della cartella informatizzata del paziente. *SSIM* obietta che una distruzione generale dei dati dopo 10 anni non ha senso e propone che un paziente possa richiedere che i dati siano cancellati dopo un periodo di conservazione minimo (variabile in funzione del Cantone e della tipologia di dati).

Capoverso 1 lettera b: *Tessaris* scrive che la lettera b deve essere adeguata alla sua proposta di modifica della lettera a. I dati dovrebbero essere disponibili anche allo scadere del termine stabilito dal professionista della salute curante. *SCH* propone di sostituire il verbo «vernichten» con la seguente definizione: «[…] Daten sind gemäss aktuellem Stand der Technik unwiderruflich zu löschen». *PharmaSuisse* raccomanda un'ulteriore lettera per il capoverso 1 con il seguente tenore: «im Fall der Vernichtung von Daten im elektronischen Patientendossier gemäss Buchstabe a, muss die Patientin oder der Patient mindestens 3 Monate im Voraus informiert werden». Secondo *FMH* bisognerebbe fare in modo che il paziente possa ripristinare i dati per proprio conto, invece di cancellarli. Se il paziente torna sulla sua decisione, potrà recuperare i dati. *Medshare* propone una nuova formulazione della lettera b in vista della nuova regolamentazione ancora da adottare sulla successione digitale. In effetti i dati verrebbero cancellati solo dopo la morte e solo nel caso in cui gli eredi non chiedano la conservazione della cartella

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

entro un termine ancora da definire. 7 Cantoni[39] chiedono lo stralcio della lettera b.

Capoverso 1 lettera c: *HL7*, *IHE* e *SSIM* chiedono di precisare cosa s'intende per «Ablagen (…), die ausschliesslich dafür vorgesehen sind». Se s'intende una separazione fisica, bisognerà definirla. In generale bisogna chiedersi se un'ordinanza debba occuparsi dei livelli server o di tecnologie di memorizzazione. Le separazioni fisiche di una cartella virtuale, tenuta su infrastrutture virtuali, è una contraddizione in termini. Per *IG eHealth* e*SCH* non è chiaro cosa s'intenda con il termine «ausschliesslich», perché potrebbe essere interpretato come doppio archivio, il che non sarebbe opportuno. Propongono di stralciare il termine «ausschliesslich» dalla lettera c. *VGIch* chiede un chiarimento su «dafür vorgesehene Ablagen» e sui casi eccezionali tecnicamente motivati (vedi rapporto esplicativo). Gli ospedali potrebbero essere privati del notevole vantaggio dei repository IHE-compatibili, che consentirebbero una registrazione diretta dei documenti locali. Bisognerebbe consentire espressamente alle comunità di riferimento di tenere un repository secondario centrale con copie provenienti dal sistema primario. Inoltre occorre stilare un elenco esaustivo dei casi tecnici eccezionali e, come soluzione alternativa, autorizzare la registrazione diretta di documenti locali nei repository dei fornitori di prestazioni. Anche *medshare* chiede di precisare cosa s'intende con «Ablagen (…), die ausschliesslich dafür vorgesehen sind».

VAKA obietta che questa limitazione elimina le possibilità di processi funzionali utili e causa ridondanze, che a loro volta fanno lievitare i costi. Inoltre non viene rispettato il principio della conservazione decentrale dei dati come prevista nel modello di base. In questo contesto le comunità e i loro modelli aziendali verrebbero privati di aspetti e vantaggi importanti derivanti dall'impiego mirato. *VAKA* chiede lo stralcio della lettera c, incluse le relative prescrizioni nelle CTO. La stessa richiesta è avanzata da altri 8 partecipanti[40]. I Cantoni *ZG*, *NW*, *ZH*, *SZ* e *ZAD* scrivono che la conservazione separata dei dati non serve a nulla perché i dati degni di particolare protezione vengono già archiviati nel sistema primario dei fornitori di prestazioni. La conservazione separata dei dati deve essere sostituita da prescrizioni tecniche di sicurezza che i sistemi primari devono rispettare per poter essere utilizzati come luogo di archiviazione per la cartella informatizzata del paziente. *LUKS* fa notare che la lettera c aumenta inutilmente il costo del sistema. La cartella informatizzata del paziente è sempre stata definita come cartella virtuale con repository decentrali. Per questi repository si devono definire dei requisiti. *KSSG* chiede di riformulare il capoverso in modo da consentire una separazione logica dei documenti della cartella informatizzata del paziente da altri documenti. *K3* e *VZK* ricordano che gli ospedali tengono già le cartelle cliniche sotto forma elettronica. Memorizzare gli stessi dati in un ulteriore repository provoca doppioni inutili. È sufficiente che le chiavi di accesso ai dati siano memorizzate in sistemi di archiviazione separati, ma i dati devono poter essere letti dalle cartelle interne agli ospedali. *Privatim* attira l'attenzione su un colloquio telefonico con l'UFSP, secondo il quale questa disposizione deve essere interpretata nel modo seguente: i dati provenienti dai sistemi primari possono essere memorizzati solo nei repository che si trovano nelle comunità, per cui è esclusa la memorizzazione dei dati provenienti dai sistemi primari direttamente nella cartella informatizzata del paziente. Questa disposizione non è abbastanza chiara. Essendo però un punto essenziale, deve essere specificata con una formulazione precisa nel testo dell'ordinanza, senza rinvii al rapporto esplicativo. Per *HIN* e *BINT* è eccessivo mettere a disposizione supporti di memoria di dati dedicati solo per la cartella informatizzata del paziente. Sarebbe sufficiente una separazione logica dei dati, che sia rintracciabile in qualsiasi momento. La lettera c deve essere quindi adeguata come segue: «[…] elektronischen Patientendossier so in hierzu geeignete Ablagen zu speichern, dass diese jederzeit von anderen Daten getrennt werden können (logische Trennung)». Di conseguenza deve essere modificato anche il rapporto esplicativo. Sulla stessa falsariga, *USB* scrive che la possibilità di una separazione logica dei dati secondari della cartella informatizzata del paziente come prevista nel rapporto esplicativo deve essere stabilita esplicitamente anche nell'ordinanza. Propone pertanto di modificare la lettera c come segue: «[…] elektronischen Patientendossier physikalisch oder logisch ausgeschieden geführt werden sollen».

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

[40] K3, VZK, LUKS, FMH, ZG, NW, ZH, ZAD

Capoverso 2: *IG eHealth*, *PH CH* e *Posta* criticano la formulazione: «Sie haben auf Verlangen der Patientin oder des Patienten» e chiedono chi s'intende per «Sie». Secondo *IG eHealth* e *PH CH* è preferibile riformulare il capoverso 2 come segue: «Die Gemeinschaften haben auf […]», per specificare che si tratta delle comunità. Il Cantone *AI* segnala che la memorizzazione dei dati e i relativi processi amministrativi devono essere adeguati alle norme in materia di protezione dei dati. Il Cantone *BE* e *STSAG* ritengono che la cancellazione selettiva di dati nella cartella informatizzata del paziente debba essere svolta unicamente dal paziente e non possa essere imposta ai professionisti della salute. Gli strumenti a tale scopo sono già disponibili; il paziente può gestire i nuovi dati nel grado di riservatezza «segreti» e poi cancellarli o attribuirli ad altri gradi di riservatezza. Propongono la seguente formulazione del capoverso 2: «Sie haben der Patientin oder dem Patienten zu ermöglichen, die Verfügbarkeit der Daten nach Absatz 1 auf 10 bzw. 20 Jahre einzuschränken». Secondo *CDS* e 8 Cantoni[41] è importante motivare i fornitori di prestazioni a utilizzare la cartella informatizzata del paziente e non scoraggiarli con disposizioni complicate. Le prescrizioni sull'iscrizione e la gestione della cartella informatizzata devono essere compatibili con i processi terapeutici.

Capoverso 2 lettera a: 6 Cantoni[42] auspicano lo stralcio della lettera a, perché riguarda i professionisti della salute e i loro sistemi primari, ma non la comunità. *Insel* scrive che la lettera a deve essere stralciata e la responsabilità affidata ai pazienti. *KSSG* e *VGIch* nutrono grosse perplessità sulla disponibilità delle risorse necessarie per chiedere al paziente se pubblicare o meno un documento. *KSSG* ricorda che i pazienti hanno la possibilità di classificare i documenti come «segreti». *VGIch* avverte che è praticamente impossibile adeguare le funzionalità tecniche del software nei sistemi primari per poter svolgere queste manipolazioni. Entrambi i partecipanti propongono lo stralcio della lettera a. *Posta* chiede di quali dati si tratta e quali sono i criteri per determinarli. Questa disposizione è troppo ampia e per questo motivo non è realizzabile. Come alternativa, il paziente potrebbe classificare come «segreti» tutti i dati trasferiti dai professionisti della salute nella cartella informatizzata del paziente. Analogamente a *Posta* anche *medshare* chiede una precisazione del termine «dati», che vale anche per altri passaggi dell'ordinanza in cui compare lo stesso termine. *IG eHealth* e *PH CH* propongono la seguente modifica della lettera a: «alle neuen Dokumente ab einem vom Patienten bestimmten Zeitpunkt mit der Vertraulichkeitsstufe „geheime Daten" oder „sensible Daten" in seinem elektronischen Patientendossier zu speichern».

Capoverso 2 lettera b: 18 partecipanti[43] ripetono a proposito del capoverso 2 lettera b i commenti già espressi sul capoverso 1 lettera a. *IG eHealth* e *PH CH* segnalano che se viene accolta la loro proposta sulla lettera a, la lettera b deve essere soppressa. Anche *KSSG* chiede lo stralcio della lettera b. Se il paziente vuole prolungare il termine di conservazione, può archiviare i suoi documenti nel supporto di memoria messo a disposizione dalla cartella informatizzata del paziente. *Posta* chiede se questa lettera si riferisce alla comunità o al professionista della salute e, in quest'ultimo caso, quali sono esattamente le modalità previste. Se il testo non si riferisce alla comunità, è necessario un chiarimento. Il Cantone *NW* propone di lasciare al paziente la possibilità di conservare i suoi dati fino alla revoca. *Moeri* considera obsoleta la lettera b. *SUVA* critica il meccanismo previsto nelle lettere a e b, perché richiede un intervento attivo da parte del paziente, e chiede lo stralcio delle due lettere.

Capoverso 2 lettera c: *K3*, *VZK*, *VGIch* e *Insel* ripetono la loro posizione sulla lettera a e chiedono lo stralcio della lettera c. Per *VAKA* l'«use case» non è chiaro. Mantenendo il grado di riservatezza «dati segreti» si ottiene lo stesso effetto, ma con un onere trascurabile, e la lettera c può essere stralciata. *IG eHealth* e *PH CH* chiedono qual è la differenza fra «cancellare» e «distruggere». Anche secondo *SCH* il significato di «distruggere» non è chiaro. *IEGH* e *PH CH* propongono la seguente formulazione alternativa: «[…] aus dem elektronischen Patientendossier zu löschen». *SCH* avanza la seguente proposta: «[…] aus dem elektronischen Patientendossier unwiderruflich zu löschen». *SMCF* scrive che una tale distruzione non dovrebbe essere possibile, ma che dovrebbe essere prevista solo una disattivazione.

41 BL, GL, LZ, OW, UR, NW, SH, SZ
42 FR, GE, VS, VD, JU, NE
43 Insel, AI, AR, BL, CDS, GL, OW, UR, LU, SZ, SH, SG, TG, ZG, ZH, ZAD, FMH, Physioswiss

Capoverso 3: *LUKS* e *SSIM* evidenziano che questa disposizione attribuisce ampie competenze al DFI e all'UFSP. Mentre *LUKS* chiede di sopprimere la delega al DFI e all'UFSP e di inserire i principali requisiti direttamente nell'ordinanza, *SSIM* propone la creazione di un'istanza di controllo e ricorso indipendente dall'amministrazione. *ASI*, *FSAS*, *SWOR* e *Physioswiss* approvano le condizioni quadro centralizzate stabilite nell'ambito del capoverso 3. Le basi prese in considerazione corrispondono agli standard internazionali, che disciplinano in modo sicuro lo scambio elettronico dei dati. *ASI*, *FSAS* e *SWOR* aggiungono che è necessaria la creazione di un centro di competenza nel campo della semantica. Solo in questo modo si può affrontare in modo adeguato l'impiego delle terminologie di riferimento (SNOMED CT). *ASI* e *SWOR* rimandano al loro parere sull'OCIP-DFI Allegato 3: Metadati. *Posta* auspica la spiegazione del termine «profili d'integrazione» e chiede un glossario con le principali definizioni. *LUKS* e *FMH* ricordano che la verbalizzazione degli accessi ha ripercussioni in materia di responsabilità per il personale medico curante. La verbalizzazione deve provare quali dati sono stati consultati dal personale curante al momento dell'accesso. Questa osservazione vale anche per le disposizioni seguenti. Secondo *VGIch* i dati verbalizzati devono indicare anche gli accessi da parte di amministratori o personale dei punti di contatto.

FMH ritiene che i dettagli tecnici non debbano esser disciplinati a livello di ordinanza e rimanda al suo parere nelle osservazioni generali. Di conseguenza chiede lo stralcio del capoverso 3 lettere b – d.

Capoverso 4: 6 Cantoni[44]segnalano un errore nella traduzione francese. Il DFI può rinunciare a una traduzione nelle lingue nazionali se il testo originale è inglese, ma se l'originale è in una delle lingue ufficiali deve assicurarne la traduzione nelle altre lingue ufficiali. Il capoverso 4 deve essere corretto come segue : «[…] à les faire traduire dans les langues officielles». *FMH* chiede che le prescrizioni siano disponibili almeno nelle tre principali lingue nazionali oppure solo in inglese. *SBC* chiede la soppressione del capoverso 4.

Capoverso 5: *LUKS* e *SSIM* reiterano la loro posizione sull'articolo 9 capoverso 3. Sulla stessa falsariga, *FMH* chiede di sopprimere la competenza di delega dell'UFSP e di sostituirla con una disposizione a livello di ordinanza del Consiglio federale. Se questa proposta non viene accettata, si dovrà creare un'istanza di controllo e ricorso indipendente dall'amministrazione. *KDSBSON*, *DSBAG*, *privatim* e i Cantoni *ZG* e *BE* ritengono inutile la disposizione «facoltativa». Bisognerebbe verificare lo stato della tecnica periodicamente (a intervalli da definire) e, in caso di cambiamenti che potrebbero rappresentare una minaccia, apportare i necessari correttivi. Propongono la seguente modifica del capoverso 5: […] (BAG) überprüft die Vorgaben nach Absatz 3 regelmässig auf ihre Vereinbarkeit mit dem Stand der Technik und nimmt bei Abweichungen, die zu einer Bedrohungslage führen könnten, Anpassungen vor». *K3*, *VZK* e il Cantone *ZH* preferirebbero che solo il DFI fosse autorizzato a emendare le disposizioni dell'ordinanza o i suoi allegati. *K3* e *VZK* propongono pertanto la seguente modifica del capoverso 5: «Das EDI kann die Vorgaben […]». *HIN* fa notare che al momento dell'introduzione i profili d'integrazione e i formati di scambio non sono completi. Dovrebbe essere introdotto un processo regolamentato di gestione del cambiamento e di versionamento, che armonizzi gli adeguamenti con le parti interessate e i gestori in modo da assicurare in qualsiasi momento l'interoperabilità e l'intercambiabilità dei dati. Raccomanda la seguente modifica del capoverso 5: «Hierbei ist insbesondere eine Abstimmung mit den Betreibern, eine Versionierung und die Rückwärtskompatibilität sicherzustellen, so dass die Austauschbarkeit von Daten jederzeit gewährleistet ist».

Art. 10	Zugangsportal für Gesundheitsfachpersonen
Das EDI legt die Anforderungen an das Zugangsportal für Gesundheitsfachpersonen fest.	

VAKA fa notare che vengono menzionati diversi portali di accesso (per pazienti). Chiede una dichiarazione più precisa o una fusione dei portali o quantomeno una precisazione che potrebbe trattarsi di un portale con due GUI / maschere di login diverse. Inoltre *VAKA*, come anche il Cantone *AG*, chiede che i termini «dati» e «documenti» siano utilizzati in modo uniforme in tutte le ordinanze. Il Cantone *AG* dichiara inoltre di attribuire molta importanza alla trasparenza nel portale di accesso ed è favorevole al

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

download di documenti nel sistema primario per adempiere l'obbligo di documentazione. *Posta* chiede se è veramente necessario un portale di accesso per i professionisti della salute e se occorre un portale di accesso dedicato per i professionisti della salute e i pazienti. *BFH* chiede che già in questa sede si faccia riferimento all'allegato (CTO) per facilitare il reperimento dei requisiti. Per quanto riguarda il portale di accesso per i professionisti della salute, *HÄ CH* e *ÄTG* sottolineano che bisogna dare la massima priorità a una struttura chiara con una presentazione e dei filtri adeguati. Solo in questo modo è possibile svolgere il lavoro quotidiano in modo razionale. L'attualità e la qualità dei dati vengono prima della quantità. *IG eHealth* und *PH CH* ritengono che la delega della definizione dei portali di accesso per i professionisti della salute al DFI è molto ampia. Bisognerebbe definire dei requisiti minimi per il portale di accesso. Questi due partecipanti avanzano anche una proposta di formulazione concreta per l'articolo 10. *K3* e *VZK* sostengono che se i professionisti della salute hanno solo un accesso limitato ciò deve essere ben visibile e rimandano alla loro proposta di modifica all'articolo 3 lettera f.

SCH ed *economiesuisse* constatano che nelle raccomandazioni di eHealth Suisse e nel messaggio sulla LCIP l'accesso ai dati dei pazienti era previsto anche mediante un portale di accesso esterno. Nelle attuali ordinanze, invece, la certificazione di un portale di accesso esterno non è più contemplata. Manca così un accesso «light» alla cartella informatizzata del paziente LCIP per esempio per una comunità che non vuole fungere da comunità di riferimento. *Economiesuisse* deplora questa lacuna, mentre *SCH* scrive che ciò non favorisce lo sviluppo di eHealth in Svizzera e frena degli «use case» innovativi nell'ambito di mHealth, l'empowerment del paziente e in generale le innovazioni nel settore sanitario. *SSIM* e *SBC* scrivono che i portali esterni potrebbero essere realizzati anche sotto forma di applicazioni mobili e offrire così ulteriori servizi innovativi. A loro parere sarebbe peccato che mHealth venga sviluppato in modo completamente separato da eHealth. Analogamente a *SCH* aggiungono che i portali esterni danno un contributo essenziale all'empowerment dei pazienti e favoriscono l'innovazione con nuovi servizi di operatori terzi. Nel suo parere *SBC* illustra un esempio concreto di applicazione. Anche *HL7*, *IHE*, *SBC*, *SSIM* ed *economiesuisse* ritengono che lo spazio di fiducia LCIP non dovrebbe limitarsi ai fornitori di prestazioni della comunità come sistema chiuso, poiché anche i portali esterni certificati, con le loro innovazioni, potrebbero generare un valore aggiunto per i pazienti e i fornitori di servizi online e infine per l'intero sistema sanitario svizzero, l'economia e la piazza d'innovazione svizzera. Con una proposta identica, 6 partecipanti[45] chiedono un nuovo articolo 10bis «Portali di accesso esterni». Analogamente alla formulazione proposta da *IG eHealth* e *PH CH* per l'articolo 10, si rinuncia a riportare l'intero testo della proposta e si rimanda ai pareri disponibili online.

Art. 11 Datenschutz und Datensicherheit

[1] Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben. Dieses muss insbesondere folgende Elemente umfassen:

a. die Benennung eines oder einer Datenschutz- und Datensicherheitsverantwortlichen;

b. ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen;

c. ein Verzeichnis der Datenablagen;

d. ein Verzeichnis der angeschlossenen Primärsysteme;

e. die Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen ;

f. die Datenschutz- und Datensicherheitsanforderungen an das Personal und Dritte.

[2] Sie müssen die im Datenschutz- und Datensicherheitsmanagementsystem als sicherheitsrelevant eingestuften Vorfälle der Zertifizierungsstelle und dem BAG melden.

[3] Das EDI legt die Anforderungen in Bezug auf Datenschutz und Datensicherheit fest.

[4] Die Datenspeicher müssen sich in der Schweiz befinden und dem Schweizer Recht unterstehen.

6 partecipanti[46] ritengono che sarebbe più utile stabilire in modo generale ed astratto le prescrizioni

[45] HL7, IHE, SBC, SSIM, economiesuisse, SCH

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

dell'articolo 11, che devono essere soddisfatte in materia di protezione e sicurezza dei dati. Viene lasciato alle comunità, alle comunità di riferimento e ai fornitori di prestazioni decidere come rispettare queste disposizioni. Di conseguenza, l'articolo 11 deve essere completamente riveduto. *Posta* propone la pubblicazione di un elenco con i ruoli che deve possedere una comunità. A questo proposito sarebbe ipotizzabile anche un capitolo nel rapporto esplicativo. *VAKA* e il Cantone *AG* scrivono che un sistema di gestione della protezione e della sicurezza dei dati è auspicabile dal punto di vista della protezione dei dati, ma comporta un onere per le comunità. Chiedono di inserire nel rapporto esplicativo un riferimento su come evitare questo onere, p. es. permettendo a diverse comunità di assumere o conferire un mandato a una persona indipendente come responsabile della protezione dei dati. Il Cantone *AG* ritiene troppo vaga la formulazione sul tema del criptaggio. Le prescrizioni sul criptaggio non devono essere ancorate solo nelle CTO, ma già nell'OCIP. *SMCF* scrive, che in vista di queste esigenze appare legittimo limitare il numero delle comunità in Svizzera a una decina e non a 20-40 comunità. Secondo *VGIch* la competenza delle comunità in materia di protezione e sicurezza dei dati dovrebbe terminare nel punto di consegna della prestazione oppure nell'interfaccia per la ricerca di dati o la configurazione di documenti dell'istituzione affiliata. A questo scopo dovrebbe essere aggiunto un capoverso all'articolo 11. *VGIch* osserva inoltre che le prescrizioni e i contenuti delle CTO non devono interferire con i sistemi primari o, in caso contrario, dovrebbero definire al massimo dei principi generali sulla sicurezza dei dati.

Capoverso 1: *FMH* ricorda che devono essere rispettate le prescrizioni della legge sulla protezione dei dati e deve essere evitata una regolamentazione eccessiva. *SQS* propone la seguente formulazione per il capoverso 1: «Gemeinschaften müssen nach Art. 11 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz zertifiziert sein. Sie müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben. Dieses muss die Anforderungen des Art. 4 Abs. 2 Verordnung über die Datenschutzzertifizierung VDSZ vom 28. September 2007 und der Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 19. März 2014 des EDÖB erfüllen. Dieses muss[…]». Nel suo commento avanza un'ulteriore proposta alternativa con riferimento alle norme ISO 9001 e ISO/IEC, che sono riconosciute a livello internazionale. *OFAC* fa notare che le comunità, quali organi cantonali, saranno soggette al diritto del loro Cantone in materia di protezione dei dati. Alcune nozioni importanti della protezione dei dati, come il sistema di gestione e sicurezza dei dati o il processo di certificazione, non esistono nella maggior parte delle legislazioni cantonali. Bisogna poi considerare le notevoli differenze fra le leggi cantonali. Le direttive dell'IFPDT sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere devono valere per ogni tipo di organizzazione. *Economiesuisse*, *SBC*, *HL7* e *IHE* chiedono che le comunità possano delegare il sistema di gestione della protezione e della sicurezza dei dati, perché altrimenti i costi saliranno inutilmente. Concretamente propongono la seguente aggiunta al capoverso 1: «[…] betreiben, oder durch Delegation betreiben lassen. Dieses muss […]».

Capoverso 1 lettera a: *LUKS* auspica lo stralcio della lettera a. I requisiti, i compiti e i vantaggi del responsabile della protezione dei dati non sono chiari. Il suo parere è condiviso da *CDS* e 6 Cantoni[47], che assieme ad altri 6 partecipanti[48] chiedono di rinunciare a responsabili speciali per la protezione e la sicurezza dei dati. Il Cantone *AI* raccomanda di non nominare un organismo indipendente se l'incaricato alla protezione dei dati ha abbastanza capacità per assolvere questo compito.

Capoverso 1 lettere b e c: *ISSS* propone di precisare la lettera b con la seguente formulazione: «b. Ein System zur proaktiven Erkennung von und zum Umgang mit Vorfällen im Bereich Angriffssicherheit und Betriebsausfallsicherheit» e di modificare la lettera c come segue: «c. ein Verzeichnis der Datenablagen, Berechtigungen und Prozesse zur Datensicherung und sicheren Aufbewahrung».

Capoverso 1 lettera d: *KDSBSON* e *DSBAG* ricordano che durante l'elaborazione della legislazione sulla cartella informatizzata del paziente non si era mai parlato di un collegamento diretto dei sistemi primari con la cartella informatizzata del paziente. Era previsto piuttosto un collegamento dei sistemi secondari, come nota anche il Cantone *FR.* Questi partecipanti chiedono di riconsiderare l'opportunità

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

di un collegamento dei sistemi primari, che a loro parere è problematico e sconsigliabile dal punto di vista del diritto sulla protezione dei dati. Se è veramente auspicato un collegamento dei sistemi primari, questi devono rispettare le prescrizioni della legislazione sulla cartella informatizzata del paziente per quanto riguarda la protezione dei dati e la sicurezza delle informazioni. *Privatim* rimanda al parere espresso a tale proposito nelle osservazioni generali. *SQS* segnala che sia il sistema di gestione della protezione dei dati secondo l'OCPD sia il sistema di gestione secondo l'ISO 9001 e il sistema di gestione della sicurezza delle informazioni secondo l'ISO/IEC 27001 comprendono tutti i sistemi e non solo i sistemi primari collegati. Se uno di questi standard viene scelto come norma di certificazione per le comunità e le comunità di riferimento, la menzione esplicita di tale requisito diventa inutile. Di conseguenza propone di stralciare la lettera d. Per il Cantone *BE* l'attuale formulazione suggerisce che i sistemi primari siano collegati «direttamente» alla cartella informatizzata del paziente. In realtà sono invece collegati solo indirettamente con la cartella informatizzata del paziente attraverso l'archivio di documenti (copia sincronizzata). Sarebbe quindi opportuno riformulare la lettera d come segue: «d. ein Verzeichnis der abgebildeten Primärsysteme». *FMH* chiede cosa significa la lettera d e se sia veramente realistica oppure non sia una pretesa eccessiva. La lettera d dovrebbe essere stralciata o sostituita con un registro di archivi secondari. Anche 6 Cantoni[49] considerano poco chiara la lettera d. Chiedono di precisare, per esempio nel rapporto esplicativo, quali dati devono essere contenuti nel registro. Non è possibile fornire un elenco dei computer e software utilizzati da migliaia di professionisti della salute. La lettera d deve essere quindi soppressa. Il Cantone *NE* aggiunge che il testo dell'ordinanza o il rapporto esplicativo deve precisare quali dati devono essere contenuti nel registro dei sistemi primari. *ISSS* propone di precisare la lettera d con la seguente formulazione: «[…] Primärsysteme, welche direkten oder indirekten Zugang zu den Daten / Kommunikation haben oder erlangen können». *Lovis* chiede se il registro di sistemi primari collegati si riferisce a organizzazioni o sistemi.

Capoverso 1 lettere e e f: Per *CURAVIVA*, *Insos* e il Cantone *TG* la formulazione di questa (sotto) delega è troppo vaga. Essa dovrebbe indicare il contenuto o, almeno, gli elementi basilari delle prescrizioni in materia di protezione e sicurezza dei dati per le strutture sanitarie affiliate, i loro professionisti della salute, il loro personale e terzi. Ne va della leggibilità della legge, della corretta applicazione da parte degli attori coinvolti e, in definitiva, della certezza del diritto. *Senesuisse* considera insoddisfacenti le disposizioni delle lettere e ed f. Le comunità devono sapere con maggiore chiarezza quali requisiti devono esigere dall e strutture sanitarie e dai professionisti della salute nonché dal personale e da terzi. Occorre completare il testo dell'ordinanza oppure stilare un aiuto all'esecuzione con un contenuto adeguato.

Capoverso 2: *HL7* e *IHE* sono favorevoli alla determinazione di un termine fra l'insorgere e la notifica di tali incidenti. Analogamente *medshare* chiede a questo proposito l'introduzione di una periodicità. *Posta* chiede quali requisiti deve soddisfare la segnalazione e raccomanda di adeguare questa disposizione alla nuova direttiva dell'UE sulla protezione dei dati. Per *SPO* non è chiaro se questo obbligo di segnalazione è inteso come vincolante e se sono stati definiti gli eventi considerati rilevanti per la sicurezza. Chiede quindi una formulazione più chiara e comprensibile. Anche *FRC* desidera un chiarimento sulle modalità e soprattutto sui termini per le notifiche di incidenti nel sistema. La reazione dovrebbe essere infatti possibilmente immediata.

SQS fa notare che gli organismi di certificazione sono responsabili solo della certificazione secondo le norme di certificazione e svolgerebbero un controllo annuale dei processi di certificazione presso le comunità di riferimento e le comunità. Negli intervalli fra gli audit non avrebbero alcuna funzione a livello di attività operativa. Per questo motivo gli incidenti di cui al capoverso 2 dovrebbero essere segnalati solo all'UFSP e non agli organismi di certificazione. Attraverso l'articolo 36 capoverso 1 lettera c e l'articolo 37 capoverso 3 lettera a di questa ordinanza, l'UFSP potrebbe coinvolgere gli organismi di certificazione qualora, sulla base della segnalazione di gravi incidenti rilevanti per la sicurezza, una verifica da parte dell'organismo di certificazione potrebbe impedire la minaccia di una violazione della protezione e della sicurezza dei dati. *OFAC* scrive che i servizi dell'IFPDT fanno capo alla Cancelleria federale al fine di garantire la loro indipendenza. Di norma spetta a loro valutare la gravità di un incidente e decidere

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

se le parti interessate devono prendere delle misure. Lo stesso vale per il DFI e l'UFSP.

Capoverso 3: *SSIM* ritiene necessario garantire che i requisiti in materia di protezione e sicurezza dei dati siano conformi alla legge sulla protezione dei dati, senza però eccedere. Anche *LUKS* chiede di evitare una regolamentazione eccessiva e consiglia di applicare anche qui la legge sulla protezione dei dati. Visto che non è necessaria una disposizione supplementare, il capoverso 3 va riveduto. *ISSS* e *Tessaris* propongono la seguente aggiunta al capoverso 3: «[…] Datenschutz und Datensicherheit und deren Anpassung an die Entwicklung der Bedrohungslage fest». Come nel suo commento sul capoverso 1, *SQS* segnala che, scegliendo il sistema di certificazione secondo OCPD, i requisiti sono definiti nelle «Direttive del 19 marzo 2014 dell'IFPDT sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere». L'ordinanza deve quindi stabilire solo eventuali requisiti supplementari. *OFAC* è del parere che le esigenze relative alla protezione dei dati dovrebbero essere stabilite da un dipartimento federale e non dai servizi dell'IFPDT. Stabilire i requisiti implica anche controllarne il rispetto. I servizi dell'IFPDT fanno capo alla Cancelleria federale in modo da garantire la neutralità dei controlli e della sorveglianza. Una sorveglianza svolta dall'UFSP non sarebbe invece neutrale, soprattutto riguardo ai servizi centrali di ricerca, che rimangono sotto la responsabilità legale dell'UFSP.

Capoverso 4: *KDSBSON*, *DSBAG*, *privatim* e i Cantoni *BE* e *FR* ritengono che questa disposizione sia indispensabile dal punto di vista della protezione dei dati perché riguarda dati sanitari personali degni di particolare protezione e perché nell'ambito della cartella informatizzata del paziente sussiste anche il pericolo della creazione di profili della personalità. Chiedono inoltre di considerare se la sede sociale e il posto di lavoro dei collaboratori coinvolti non debba trovarsi obbligatoriamente in Svizzera. Analogamente il Cantone *TG* ritiene che si debba evitare il trattamento dei dati all'estero e modificare di conseguenza questo capoverso. *ISSS* avanza una proposta concreta con il seguente tenore: «Die Datenleitungen, Datenverbindungen, Datenübermittlung, Datenspeicherung und Datenverarbeitung müssen sich in der Schweiz befinden und dem Schweizer Recht unterstehen». *HIN* capisce e condivide le intenzioni del capoverso 4. Aggiunge che le persone giuridiche dovrebbero essere menzionate esplicitamente e a questo scopo propone la seguente formulazione: «Leistungen zur Datenspeicherung müssen von juristischen Personen erbracht werden, die in der Schweiz domiziliert sind und Schweizer Recht unterstehen. Die Datenspeicher müssen […]».

Art. 12	Kontaktstelle für Gesundheitsfachpersonen
Die Gemeinschaften müssen für die Gesundheitsfachpersonen eine Kontaktstelle bezeichnen, die diese im Umgang mit dem elektronischen Patientendossier unterstützt.	

CURAVIVA, *Insos* e il Cantone *AG* approvano la costituzione di punti di contatto per i professionisti della salute. *ASI*, *SWOR* e *Physioswiss* considerano il sostegno competente dei professionisti della salute come un fattore decisivo per il successo della cartella informatizzata del paziente. Anche *senesuisse* è favorevole alla creazione di tali centri di contatto, ma sottolinea la necessità di garantirne il finanziamento a lungo termine, che invece non è assicurato dagli aiuti finanziari previsti. *HÄ CH* e *ÄTG* avvertono che l'offerta di hotline può richiedere molto tempo e denaro. Soprattutto nella fase iniziale bisognerebbe prevedere risorse sufficienti. L'ideale sarebbe assicurare un funzionamento gratuito o quantomeno un tetto di spesa. Questi costi supplementari dovrebbero essere contemplati e compensati nelle tariffe. Sottolineano che gli adeguamenti dei sistemi primari, interfacce, certificazione, hotline ecc. non devono essere considerati dei «business case». *BINT* chiede di aggiungere un nuovo articolo dopo l'articolo 12 con il seguente tenore: «Die Gemeinschaften stellen sicher, dass der gemeinschaftsübergreifende Zugriff auf ihre Daten, bei Vorliegen der Patientenbewilligung, jederzeit und kostenlos möglich ist». *KSSG* obietta che le caratteristiche di questo servizio di sostegno sono troppo vaghe: alcune sono concretizzate nelle CTO, ma altre – soprattutto quelle di natura organizzativa – rimangono completamente in sospeso. Il Cantone *BS* ritiene che le comunità dovrebbero essere libere di decidere se gestire uno o più punti di contatto per i professionisti della salute e i pazienti. Gli articoli 12 e 19 dovrebbero essere completati per specificare che deve essere designato almeno un punto di contatto.

Secondo *SPO* si chiede se dall'ordinanza emerge chiaramente che devono essere rispettate anche le prescrizioni indicate nel rapporto esplicativo, per esempio l'obbligo di segretezza analogo a quello del

medico.

Sezione 2: Stammgemeinschaften

Art. 14	Information der Patientin oder des Patienten
[1] Vor der Eröffnung eines elektronischen Patientendossiers muss die Stammgemeinschaft die Patientin oder den Patienten insbesondere über folgende Punkte informieren:	
a.	den Zweck des elektronischen Patientendossiers;
b.	die Grundzüge der Datenbearbeitung;
c.	die Folgen der Einwilligung und die Möglichkeit des Widerrufs;
d.	die Erteilung von Zugriffsrechten.
[2] Sie muss der Patientin oder dem Patienten Datenschutz- und Datensicherheitsmassnahmen empfehlen.	

CMC, *KAeG SG*, *BüAeV* e *GAeSO* criticano il fatto che il finanziamento dell'informazione dei pazienti non è disciplinato. Partono dal presupposto che le comunità di riferimento ribalteranno i costi sui professionisti della salute a loro affiliati o li integreranno nelle loro quote di adesione. In base al principio di causalità, i costi legati all'informazione dei pazienti dovrebbero essere assunti da questi ultimi. Chiedono l'aggiunta della seguente lettera al capoverso 1: «e. Bemessungsgrundlagen und Verwendung der zu bezahlenden Beiträge». *K3*, *VZK* e *VAKA* scrivono che le informazioni da comunicare ai pazienti secondo l'articolo 14, ma anche secondo le CTO, sono estremamente vaste e dettagliate. Questo non è però l'obiettivo di un'informazione. Chiedono una revisione e una soluzione più pragmatica e semplice. *K3* e *VZK* aggiungono che non ha senso raccomandare delle misure di protezione e sicurezza dei dati ai pazienti, ma sarebbe più opportuno implementare queste prescrizioni come standard nei sistemi stessi. A questo proposito *FRC* fa notare che per il paziente sarebbe importante anche essere informato se il suo medico, farmacista, fisioterapista, ecc. partecipa o meno alla cartella informatizzata del paziente e quali sono le conseguenze per il paziente stesso. *Santésuisse* ritiene che questa informazione debba essere fornita dall'IDP o dall'ufficio di registrazione. A suo parere, il paziente dovrebbe essere informato delle conseguenze della cartella informatizzata del paziente quando la apre o ne fa richiesta. Altrimenti dovrebbe recarsi appositamente nella sede della comunità di riferimento. *SPO* chiede di aggiungere tre capoversi all'articolo 14: «Capoverso 3: Sie stellt sicher, dass die in Art. 14.1 aufgeführten Informationen erfolgt sind und ist darüber beweispflichtig. Capoverso 4: Sie informiert die Patientinnen und Patienten regelmässig und schriftlich über die erfolgten Bearbeitungen von Daten. Capoverso 5: Sie stellen sicher, dass Änderungen im Bereich der Zugriffsrechte für Gesundheitsfachpersonen nach Art. 9 Abs. 3 und Art. 10 Abs. 2 Bst. b Ziff. 1 EPDG protokolliert werden».

Capoverso 1: *ASI*, *FSAS* e *SWOR* considerano problematico attribuire alla comunità di riferimento la competenza di informare in modo sufficiente i pazienti. La comunità di riferimento deve garantire che sia assicurata la competenza professionale per tale informazione. *KSSG* e *UDC* desiderano una descrizione più precisa di come deve avvenire l'informazione. *KSSG* presenta un calcolo concreto per illustrare che l'informazione diretta da parte di un collaboratore rappresenta un grosso onere, e chiede una descrizione delle modalità d'informazione del paziente nelle disposizioni d'esecuzione o nelle CTO. Secondo 6 Cantoni[50] è altresì importante spiegare ai pazienti le conseguenze di una revoca: perdita di dati, nessuna anamnesi medica in caso di nuovo consenso. Propongono di aggiungere una lettera al capoverso capoverso 1: «e. la possibilité de révoquer le dossier et les conséquences d'une révocation». *FRC* propone dal canto suo la seguente aggiunta alla lettera c: «[…] consentement, ou d'un non consentement, et la possibilité […]». *SPO* deplora che il brano di frase «aus einem Widerruf dürfen ihr oder ihm keine Nachteile erwachsen» sia stato cancellato dalla LCIP, sezione 2, articolo 3 cpv. 3. Propone la seguente aggiunta al capoverso 1 lettera c: «[…] des Widerrufs sowie die möglichen Folgen eines Widerrufs». *CURAVIVA*, *Insos* e il Cantone *TG* segnalano che nel caso di persone incapaci di discernimento deve essere informato il loro rappresentante e propongono la seguente formulazione per il capoverso 1: «[…] oder den Patienten und gegebenenfalls ihre bzw.

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

seine Stellvertretung insbesondere über die […]». *CURAVIVA* e *Insos* scrivono inoltre che deve essere informato comunque anche il paziente, nonostante la sua incapacità di discernimento. *HL7*, *IHE* e *Integic* avanzano una proposta simile: «[…] oder den Patienten oder Stellvertreter/in insbesondere über folgende […]». Anche *senesuisse* lamenta la mancanza di disposizioni sui pazienti divenuti incapaci di discernimento. Trattandosi però di casi frequenti nella pratica, propone di apportare le aggiunte necessarie sulla base dell'articolo 377 lettera f CC. *Privatim*, *KDSBSON*, *DSBAG* e i Cantoni *BE* e *ZG* ritengono che questa disposizione dovrebbe includere l'obbligo per la comunità di riferimento di informare i pazienti sui possibili rischi che l'impiego della cartella informatizzata del paziente implica per la sicurezza delle informazioni. Chiedono di aggiungere la seguente lettera al capoverso 1: «e. die informationssicherheitsrechtlichen Risiken der Nutzung des elektronischen Patientendossiers». *Tessaris* avanza la seguente proposta per la formulazione del capoverso 1: «Die Stammgemeinschaften informieren die Öffentlichkeit, die Gesundheitsfachpersonen und Patienten in allgemeiner Weise über folgende Punkte betreffend Eröffnung, Betrieb und Aufhebung des elektronischen Patientendossiers». Alla lettera d propone inoltre la seguente aggiunta: «die Bedeutung der Festlegung der Vertraulichkeitsstufen sowie die Erteilung […]». Analogamente *FMH* chiede di estendere l'informazione anche alle conseguenze di una restrizione all'accesso.

Capoverso 2: A proposito dell'informazione dei rappresentanti di persone incapaci di discernimento, *CURAVIVA*, *Insos* e il Cantone *TG* propongono un'aggiunta anche al capoverso 2: «[…] oder dem Patienten und gegebenenfalls ihrer bzw. seiner Stellvertretung Datenschutz- und Datensicherheitsmassnahmen empfehlen». *HL7*, *IHE*, *Integic*, *LUKS* e *medshare* desiderano una precisazione delle raccomandazioni e s'informano sui criteri da applicare. *FMH* chiede lo stralcio del capoverso 2. 7 partecipanti[51] segnalano che le misure di protezione e di sicurezza dei dati non dovrebbero essere raccomandate ai pazienti, bensì preimpostate a livello tecnico, p. es. con accessi protetti da password, criptaggio vincolante, ecc. (Privacy by Default). Una semplice raccomandazione accolla la responsabilità al paziente e, considerata la tipologia dei dati trattati, non è considerata sufficiente. *Tessaris* propone il seguente testo per il capoverso 2: «Die Stammgemeinschaften machen die Gesundheitsfachpersonen sowie die Patientinnen / Patienten in allgemeiner Weise auf die Anforderungen aus dem Datenschutz und die Risiken für die im elektronischen Patientendossier gespeicherten Daten aufmerksam». *VGIch* fa notare che l'informazione (cpv.1) / raccomandazione (cpv. 2) equivale a una consulenza giuridica, che rientra fra i campi di attività con riserva di approvazione, richiede un'apposita formazione e comporterebbe una responsabilità civile per consulenza. Bisogna distinguere chiaramente fra informazione e raccomandazione; le CTO devono essere formulate in modo più chiaro.

Art. 15	Einwilligung
Die Stammgemeinschaft hat von der Patientin oder dem Patienten die Einwilligung zur Führung eines elektronischen Patientendossiers einzuholen. Diese muss von der Patientin oder vom Patienten unterzeichnet sein.	

ASI, *FSAS* e *SWOR* chiedono quale sia esattamente il ruolo delle comunità di riferimento e se possono fare «pubblicità» attiva fra i pazienti. *KSOW* e il Cantone *ZG* s'informano se anche il consenso e quindi la firma possono avvenire per via elettronica. *Economiesuisse* considera opportuna la possibilità di firma elettronica e *Posta* propone che la firma elettronica sia riconosciuta ai fini del consenso. Secondo *SCH* la firma elettronica qualificata di cui all'articolo 14 CO deve essere chiaramente accettata perché contribuisce a raggiungere l'obiettivo della massima digitalizzazione possibile. Dovrebbero essere ammessi anche altri strumenti ausiliari per l'identificazione inequivocabile delle persone. La precisazione dovrebbe essere chiaramente formulata a livello di ordinanza. Viene proposta la seguente aggiunta all'articolo 15: « […] unterzeichnet sein. Zulässig ist auch die Nutzung anderer Hilfsmittel zur eindeutigen Bestimmung der Identität der Patientin oder des Patienten». Anche *IG eHealth* e *PH CH* vogliono assicurarsi che il consenso possa avvenire con firma elettronica e propongono la seguente formulazione per l'articolo 15: «[…] Diese muss von der Patientin oder dem Patienten nach Artikel 14 capoverso 2bis des BG betreffend die Ergänzung des ZGB, 5. Teil: Obligationenrecht, unterzeichnet sein». *CMC*, *KAeG SG*, *BüAeV* e *GAeSO* auspicano che il consenso debba essere firmato di proprio pugno dal paziente oppure essere conferito con firma elettronica equivalente alla firma autografa. *Tessaris* propone che i

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

professionisti della salute o la comunità richiedano dal paziente il consenso alla tenuta della cartella informatizzata del paziente all'inizio o al più tardi alla fine del trattamento. Il consenso deve essere stilato per iscritto e firmato oppure stabilito in un verbale elaborato e firmato dal professionista della salute curante in presenza di testimoni. *VAKA* obietta che la nozione di «firma» non è definita in modo sufficientemente chiaro. È ipotizzabile per esempio una firma su un tablet al posto della firma autografa su carta. Si devono assicurare delle modalità semplici per apporre una firma valida – una richiesta avanzata anche da *Medgate*, *K3* e *VZK*. *K3* e *VZK* scrivono inoltre che dovrebbe essere possibile accordare il consenso anche a domicilio, in uno Swisscom Shop o in un ufficio postale. Il Cantone *AG* evidenzia che per assicurare i mezzi di prova sono necessarie la forma scritta e la firma autografa. La firma elettronica corrisponderebbe alle prescrizioni del CO, ma non è ancora diffusa nella pratica. *PKS* e *SSIM* criticano che i processi di apertura impediscono un impiego ad-hoc presso il fornitore di prestazioni, perché la comunità di riferimento deve ricevere un previo consenso scritto. Dovrebbe essere possibile aprire una cartella informatizzata del paziente direttamente presso il fornitore di prestazioni e apporre direttamente la firma sul posto senza bisogno di infrastrutture supplementari. *Santésuisse* scrive, con riferimento al suo commento sull'articolo 14, che anche a questo proposito sarebbe opportuno affidare all'IDP o al suo ufficio di registrazione il compito di richiedere il consenso al momento della registrazione.

Tessaris scrive che le persone capaci di discernimento dovrebbero poter esercitare i loro diritti sulla cartella informatizzata del paziente da sole o tramite un rappresentante da loro designato, mentre per le persone incapaci di discernimento dovrebbe essere il rappresentante da loro designato a esercitare questo diritto. *Posta* chiede una precisazione su come viene verificata la capacità di discernimento / imputabilità dei pazienti e cosa succede quando viene persa. S*enesuisse* ripete a questo proposito il suo parere sull'articolo 14.

Secondo *CMC*, *KAeG SG*, *BüAeV* e *GAeSO* l'esistenza del consenso fa supporre che i professionisti della salute possano inserire nella cartella informatizzata del paziente tutti i dati rilevanti per la salute, a meno che il paziente non abbia stabilito altrimenti. Ciò è di per sé auspicabile. In virtù di questa disposizione bisogna tuttavia aspettarsi che i professionisti della salute inseriranno tutti i dati nella cartella informatizzata del paziente per evitare di essere criticati in un secondo tempo per non aver registrato informazioni «importanti». Per impedire un'inondazione di dati, i professionisti della salute dovrebbero ricevere il maggior margine di discrezionalità possibile nella scelta dei dati rilevanti per il trattamento, tanto più che questi non sono sufficientemente descritti nel messaggio. Chiedono un articolo supplementare con la seguente formulazione: «Ob Daten behandlungsrelevant und im elektronischen Patientendossier zu erfassen sind, liegt im Ermessen der Gesundheitsfachpersonen». Come *ZAD,* criticano inoltre che l'ordinanza non specifica ancora se i professionisti della salute possono modificare o cancellare i dati da loro inseriti nella cartella informatizzata del paziente. Mentre *ZAD* chiede una disposizione generale, i suddetti partecipanti desiderano che sia modificata la LCIP. Il Cantone *ZH* segnala la necessità di definire i dati da rendere accessibili nella cartella informatizzata del paziente. Chiede inoltre di chiarire se un medico si rende punibile in caso di mancata o incompleta registrazione di dati.

Art. 16 Verwaltung

[1] Stammgemeinschaften müssen:

a. den Eintritt und den Austritt von Patientinnen und Patienten regeln;
b. die Patientin oder den Patienten identifizieren;
c. sicherstellen, dass Patientinnen und Patienten und deren Stellvertretung für den Zugriff auf das elektronische Patientendossier nur gültige Identifikationsmittel verwenden, die von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurden;
d. eine Patientenidentifikationsnummer nach den Vorgaben der Artikel 5 und 6 anfordern;
e. Prozesse zum Wechsel der Stammgemeinschaft vorsehen.

[2] Stammgemeinschaften müssen die Umsetzung der Artikel 2 Absätze 1–4 und Artikel 3 sicherstellen.

Il Cantone *AG* osserva che i suddetti compiti amministrativi potrebbero essere sì necessari, ma – alla stessa stregua del cambio di comunità di riferimento da parte del paziente – comportano oneri eccessivi per le comunità di riferimento. *Medshare* avanza la seguente proposta per precisare il capoverso 1 lettera a: «[…] die Eröffnung und den Widerruf des elektronischen Patientendossiers von Patientinnen

und Patienten regeln». Per la lettera b propone la seguente formulazione: «die Patientin oder den Patienten authentifizieren und identifizieren». *Tessaris* chiede di completare il capoverso 1 lettera b come segue: «[…] identifizieren oder durch die antragstellende Gesundheitsfachperson identifizieren lassen». *VAKA*, *K3* e *VZK* obiettano che dall'articolo non risulta chiaramente se è sufficiente l'impiego di mTAN, e propongono pertanto di menzionare espressamente che la procedura mTAN e la sua autorizzazione sono considerate sufficienti (articolo seguente e CTO). Se il paziente desidera un metodo per lui più sicuro, può sempre utilizzarlo. *Posta* chiede un chiarimento sull'interpretazione dell'articolo 16 per le persone non residenti in Svizzera. A proposito del capoverso 1 lettera d, *IG eHealth* e *PH CH* fanno notare che secondo le attuali disposizioni il numero d'identificazione del paziente (NIP) può essere attribuito solo alle persone assicurate obbligatoriamente secondo l'articolo 1 LAVS. Altre persone, come p. es. i frontalieri, non potrebbero avere una cartella informatizzata e sarebbero quindi escluse dal sistema, sebbene abbiano diritto alle prestazioni sociali in virtù degli accordi bilaterali. *IG eHealth* e *PH CH* rimandano a questo proposito alla loro proposta di modifica dell'articolo 5 capoverso 1. Secondo loro il capoverso 1 lettera e è formulato in modo troppo generico. Propongono quindi il seguente testo: «[…] für einen Wechsel des Patienten in eine andere Stammgemeinschaft alle nötigen Daten, Zugriffsregeln und Logeinträge der neuen Stammgemeinschaft für eine Übernahme zugänglich machen, so dass Zugriffe auf das elektronischen Patientendossier weiterhin in vergleichbarem Umfang erfolgen können. Das EDI legt den Umfang der Formate der zu transferierenden Daten fest». *Moeri* scrive che devono essere previsti dei processi per il cambio di comunità di riferimento per i pazienti e i loro dati. I Cantoni *ZH*, *ZG* e *NW* nonché *ZAD* segnalano che le prescrizioni devono essere formulate in modo più diretto e specificare che le comunità di riferimento possono essere cambiate. Le modalità di applicazione sono lasciate alla competenza delle comunità di riferimento. I suddetti partecipanti chiedono la completa revisione di questa disposizione e avanzano proposte concrete di formulazione, che per la loro entità non possono essere riportate nel presente rapporto.

Art. 17	Zugangsportal für Patientinnen und Patienten
Das EDI legt die Anforderungen an das Zugangsportal für Patientinnen und Patienten fest.	

CURAVIVA, *Insos* e il Cantone *TG* obiettano che la formulazione di questa (sotto-) delega non soddisfa i requisiti minimi di precisione e densità normativa. Non fosse che per trasparenza e leggibilità, l'articolo 17 dovrebbe indicare almeno gli elementi basilari dei requisiti applicabili al portale d'accesso destinato ai pazienti. *FRC* fa notare che l'informazione dei pazienti sull'impiego del portale di accesso sarà complessa e propone pertanto che le associazioni dei pazienti, le organizzazioni di tutela e di ricorso dei pazienti e le associazioni dei consumatori siano invitate formalmente a collaborare alle attività di informazione e siano retribuite nell'ambito di mandati di prestazioni. Devono essere anche incoraggiate a collaborare fra di loro. *SMCF* osserva che sulla base di queste disposizioni è difficile giudicare le modalità di accesso per il paziente. Eppure le modalità avranno un notevole influsso sull'impiego della cartella informatizzata del paziente e sulla mole di lavoro a carico dei professionisti della salute in questo ambito.

LUKS propone di inserire una disposizione sulla certificazione di portali di accesso «esterni» per i pazienti, cioè di portali non appartenenti a una comunità di riferimento. Bisogna rinunciare a limitazioni non necessarie dal punto di vista oggettivo e consentire soluzioni e modelli aziendali innovativi. 11 partecipanti[52] temono che le prescrizioni dell'UFSP possano limitare in misura eccessiva possibili modelli aziendali destinati a finanziare l'esercizio della cartella informatizzata del paziente. Il diritto di esecuzione, soprattutto le CTO, deve essere predisposto in modo tale da lasciare spazio a soluzioni innovative e nuovi modelli aziendali. Anche questi partecipanti sottolineano la necessità di evitare restrizioni inutili.

FSAS, *Physioswiss*, *ASI* e *SWOR* evidenziano che un portale di accesso attrattivo e facilmente accessibile rappresenta un importante sostegno per i pazienti ed è quindi un fattore di successo. Il Cantone *AG* si esprime a favore di chiare regole per il portale di accesso e l'assenza di barriere. *VGIch* ritiene che i requisiti di base (p. es. assenza di barriere) debbano essere disciplinati nell'ordinanza e non nelle norme di esecuzione del DFI, altrimenti viene violato il principio della legalità. *FMH* scrive che secondo l'articolo 11 LCIP i portali di accesso devono essere certificati, indipendentemente dal fatto che facciano

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

parte dell'offerta di una comunità di riferimento o di una comunità normale. A suo parere, bisognerebbe inserire almeno una disposizione sulla possibilità di certificare i portali di accesso di comunità che non siano comunità di riferimento.

Posta individua in questa disposizione una grossa «concentrazione di potere» nelle mani del DFI. A suo parere le ordinanze dovrebbero menzionare gli «use case», senza tuttavia impedire futuri «use case», e chiede di conseguenza la loro definizione e aggiunta. *Senesuisse* ha l'impressione che queste norme di pura delega al DFI siano troppo concise. L'ordinanza dovrebbe quantomeno stabilire e pubblicare i principi di base. *IG eHealth* e *PH CH* sono contrari a delegare completamente al DFI la definizione dei portali di accesso per i pazienti. Devono essere definiti dei requisiti minimi per il portale di accesso in modo da assicurare l'uniformità e l'interoperabilità della cartella informatizzata del paziente. Nei loro pareri propongono pertanto un nuovo articolo 17, che per la sua entità non può essere riportato nel presente rapporto.

Art. 18	Verfügbarkeit der von Patientinnen oder Patienten erfassten Daten
Das EDI legt die Anforderungen an den Umgang mit den von Patientinnen und Patienten über das Zugangsportal erfassten Daten fest.	

CURAVIVA, *Insos*, il Cantone *TG*, *senesuisse* e *SMCF* ripetono i pareri espressi sull'articolo 17. *VAKA* ricorda il collegamento con il numero 10.2 RTO e scrive che il rapporto costi-benefici e in particolare l'estensione al di fuori di un download non è possibile con l'archiviazione completamente offline. Il download di documenti è già previsto in altri articoli. L'importazione al di fuori del mero documento del paziente non è possibile né appropriata. Il Cantone *AG* è favorevole a un'archiviazione chiaramente delimitata dei dati appartenenti ai pazienti. L'esportazione di questi dati è considerata ammissibile e opportuna.

Art. 19	Kontaktstelle für Patientinnen und Patienten
Stammgemeinschaften müssen für die Patientinnen und Patienten eine Kontaktstelle bezeichnen, die sie im Umgang mit dem elektronischen Patientendossier unterstützt.	

Senesuisse, il Cantone *BS*, *CURAVIVA* e *Insos* ripetono i pareri espressi sull'articolo 12, ma nella fattispecie riferiti ai pazienti invece che ai professionisti della salute. *SMCF* reitera i suoi commenti sugli articoli 17 e 18. *ASI*, *FSAS*, *SWOR* e *Physioswiss* considerano che il sostegno dei pazienti nell'uso della cartella informatizzata sia un'importante fattore di successo per la realizzazione della cartella stessa. *ASI*, *FSAS* e *SWOR* propongono di verificare anche la possibilità di sostegno da parte delle autorità nazionali. Secondo il Cantone *AG* è necessario un service desk per i pazienti. La consulenza, i reclami e i servizi di ombudsman provocano tuttavia un notevole onere supplementare. *FRC* ritiene essenziale che le comunità di riferimento designino un servizio di assistenza ai pazienti per aiutarli nell'impiego della loro cartella informatizzata. D'altra parte è anche importante che il paziente disponga di diversi supporti e servizi d'informazione, anche al di fuori della comunità, per evitare conflitti di interesse e garantire una migliore indipendenza dell'informazione fornita. L'obiettivo è un eccellente coordinamento dei flussi d'informazione.

KSSG s'informa sui requisiti riguardanti i tempi di reazione. Per la costituzione di un service desk, una comunità di riferimento deve impiegare circa 2-3 collaboratori per ridurre i tempi di attesa. Se i tempi di reazione sono un elemento della certificazione, questo articolo va ripreso nelle CTO. *VGIch* scrive che le stesse prescrizioni valgono anche per la verbalizzazione, come per i professionisti della salute. Su questo punto l'ordinanza è lacunosa e il commento esplicativo troppo vago. Bisogna assicurare l'interoperabilità. Gli accessi devono essere protocollati da tutti. *H+* fa notare che, ai fini dell'attuazione pratica negli ospedali, è necessario designare dei responsabili della cartella informatizzata del paziente come punto di contatto per i pazienti. Non è realistico affidare questo compito a ogni professionista della salute. La specializzazione delle mansioni richiede anche una formazione continua. Nell'ambito dei «Dati da fornire per la valutazione» bisognerebbe verificare come analizzare e quantificare questo onere supplementare.

Art. 20 Aufhebung des elektronischen Patientendossiers

[1] Ein elektronisches Patientendossier wird von der Stammgemeinschaft aufgehoben, wenn:

a. die Patientin oder der Patient die Einwilligung zu dessen Führung widerruft;

b. während 10 Jahren niemand darauf zugreift; oder

c. die Patientin oder der Patient verstorben ist.

[2] Dazu muss die Stammgemeinschaft sämtliche Zugriffsrechte auf das entsprechende Patientendossier entziehen und:

a. im Fall der Aufhebung:

1. alle Gemeinschaften sowie die ZAS innert angemessener Frist über die Aufhebung informieren,

2. die Widerrufserklärung während 10 Jahren aufbewahren;

b. im Fall der Nichtnutzung nach Absatz 1 Buchstabe b die Patientin oder den Patienten 3 Monate vor der Aufhebung informieren.

VAKA ricorda il collegamento con il numero 12.14.1 CTO e scrive che una revoca o un'uscita senza formalità non è conforme al dovere di conservazione (10 anni). La revoca senza formalità deve essere corretta con: «nicht ganz formlos». 6 Cantoni[53] scrivono che non si deve sopprimere una cartella informatizzata del paziente per motivi di economicità. Considerato quanto costa tutto il resto non bisogna risparmiare nelle cose sbagliate. Aggiungono che i termini per la conservazione dei dati e della cartella informatizzata del paziente pregiudicano la necessità stessa di disporre di una cartella informatizzata del paziente, che deve invece appartenere al paziente per tutta la vita e contiene tutti i suoi dati medici utili per futuri trattamenti. *HIN* fa notare che non ha senso cancellare i dati dopo 10 anni, tanto più che oggi i fattori di rischio e le informazioni mediche sul paziente possono essere conosciuti molto prima. *CMC*, *KAeG SG*, *BüAeV* e *GAeSO* constatano che secondo l'articolo 20 i dati di cui all'art. 9 cpv. 1 lett. b devono essere cancellati, mentre i dati verbalizzati devono essere conservati per 10 anni. Stando al numero 2.10.2 CTO i dati verbalizzati non contengono dati medici. Chiedono come è possibile determinare in un secondo tempo tramite i dati verbalizzati chi, quando e quali dati sono stati consultati e se i dati che dovrebbero essere cancellati in caso di revoca non dovrebbero essere custoditi in un'area separata dell'archivio, alla quale i professionisti della salute non hanno accesso. *K3* e *VZK* propongono che la soppressione della cartella informatizzata del paziente non avvenga immediatamente, ma solo dopo un determinato periodo. Ciò consentirebbe agli aventi diritto di memorizzare i dati in caso di bisogno, p. es per accertamenti genetici. *Privatim* chiede che l'ordinanza stabilisca espressamente che tutte le parti coinvolte nella cartella informatizzata del paziente possano trattare i dati personali contenuti nella cartella informatizzata del paziente esclusivamente per l'adempimento dei compiti che sono loro attribuiti dalla LCIP o da un altro atto normativo ad essa legato. Questo principio può essere desunto dall'articolo 4 capoverso 3 della legge sulla protezione dei dati (LPD), ma merita di essere esplicitato nell'ordinanza per la tipologia dei dati personali ottenuti nel contesto della cartella informatizzata del paziente. Concretamente propone la seguente formulazione: «1. Alle mit dem Aufbau, dem Betrieb und der Nutzung des elektronischen Patientendossiers betrauten Personen oder Institutionen dürfen die in dessen Zusammenhang anfallenden Personendaten ausschliesslich zum Zweck der ihnen durch das EPDG samt den dazugehörenden Ausführungserlassen übertragenen Aufgaben oder gestützt auf eine andere, hinreichend bestimmte gesetzliche Grundlage bearbeiten. 2. Eine Weitergabe von Personendaten zu Werbezwecken ist in jedem Fall untersagt». Secondo il Cantone *AG* le prescrizioni sulla revoca, la cancellazione e il termine di conservazione di 10 anni sono plausibili; il termine di conservazione di 10 anni è opportuno dal punto di vista del diritto probatorio. Importante è il preavviso del paziente 3 mesi prima della cancellazione. *Lovis* è del parere che la cartella informatizzata del paziente non dovrebbe mai essere cancellata.

Capoverso 1: Secondo *IG eHealth*, *PH CH* ed *economiesuisse* l'attuale formulazione sulla soppressione della cartella informatizzata del paziente potrebbe permettere la cancellazione automatica e irrevocabile dei dati medici del paziente senza che questi ne sia informato. Poiché, a seconda della legislazione cantonale, anche i dati dei sistemi primari dovrebbero essere cancellati, si potrebbe verificare una perdita indesiderata di dati. Propongono di aggiungere la seguente lettera all'inizio del capoverso: «a. nach unbeantwortetem Verstreichen einer Frist von 90 Tagen auf schriftliche Aufhebungsmitteilung an den Patienten, seine Vertreter und seinen Arzt des Vertrauens (Hausarzt)». La lettera c dovrebbe avere il

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

seguente tenore: «c. von einer Gesundheitsfachperson oder Hilfsperson das Todesdatum erfasst wurde und eine Amtsstelle, ein Angehöriger oder ein Vertreter des Patienten der Stammgemeinschaft den Tod des Patienten bescheinigt hat.» Le attuali lettere a – c diventerebbero le lettere b – d. *STSAG* propone di modificare il brano di frase «kann von der Stammgemeinschaft aufgehoben werden» poiché, non essendo previsto un obbligo di notifica, la comunità di riferimento può non essere a conoscenza del decesso. La cancellazione di documenti e la soppressione della cartella informatizzata (salvo in caso di decesso) dovrebbero essere prerogativa unica del paziente. Come alternativa, tutti i documenti potrebbero essere cancellati se sono stati inseriti più di 10 anni prima nella cartella informatizzata del paziente (rimarrebbero però nel sistema primario ed eventualmente potrebbero essere reinseriti nel repository in un secondo momento con un onere amministrativo minimo). Secondo *SUVA* la soppressione ha senso solo se il paziente revoca il consenso alla tenuta della sua cartella informatizzata.

Capoverso 1 lettera a: *Tessaris* è del parere che la revoca debba soddisfare gli stessi requisiti del consenso alla gestione della cartella informatizzata del paziente. La dichiarazione di revoca dovrebbe essere tale da soddisfare anche i r equisiti del capoverso 2 lettera a numero 2. *Tessaris* propone la seguente formulazione per la lettera a: «[…] dessen Führung durch unterschriftlich oder durch eine an die behandelnde Gesundheitsfachperson abgegebene und von dieser protokollierte und unterzeichnete Erklärung widerruft».

Capoverso 1 lettera b: *LUKS* scrive che sopprimere la cartella informatizzata del paziente dopo 10 anni dall'ultimo accesso è in contraddizione con il principio di una cartella valida per tutta la vita e con lo scopo stesso della cartella informatizzata del paziente. Secondo *FMH* ciò non è nell'interesse del paziente, né corrisponde allo spirito della legge. Per *SSIM* non ha senso una cancellazione generalizzata in caso di non accesso, mentre *Insel* considera inadeguato il termine di 10 anni. *Insel* aggiunge che è sempre possibile far cancellare i dati (art. 20 cpv. 1, lett. a) e che, per motivi di chiarezza, le conseguenze della soppressione, ovvero cancellazione di tutti i dati, dovrebbero essere menzionate espressamente nel capoverso 2 lettera a numero 3. Il termine dovrebbe essere prolungato a 20 anni, anzi preferibilmente dovrebbe essere cancellato completamente come impostazione default.

HÄ CH e *ÄTG* fanno notare che questa disposizione vale solo previa dichiarazione di consenso del paziente e dopo aver informato per tempo il medico curante. A questo proposito rimandano al commento sull'articolo 9 capoverso 1. Lo stesso vale anche per il capoverso 2 lettera b. *ASPS* e *Spitex* ritengono che, se il tempo di conservazione è limitato, per le persone sane non ha senso aprire una cartella informatizzata del paziente. Le persone che hanno subito un evento acuto, ma rimangono poi in buona salute per 10 anni perderebbero la loro registrazione. Bisognerebbe omettere il limite temporale o stralciare i due capoversi. *KSOW* osserva che fra una registrazione e il prossimo caso possono trascorrere 10 anni. I dati non devono quindi essere cancellati automaticamente. Occorre sempre il consenso del paziente. *ASI*, *FSAS* e *SWOR* sono a favore di un rinnovo automatico della cartella informatizzata del paziente, salvo ordine contrario del paziente. *Bleuer* scrive che, se il paziente non stabilisce altrimenti, la cartella informatizzata deve essere conservata per almeno 10 anni dopo la sua morta accertata. *SMCF* segnala che dovrebbe essere possibile solo la disattivazione della cartella informatizzata del paziente e non la sua soppressione automatica. Prima della distruzione dei dati medici si dovrebbero inoltre applicare i termini consueti. Complessivamente 13 partecipanti[54] chiedono lo stralcio della lettera b, *Moeri* la definisce obsoleta.

Capoverso 1 lettera c: 7 partecipanti[55] avvertono che non è chiaro come la comunità di riferimento venga a conoscenza del decesso del paziente. Chiedono di considerare l'eventuale introduzione di un dovere di notifica da parte dell'UCC e, a seconda del risultato di tale verifica, modificare la lettera c e l'articolo 9 capoverso 1 lettera b. *Privatim*, *DSBAG* e i Cantoni *AG* e *BE* desiderano che si esamini l'opportunità di un termine transitorio di diversi anni dopo il decesso di un paziente. Anche *SSIM* osserva che in determinate circostanze può essere importante accedere alla cartella informatizzata di un paziente defunto e chiede di definire un termine adeguato nella lettera c. *LUKS* avanza la stessa richiesta e propone

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

[55] privatim, DSBAG, KDSBSON, BE, SZ, ZG, AG

un termine p.es. di tre mesi. Dovrà inoltre essere definita la possibilità di consegnare i documenti del defunto ai familiari. *KSSG* obietta che la morte di un paziente non viene comunicata attivamente a un fornitore di prestazioni. Per precisare quando decorre l'obbligo di soppressione della cartella, propone la seguente aggiunta alla lettera c: «Bei Erlangung der Kenntnis, dass die Patientin […]».*Posta* desidera un chiarimento su come le comunità di riferimento apprendono del decesso. Anche il Cantone *ZH* e *ZAD* chiedono di chiarire come le comunità di riferimento vengono informate dell'avvenuto decesso, e sottolineano che la cartella informatizzata di un paziente deceduto non può essere resa accessibile a persone che il defunto non abbia espressamene nominato come suoi rappresentanti – cosa che vale anche per i familiari. Anche *K3* e *VZK* obiettano che le strutture sanitarie e i professionisti della salute non vengono necessariamente a conoscenza del decesso di un paziente. Sarebbe opportuno che l'UCC inviasse una notifica alle comunità di riferimento quando apprende del decesso. *FMH* sostiene che la cartella informatizzata non dovrebbe essere soppressa subito dopo la morte del paziente. Il diritto vigente prevede la possibilità di far valere pretese per errori terapeutici fino a 10 anni dopo il trattamento. Per la soppressione occorre trovare una soluzione giuridicamente coerente per le questioni di responsabilità civile/conservazione dei dati. *SUVA* chiede lo stralcio della lettera c. 6 Cantoni[56] chiedono se la cartella informatizzata del paziente può avere un interesse medico-legale. Ipotizzano la possibilità di mantenerla nascosta e inaccessibile per un determinato periodo (p. es. 10 anni), per poi cancellarla definitivamente.

Capoverso 2: *Integic*, *HL7* e *IHE* desiderano la seguente aggiunta al capoverso 2: «[…] entsprechende Patientendossier sofort entziehen und […]». *KSSG* chiede in quale forma le comunità di riferimento debbano informare le comunità sulla soppressione della cartella informatizzata del paziente. Finora per questa funzione non sono stati definiti dei profili d'integrazione IHE, ma questa lacuna deve essere colmata.

Capoverso 2 lettera a: *CURAVIVA*, *Insos* e il Cantone *TG* segnalano che la nozione di termine adeguato è troppo vaga e propongono la seguente aggiunta al numero 1: «[…] ZAS innert einem Monat von der Aufhebung informieren». *HL7* e *IHE* chiedono di aggiungere i seguenti numeri alla lettera a: «3. die Vernichtung der Daten gemäss Artikel 9 Buchstabe b frühestens 10 Tage und spätestens 60 Tag nach der Aufhebung durchzuführen» e «4. Auf Gesuch hin die angeordnete Vernichtung der Daten um 60 Tage auszusetzen. Als Gesuchsteller gelten die Patientin oder der Patient, eine Erbengemeinschaft, welche sich mittels Erbbescheinigung ausweisen kann oder ein Willensvollstrecker, der sich mittels Willensvollstreckerzeugnis ausweist.» *Medshare* propone esattamente gli stessi nuovi numeri, ma con la differenza che al numero 3 chiede «frühestens 30 Tage». Secondo *Physioswiss* il processo non può consistere nell'informare tutte le comunità sulla soppressione di una cartella informatizzata del paziente. Questa disposizione va cancellata ed eventualmente sostituita da un altro processo. Lo stralcio è chiesto anche da *FMH*, la quale fa notare che una comunità può eventualmente venire a conoscenza dell'esistenza della cartella informatizzata del paziente solo quando le viene annunciata la sua cancellazione. Non si dovrebbero cancellare i dati negli archivi locali né annullare il NIP. Ciò renderebbe superflua l'informazione alla comunità e anche all'UCC. *Posta* fa notare che non è chiaro come debba avvenire la soppressione della cartella informatizzata del paziente in tutte le comunità. Solo la comunità di riferimento dovrebbe sopprimere la cartella. Secondo *VGIch* non è chiaro lo scopo dell'obbligo d'informazione a tutte le comunità. Se necessario potrebbe essere l'UCC – eventualmente in forma automatizzata – a informare le altre comunità. Una revoca dovrebbe essere valida a effetto immediato. Un altro punto da chiarire è l'interpretazione del termine adeguato di cui all'articolo 20. Le CTO ripetono la nozione dell'adeguatezza, ma le CTO dovrebbero definire i requisiti tecnici e organizzativi della certificazione e non interpretare l'ordinanza. È consigliabile indicare un termine (p. es. un mese) nell'OCIP stessa. Riguardo alla lettera a numero 2, *Posta* preferirebbe la seguente formulazione: «den Nachweis der Widerrufserklärung[…]».6 Cantoni[57] scrivono che, in caso di soppressione della cartella informatizzata del paziente, il NIP dovrebbe essere mantenuto come indicato all'articolo 9. In questo caso non sarebbe necessario informare l'UCC. Di conseguenza propongono il seguente testo della lettera a numero 1: «[…] les communautés dans un délai approprié». *FMH* rimanda al suo commento sull'articolo

[56] GE, VS, VD, JU, FR, NE
[57] GE, VS, VD, JU, FR, NE

9 e chiede cosa significa «soppressione». Inoltre non è chiaro come gestire gli aspetti medico-legali in caso di soppressione dopo revoca del consenso.

Capoverso 2 lettera b: *ÄTG*, *ASPS* e *Spitex* ripetono il parere espresso sul capoverso 1 lettera b. Per *FMH* questa soluzione non è praticabile. Se la cartella informatizzata rimane inutilizzata per 10 anni vi è una buona probabilità di non poter raggiungere il paziente. La lettera b va quindi cancellata, come chiede anche *SUVA.* Anche 6 Cantoni[58] chiedono lo stralcio della lettera b. Secondo loro sarebbe auspicabile che dopo 10 anni dall'ultimo accesso non siano più validi neanche i dati personali (indirizzo, numero di telefono, ecc.). Secondo *Moeri* la lettera b è obsoleta. *SBC* chiede che i pazienti siano informati già 6 mesi prima della soppressione.

Sezione 3: Datenlieferung für die Evaluation

Art. 21

[1] Gemeinschaften und Stammgemeinschaften müssen dem BAG regelmässig Daten für die Evaluation nach Artikel 18 LCIP zur Verfügung stellen.

[2] Das EDI legt die zu liefernden Daten fest.

Medshare avverte che manca il titolo dell'articolo. 7 partecipanti[59] scrivono che la disposizione deve essere precisata dal punto di vista della protezione dei dati. L'UFSP dovrebbe essere autorizzato solo a trattare i dati in forma anonimizzata. L'elenco dell'allegato 6 dell'OCIP-DFI mostra che i dati anonimizzati sarebbero sufficienti al rilevamento delle informazioni desiderate. Propongono di lasciare immutato il capoverso 1 e di trasformare il capoverso 2 in capoverso 3. Per il nuovo capoverso 2 propongono la seguente formulazione: «Das BAG darf die Daten nur in anonymisierter Form bearbeiten. Die Gemeinschaften und Stammgemeinschaften sind verpflichtet, die Daten vor der Auslieferung an das BAG zu anonymisieren oder anonymisiert zu lassen». Sulla stessa falsariga anche il Cantone *ZH* e *ZAD* scrivono che all'UFSP devono essere forniti solo dati in forma anonimizzata e che la valutazione prevista all'articolo 18 non richiede dati non anonimizzati. Propongono pertanto la seguente aggiunta al capoverso 1: «Gemeinschaften und Stammgemeinschaften stellen dem BAG regelmässig anonymisierte Daten für […]». *Medgate* chiede quanto affidabile deve essere il controllo che gli indicatori non consentano di risalire a singoli professionisti della salute o pazienti. Di norma, i dati possono essere forniti solo in forma anonimizzata. *LUKS* e *FMH* desiderano limitare al minimo indispensabile il volume di dati da fornire e aggiungono che l'onere necessario deve essere finanziato. Secondo *FMH* la cartella informatizzata del paziente non deve essere fine a sé stessa, bensì contribuire agli scopi definiti nella LCIP (art.1, cpv. 3 LCIP) e soddisfare i criteri di idoneità, efficacia ed economicità. Oltre a conformare l'ordinanza a questi obiettivi, occorre elaborare un concetto di valutazione con criteri e indicatori trasparenti. Solo dopo si potranno stabilire i dati necessari alla valutazione. I parametri riportati nell'allegato 6 OCIP-DFI non sono adatti a valutare il raggiungimento degli scopi definiti nella LCIP. *Physioswiss* sottolinea che i criteri devono essere trasparenti. Per *IG eHealth* e *PH CH* il capoverso 2 dovrebbe essere completato come segue: «[…] Daten sowie die Fristen für die Einreichung der zu liefernden Daten gemeinsam mit den betroffenen Kreisen fest». Anche *medshare* desidera fissare la periodicità e i termini, mentre *HL7* e *IHE* scrivono che la periodicità deve essere indicata al più tardi nell'allegato assieme ai dati da fornire. *VGIch* osserva che le clausole di valutazione, che sono indirizzate alle autorità federali, devono contenere almeno l'indicazione dei seguenti elementi: autorità incaricata di stilare il rapporto, destinatari dei risultati della verifica, momento della verifica, prodotto finale, criteri della verifica e oggetto della verifica. Queste esigenze non sono soddisfatte con l'uso del semplice aggettivo «regelmässig». *UDC* constata che la formulazione non specifica in quale intervallo di tempo le comunità devono fornire i dati per la valutazione. Sia la frequenza che l'entità dei dati da presentare devono essere stabilite in modo tale da non causare un onere sproporzionato alle comunità. *SSIM* critica che questa disposizione generica sui dati da fornire lascia aperta una scappatoia per un controllo indiretto dei fornitori di prestazioni e una raccolta eccessiva di dati. I dati da fornire devono essere limitati allo stretto necessario, cioè a quanto serve per una statistica anonima sull'impiego della cartella. Il capoverso 2 non deve dare mano libera al DFI.

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

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

STSAG definisce l'articolo 21 come un assegno in bianco e lo respinge in questa forma. Chiede di assicurarsi che nell'OCIP-DFI i requisiti non siano gonfiati a dismisura. *VAKA*, *K3* e *VZK* ricordano che la costituzione di una comunità di riferimento è già onerosa e costosa a causa degli elevati requisiti della certificazione. Con l'articolo 21 le comunità di riferimento subiscono nuove pressioni finanziarie senza trarne alcun beneficio. *VAKA* scrive inoltre che la valutazione della LCIP è incontestata, ma il grado di dettaglio e il tipo di emissione dei dati non meritano un appoggio. Per questo motivo chiede lo stralcio dell'articolo. Anche *K3* e *VZK* desiderano un approccio più restrittivo nella definizione dei requisiti in materia di dati. *SWOR*, *ASI* e *FSAS* considerano particolarmente preziosa la valutazione prevista, perché fornirà importanti spunti per valutare lo sviluppo della cartella informatizzata del paziente e mostrare eventuali necessità d'intervento.

3.1.4 Capitolo 4: Identifikationsmittel

Art. 22	Anforderungen an das Identifikationsmittel
Das Identifikationsmittel muss:	
a.	der Vertrauensstufe 3 der Norm ISO/IEC 29115:2013(E) entsprechen;
b.	so aufgebaut sein, dass es nur von der berechtigten Person verwendet werden kann;
c.	ein Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens zwei Authentifizierungsfaktoren verwenden; und
d.	eine Gültigkeitsdauer von höchstens zehn Jahren aufweisen.

10 partecipanti[60] considerano che i requisiti riguardanti lo strumento d'identificazione (SID) siano molto elevati. Il diritto d'esecuzione dovrebbe consentire l'uso dei SID già utilizzati negli ospedali, purché soddisfino determinati criteri. Un professionista della salute che lavora in ospedale non dovrebbe essere costretto a impiegare diversi login e sistemi di accesso. Chiedono pertanto di riconsiderare i requisiti sul SID per i professionisti della salute che lavorano negli ospedali. *Posta* auspica che là dove il personale ospedaliero applica SID validi secondo la legislazione cantonale, questi SID possano essere impiegati anche per la cartella informatizzata del paziente. Anche *VAKA* rimanda alle soluzioni già esistenti per i SID e chiede di chiarire dove e secondo quali criteri tali soluzioni possano essere utilizzate anche per l'accesso ai dati LCIP. Analogamente il Cantone *LU* chiede una revisione dell'articolo, perché esso obbliga a dotare il personale di nuovi e costosi SID per accedere alla cartella informatizzata del paziente. *Medgate* ritiene che in molti casi i requisiti posti alla conferma dell'identità e al SID siano eccessivi e quindi poco praticabili, e auspica una procedura semplificata. *SSIM* preferisce l'impiego dei SID esistenti, che sono già ampiamente diffusi. *PKS* fa notare che le disposizioni sui SID non corrispondono ai processi che i reparti del personale praticano negli ospedali per le entrate e le uscite di professionisti della salute. Nel lavoro quotidiano bisognerebbe potersi affidare alle procedure di autenticazione disponibili e consentire l'impiego dei SID già esistenti e ampiamente diffusi. *IG eHealth*, *PH CH* ed *economiesuisse* chiedono di completare l'articolo 22 con una disposizione transitoria o di modificarlo come segue: «In all jenen stationären Einrichtungen, in welchen die Gesundheitsfachpersonen ein nach kantonalem Recht gültiges IDM für den Zugriff auf Patientendaten einsetzen, kann dieses IDM auch für den Zugriff auf das elektronische Patientendossier verwendet werden». *HÄ CH* e *ÄTG* sono a favore di una soluzione pragmatica e soprattutto facilmente applicabile nella pratica quotidiana, che permetta di risparmiare tempo e denaro. Un'assegnazione dei diritti snella e delle regole semplici per il personale degli ambulatori permetterebbero ai medici di evitare i compiti di segreteria legati alle autorizzazioni di accesso. Secondo *K3* e *VZK* dovrebbe essere possibile che il sistema «cartella informatizzata del paziente» abbia «fiducia» nell'ospedale. Per gli ospedali è importante, nel loro lavoro quotidiano, non dover ricorrere a un'altra procedura di autenticazione per l'accesso alla cartella informatizzata del paziente, bensì poter semplicemente «completare» la procedura già utilizzata internamente. A questo scopo la procedura interna dovrebbe soddisfare determinati requisiti (p. es. lunghezza della password) ed essere poi completata con un terzo fattore per l'accesso alla cartella informatizzata del paziente. Sulla stessa falsariga, UDC evidenzia l'inutilità di limitarsi a pochi SID concreti. Gli strumenti di autenticazione già esistenti negli istituti potrebbero essere impiegati anche per l'accesso alla cartella informatizzata del paziente. *VAKA* e il Cantone *AG* osservano che non dovrebbe essere necessario un colloquio personale per la registrazione del SID, perché ciò scoraggerebbe molti pazienti e professionisti della salute.

[60] NW, LU, Posta, SZ, ZG, ZH, ZAD, IG eHealth, PH CH, economiesuisse

Articolo 22 lettera a: *BRH* fa notare che il controllo delle norme ISO non è garantito tramite l'UFSP. Oltre a fornire indicazioni trasparenti sulle norme citate, si dovrebbe garantire un accesso semplice e una descrizione dei processi e delle istanze di controllo di tali norme. *CURAVIVA*, *Insos* e *senesuisse* criticano il rimando a una norma ISO/IEC perché viola il principio di legalità; anche il Cantone *TG* si chiede se il rinvio a una norma ISO/IEC sia legale in un'ordinanza. I suddetti partecipanti sono comunque del parere che questo rimando viola il principio della trasparenza dei testi di legge, tanto più che il contenuto di queste norme è difficilmente accessibile. Secondo il Cantone *TG,* il grado di riservatezza 3 dovrebbe soddisfare altre caratteristiche di qualità, che l'OCIP prevede espressamente. Lo stesso vale anche per l'accreditamento, la protezione dei SID e la procedura di autenticazione. Anche *Posta* è del parere che non si dovrebbe prescrivere una norma specifica a livello di ordinanza. Basterebbe determinare dei requisiti solidi nell'ordinanza e affidare a un ufficio federale a indirizzo tecnico la competenza di definire i requisiti nel dettaglio. Chiede pertanto di stralciare la lettera a e di armonizzare la disposizione con la legge federale sulla firma elettronica (FiEle). Secondo *ISSS* bisognerebbe assicurare che gli emittenti mettano a disposizione i SID elettronici a tempo debito, nella qualità e quantità richieste. Ciò è però possibile solo se vengono impiegati i SID già riconosciuti e certificati oggi, senza chiedere nuovi SID basati su standard diversi. Nel suo parere *ISSS* attira altresì l'attenzione sugli strumenti già disponibili in Svizzera e in Europa per un'autenticazione sicura. Questi strumenti non si basano necessariamente sulla norma ISO/IEC29115. Auspica l'applicazione dei SID elettronici già definiti e ricorda che per la definizione di ulteriori SID dovrebbe essere determinante lo standard eCH. La lettera a dovrebbe quindi leggere: «a. einer der folgenden Normen oder Vorschriften entsprechen: - Qualitätsstufe 3 der eCH-0170 Norm; - geregeltes Zertifikat gemäss ZertES; - Suisse ID Authentisierungs-Zertifikat gemäss eCH-0113 Spezifikation; - eIDAS». Analogamente, *SQS* chiede di sostituire ISO/IEC29115 con la firma elettronica secondo FiEle.

Articolo 22 lettera c: *Posta* chiede una precisazione nell'ordinanza, per specificare che mTAN è un possibile SID. *SPO* è favorevole a una procedura di autenticazione secondo l'attuale stato della tecnica con almeno due fattori di autenticazione. La sicurezza dell'accesso ai dati sensibili dovrebbe essere almeno equivalente a quella delle banche. *HIN* apprezza il livello di sicurezza adeguato alla situazione e il vincolo di un'autenticazione a due fattori. Anche in ambito stazionario si dovrebbero applicare requisiti di sicurezza analoghi a quelli dei SID ampiamente diffusi fra i professionisti della salute che lavorano in campo ambulatoriale e come liberi professionisti. In qualità di IPD, *HIN* dichiara di disporre di soluzioni ed esperienza nell'impiego in grandi istituti stazionari. *SSIM* chiede di rinunciare a un'autenticazione a due livelli.

Articolo 22 lettera d: 6 partecipanti[61] fanno notare che una validità massima di 10 anni è molto lunga considerati i rapidi progressi della tecnica e lamentano la mancanza di considerazioni approfondite su questo punto nel rapporto esplicativo. Chiedono di riconsiderare il termine massimo di 10 anni. *DSBAG* propone concretamente un termine massimo di due anni, il Cantone *BE* di 5 anni. *VAKA* e *Posta* auspicano la soppressione di questa norma. Se comunque si dovesse ritenere necessaria un'indicazione temporale, secondo *Posta* questa dovrebbe essere disciplinata nell'articolo 25 e armonizzata con altre leggi.

Art. 23 Identitätsprüfung

[1] Der Herausgeber des Identifikationsmittels muss die Identität der antragstellenden Person überprüfen. Diese muss sich mit einem Ausweis nach dem Ausweisgesetz vom 22. Juni 2001 oder einem Ausweis nach den Artikeln 41–41b des Ausländergesetzes vom 16. Dezember 2005 ausweisen oder einen mit einer qualifizierten elektronischen Signatur nach dem Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur signierten Antrag auf elektronischem Weg einreichen.

[2] Wird das Identifikationsmittel für die Authentifizierung einer Gesundheitsfachperson verwendet, so muss zusätzlich überprüft werden, ob es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b LCIP handelt.

[3] Die Prüfung der Identität der antragstellenden Person nach Absatz 1 und der Qualifikation einer Gesundheitsfachperson nach Absatz 2 kann an Dritte delegiert werden.

61 DSBAG, privatim, KDSBSON, FR, ZG, BE

PKS e *SSIM* criticano, alla stessa stregua che per l'articolo 22, gli elevati ostacoli posti alla verifica dell'identità, sottolineando che bisognerebbe servirsi di metodi ben collaudati e affermati. *Posta* obietta invece che gli elevati requisiti proposti nell'avamprogetto per i SID sono in contraddizione con le esigenze molto più blande poste alla verifica dell'identità. Chiede che vengano applicati gli stessi criteri come quelli stabiliti nel progetto di revisione della OFiEle per i certificati regolamentati. Secondo *STSAG*, la verifica dell'identità dovrebbe essere risolta in modo più pragmatico: basterebbe far verificare l'identità da parte dell'istituzione (al momento dell'assunzione), definire il ruolo (p. es. in SIC) e consentire l'accesso con una validazione tecnica (p. es. HIN access gateway). L'identificazione / autenticazione nel sistema primario, aggiunta a un'infrastruttura di accesso sicura, potrebbe essere impiegata come autenticazione a due fattori, per poter consultare la cartella informatizzata di un determinato paziente senza ulteriori richieste di conferma dell'identità.

Capoverso 1: *Medgate* ripete il suo commento sull'articolo 22. 6 Cantoni[62] formulano la seguente proposta per l'articolo 23 capoverso 1: «L'éditeur ou la communauté est tenu de vérifier l'identité de la personne qui demande un moyen d'authentification». *ISSS* scrive che la definizione dei requisiti per la verifica dell'identità è parte integrante della rispettiva norma/regolamentazione (eCH-0170, eCH-0113, FiEle, eIDAS) e avanza la seguente proposta per il capoverso 1: «[…] antragsstellenden Person gemäss der jeweiligen Norm, unter der das IDM herausgegeben wird, überprüfen. […]». *Spitex* e *ASPS* obiettano che numerosi clienti di Spitex sono molto anziani e non hanno più una carta d'identità o una patente valida. Per loro è difficoltoso procurarsene una nuova, per cui occorre prevedere un'altra possibilità d'identificazione. Come nelle sue osservazioni sull'articolo 5 capoverso 2, *Tessaris* attira l'attenzione sulle persone che soggiornano in Svizzera, ma non hanno un numero di assicurato e fa notare che per questi casi è necessario ammettere anche altri modi di prova dell'identità.

Capoverso 2: *VAKA* parte dal presupposto che per questa verifica non siano stati ancora precisati né la procedura né i dati richiesti. L'UFSF dovrebbe definire chiaramente come deve svolgersi una tale verifica. *Spitex* e *ASPS* fanno notare che, finché non tutti gli infermieri sono iscritti in un registro, l'identificazione secondo l'articolo 2 lettera b LCIP è molto dispendiosa. L'ordinanza dovrebbe prevedere o disciplinare un registro per le professioni sanitarie. *FMH* chiede di non utilizzare un attributo unico «professionista della salute», ma di distinguere fra le varie categorie professionali. Anche *HIN* sostiene che l'attributo «professionista della salute» dovrebbe essere completato con il rispettivo tipo di professione medica in collaborazione con le associazioni professionali.

Capoverso 3: Secondo *K3* e *VZK*, il capoverso 3 deve essere interpretato nel senso che un ospedale o una casa di cura identifica i suoi collaboratori e può anche verificare se si tratta di professionisti della salute. Altre soluzioni sarebbero impraticabili e troppo care. *ASI* e *SWOR* approvano l'attribuzione del GLN ai professionisti della salute. La soluzione potrebbe consistere nella tenuta di un registro professionale nazionale per i professionisti della salute. *FMH* respinge la delega della verifica della qualificazione di un professionista della salute a terzi qualsiasi, perché ciò comporta un rischio da evitare. La responsabilità dovrebbe spettare a servizi qualificati, di cui bisognerebbe definire i requisiti.

Art. 24 Daten des Identifikationsmittels

[1] Der Herausgeber des Identifikationsmittels erfasst folgende Daten anhand des vorgelegten Identitätsnachweises der antragstellenden Person:

a. den Namen;
b. die Vornamen;
c. das Geschlecht;
d. das Geburtsdatum;
e. die Nummer des Identitätsnachweises nach Artikel 23 Absatz 1.

[2] Er kann bei Gesundheitsfachpersonen zusätzlich die eindeutige Identifikations-nummer (GLN) erfassen.

[3] Er kann die Angaben nach den Absätzen 1 und 2 zur Identifizierung an die Zugangsportale übermitteln.

[4] Er informiert die antragstellende Person über die Sicherheitsvorkehrungen, die sie im Umgang mit dem Identifikationsmittel treffen muss.

62 FR, NE, VS, VD, JU, GE

Posta fa notare che nel primo capoverso, fra l'elenco dei dati, manca il NAVS13. Questo attributo dovrebbe essere messo a disposizione dall'IDP solo per la cartella informatizzata del paziente e non per altri scopi. Senza queste indicazioni non è possibile semplificare il processo di registrazione per i pazienti. Se i requisiti non venissero aumentati, i pazienti dovrebbero affrontare dei processi di registrazione complessi e ne trarrebbero meno vantaggio. Il tutto comporterebbe maggiori costi per i SID, senza alcun valore aggiunto. *Posta* chiede che sia consentita almeno una possibilità di registrazione. Questa potrebbe essere impiegata anche per una verifica dell'identità non legata alla cartella informatizzata del paziente, ma potrebbe essere utilizzata solo nel contesto della cartella informatizzata del paziente. Riguardo al capoverso 1 lettera e, *Posta* aggiunge che non andrebbe registrato solo il numero della verifica dell'identità, bensì anche il tipo di documento; chiede quindi che nella definizione dei metadati venga registrata un codice per il documento d'identità. *FMH* desidera che nella lettera e il numero del documento d'identità sia sostituito con il GLN e che il capoverso 2 sia soppresso. Riguardo alla lettera e, *Tessaris* ripete il suo commento sull'articolo 23 capoverso 1. Secondo 6 Cantoni[63] il documento d'identità deve essere controllato, ma il numero non deve essere registrato. Sarebbe una perdita di tempo e non vi è motivo per memorizzare questo dato. Chiedono lo stralcio della lettera e. *Tessaris* ritiene, in linea con le sue osservazioni sull'articolo 14 capoverso 2, che l'obbligo d'informazione previsto al capoverso 4 comporti un certo rischio di responsabilità per l'emittente del SID. Per i titolari di chiavi crittografiche bisogna inoltre segnalare le norme di responsabilità secondo l'articolo 59a CO.

Art. 25	Erneuerung der Gültigkeitsdauer des Identifikationsmittels
[1] Das Identifikationsmittel kann vor Ablauf seiner Gültigkeitsdauer erneuert werden.	
[2] Der Herausgeber überprüft bei der Erneuerung des Identifikationsmittels nach Artikel 23 die Identität der antragstellenden Person.	

6 Cantoni[64] fanno notare che vi è confusione fra identificazione e autenticazione. L'articolo 25 deve essere modificato come segue: «Renouvellement de la durée de validité du moyen d'authentification. 1. 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* e *ÄTG* scrivono che, per ridurre onere e costi, la durata di validità dovrebbe essere il più lunga possibile (non inferiore a 3, minimo 2 anni).

Capoverso 2: *VAKA* sostiene che se una persona è stata identificata già una volta con un documento secondo l'articolo 23 capoverso 1, non è necessaria una nuova verifica del documento al momento del rinnovo. La nuova verifica del documento deve essere soppressa. Anche *LUKS*, *FMH* e *SSIM* ne chiedono la soppressione. Secondo 8 partecipanti[65] la nuova verifica di una persona è superflua se il SID è ancora valido. *IG eHealth* e *PH CH* propongono la seguente modifica del capoverso 2: «Verliert ein IDM seine Gültigkeit, so muss der Herausgeber des Identifikationsmittels für dessen Erneuerung nach Artikel 23 die Identität der antragstellenden Person neu überprüfen».

Art. 26	Sperrung des Identifikationsmittels
Das Identifikationsmittel kann von der Inhaberin oder dem Inhaber jederzeit unwiderruflich gesperrt werden.	

6 Cantoni[66] fanno notare che il titolare deve richiedere il blocco alla comunità. Non può farlo da solo. Propongono il seguente titolo per l'articolo 26: «Blocage du moyen d'authentification» e la seguente formulazione dell'articolo: «Le titulaire du moyen d'authentification peut demander de bloquer celui-ci à tout moment». Secondo *HÄ CH* e *ÄTG* bisognerebbe precisare che l'utente ha bisogno di sicurezza. L'onere legato al rinnovo e al cambiamento di provider deve essere limitato. Per *SCH* l'articolo 26 è troppo restrittivo. Questo punto dovrebbe essere disciplinato nel SID. A seconda delle circostanze il SID può essere impiegato anche per altre applicazioni. L'articolo 26 deve essere stralciato e, se necessario,

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

trasferito nell'allegato 5. *Tessaris* fa notare che non è prevista la forma della revoca e che pertanto è sufficiente anche una telefonata, un SMS o un'e-mail. Poiché secondo questa disposizione, il blocco è «irrevocabile», non è chiaro come il titolare debba agire dopo un blocco per smarrimento o furto del SID. *HIN* chiede che a ogni accesso alla cartella informatizzata del paziente si controlli se il SID è stato revocato (dichiarazione di nullità). Non è sufficiente disciplinare il blocco solo presso l'IDP. L'articolo 26 deve essere completato come segue: «Der Herausgeber führt eine Liste der gesperrten oder für ungültig erklärten IDM (Revokationstabelle). Die Gemeinschaft prüft bei jedem Zugriff, ob die Person korrekt authentisiert wurde und deren ID-Mittel nicht revoziert ist». *Posta* critica l'incompletezza della descrizione. L'emittente può bloccare un SID se viene informato in modo attendibile che le indicazioni non sono più valide. Vi è il pericolo che vengano create false attese. L'emittente dovrebbe poter bloccare un SID anche quando lui stesso o il titolare sospetta un abuso, per cui dovrebbero essere elencati i motivi per il blocco. Per permettere all'emittente del SID di accertarsi che la persona richiedente il blocco sia autorizzata a farlo, questa possibilità deve essere contemplata esplicitamente. Inoltre sarebbe auspicabile che il titolare venisse informato del blocco del SID per avere l'opportunità di individuare eventuali blocchi indesiderati.

3.1.5 Capitolo 5: Akkreditierung

Art. 27 Anforderungen

[1] Die Akkreditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung (AkkBV) vom 17. Juni 1996 sowie ISO/IEC 27006:201510, soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

[2] Je eine separate Akkreditierung ist erforderlich für die Zertifizierung von:

a. Gemeinschaften und Stammgemeinschaften;
b. Herausgeber von Identifikationsmitteln.

[3] Die Zertifizierungsstellen müssen neben den Voraussetzungen nach der AkkBV über eine festgelegte Organisation sowie ein festgelegtes Kontrollverfahren verfügen. Darin müssen insbesondere geregelt sein:

a. die Begutachtungs- oder Prüfkriterien, mit denen die Einhaltung der Zertifizierungsvoraussetzungen überprüft werden;
b. der Ablauf des Verfahrens, insbesondere das Vorgehen bei festgestellten Unregelmässigkeiten;
c. die Verwendung des vom BAG zur Verfügung gestellten Zertifizierungssystems zur Prüfung der Datenübertragung von Gemeinschaften und Stammgemeinschaften.

[4] Das EDI legt die Mindestanforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt, fest.

Secondo *LUKS* i requisiti posti agli organismi di certificazione sono troppo elevati e devono essere ridotti al minimo praticabile. Lo stesso è richiesto da *PKS*, *SSIM* e *FMH*. Questi ultimi scrivono che gli elevati requisiti provocano costi di accreditamento eccessivi, senza migliorare sensibilmente la sicurezza dell'intero sistema. *STSAG* chiede che i requisiti delle comunità siano definiti e controllati attraverso le comunità di riferimento e non tramite un organismo di accreditamento. Per le comunità di riferimento dovrebbe essere previsto l'accreditamento e per le comunità solo una certificazione.

A proposito dell'articolo 27 capoverso 1, *BRH*, *CURAVIVA*, *Insos* e il Cantone *TG* ripetono il parere espresso sull'articolo 22 lettera a, mentre *senesuisse* ribadisce il suo parere sull'articolo 22 lettera b. *SQS* sottolinea l'importanza fondamentale della protezione e della sicurezza dei dati per la cartella informatizzata del paziente. Secondo il rapporto esplicativo sulla LCIP il rispetto deve essere assicurato attraverso la procedura di certificazione. In particolare si fa riferimento alla procedura di certificazione secondo l'articolo 11 LPD. In questo settore è particolarmente importante applicare i principi e le procedure riconosciuti a livello internazionale. La certificazione OCPD soddisfa questo criterio perché comprende ampie parti della norma internazionale ISO/IEC 27001 riguardo agli aspetti della sicurezza delle informazioni e dei dati, che sono contemplati nel numero 3 delle direttive per la certificazione dell'organizzazione e della procedura, e perché i requisiti del sistema di gestione della protezione e della sicurezza dei dati fanno parte di questa certificazione specifica. L'accreditamento degli organismi di certificazione e i requisiti posti al personale sono disciplinati nell'OCPD. Inoltre negli ultimi anni la certificazione OCPD ha dato buoni risultati nell'ambito delle certificazioni prescritte dalla legge per i servizi di ricezione dei dati degli assicuratori malattia. *SQS* chiede la seguente modifica dell'articolo 27 capoverso 1: «[…] sowie nach der Verordnung für Datenschutzzertifizierungen (VDSZ) vom 28. September 2007, soweit […]».

SQS auspica che il capoverso 3, oltre all'applicazione dell'ordinanza sull'accreditamento e sulla designazione (OAccD), preveda anche l'applicazione della norma ISO/IEC 27006:2015. Nella versione attuale i requisiti sono ridondanti e l'articolo dovrebbe essere liberato di prescrizioni inutili. ISO/IEC 27006 è rilevante solo se la certificazione avviene secondo ISO/IEC 27001. Le lettere a e b dell'articolo 27 capoverso 3 dovrebbero essere stralciate. Riguardo al capoverso 4, *SQS* segnala che anche i requisiti relativi alla qualifica sono impliciti nell'accreditamento. Le condizioni tecniche e organizzative disciplinate nell'allegato 7 nonché i requisiti per le comunità di riferimento e le comunità non includono dei contenuti che divergano dai requisiti secondo ISO/IEC 27001:2013 o dai requisiti della certificazione secondo l'articolo 11 LPD o che richiedano conoscenze specifiche nel campo dell'informatica medica per garantire una verifica regolare nell'ambito della certificazione. Il capoverso 4 deve essere quindi stralciato.

Art. 28	Akkreditierungsverfahren
Die Schweizerische Akkreditierungsstelle zieht für das Akkreditierungsverfahren und die Nachkontrolle sowie für die Sistierung oder den Entzug einer Akkreditierung das BAG bei.	

FMH ritiene che, se si vuole che le società di medici indipendenti costituiscano delle comunità, bisogna evitare che le procedure di accreditamento richiedano troppe risorse in termini di tempo e denaro.

3.1.6 Capitolo 6: Zertifizierung

Sezione 1: Zertifizierungsvoraussetzungen

Art. 29	Gemeinschaften und Stammgemeinschaften
[1] Mit dem Zertifizierungsverfahren wird geprüft, ob eine Gemeinschaft die Zertifizierungsvoraussetzungen nach den Artikeln 8–12 oder eine Stammgemeinschaft die Zertifizierungsvoraussetzungen nach den Artikeln 8–20 erfüllt.	
[2] Das EDI regelt die Einzelheiten der Zertifizierungsvoraussetzungen.	
[3] Das BAG passt die Zertifizierungsvoraussetzungen dem Stand der Technik an.	
[4] Für den Erlass der Einzelheiten nach Absatz 2 und für die Anpassungen nach Absatz 3 werden die interessierten Kreise angehört.	

VAKA ripete il suo commento sull'articolo 18. *IG eHealth*, *PH CH* e *Posta* evidenziano che la LCIP descrive un sistema rigido. Molte prescrizioni tecniche sono stabilite dal DFI. Il presente testo normativo non specifica invece come svolgere e garantire i processi di adeguamento. Mentre *IG eHealth* e *PH CH* propongono di completare l'ordinanza con una nuova sezione «Adeguamenti del sistema», *Posta* desidera inserire un nuovo articolo «Clausole di adeguamento». *Posta* sottolinea la necessità di nominare un organo incaricato di effettuare gli adeguamenti. Chiede inoltre di descrivere un processo che indichi come e quando approvare e attuare i cambiamenti. Le comunità e il settore devono partecipare a questo processo. Per *FMH* le condizioni di certificazione sono troppo elevate.

Capoverso 3: *CURAVIVA* e *Insos* criticano la delega delle competenze, che definiscono inaccettabile nell'ottica del principio di legalità. Analogamente il Cantone *TG* ritiene troppo vaga e ampia la delega accordata all'UFSP per gli adeguamenti delle condizioni di certificazione. Secondo il Cantone *ZH* e *ZAD* è problematico che il DFI stabilisca le prescrizioni secondo il capoverso 3, ma l'UFSP possa adeguarli allo stato della tecnica. Sarebbe più opportuno che anche l'adeguamento delle disposizioni fosse affidato al DFI. L'articolo 12 capoverso 2 LCIP prevede un'autorizzazione dell'UFSP. Secondo il principio «a maiori ad minus» dovrebbe essere possibile anche un'autorizzazione del DFI. Mentre il Cantone *AG* approva la delega delle competenze all'UFSP per gli adeguamenti delle condizioni di certificazione allo stato della tecnica, *FMH* chiede che tale delega sia sostituita da una descrizione generale e funzionale dei requisiti a livello di ordinanza del Consiglio federale. Le esigenze devono essere inoltre limitate al minimo indispensabile per la costituzione di uno spazio di fiducia.

Art. 30	Herausgeber von Identifikationsmitteln
[1] Die Herausgeber von Identifikationsmitteln müssen:	
a.	in der Lage sein, Identifikationsmittel gemäss den Anforderungen nach den Artikeln 22–26 herauszugeben und zu verwalten;

b. sicherstellen, dass das Personal über die erforderlichen Fachkenntnisse, Erfahrungen und Qualifikationen verfügt;
c. Informatiksysteme und -produkte verwenden, die vertrauenswürdig sind und zuverlässig betrieben werden;
d. Datenschutz und Datensicherheit mit geeigneten organisatorischen und technischen Massnahmen gewährleisten und die entsprechenden Kontrollen sicherstellen.

[2] Das EDI erlässt Vorgaben für den Schutz der Identifikationsmittel und für das Verfahren zu deren Authentifizierung. Sie richten sich nach ISO/IEC 15408:200911 und entsprechen der Evaluierungsstufe 2.

[3] Das EDI regelt die Einzelheiten der Zertifizierungsvoraussetzungen. Das BAG kann dazu Empfehlungen erlassen.

[4] Das BAG passt die Zertifizierungsvoraussetzungen dem Stand der Technik an.

[5] Für den Erlass der Einzelheiten nach Absatz 3 und für die Anpassungen nach Absatz 4 werden die interessierten Kreise angehört.

BRH ripete a questo proposito il suo commento sull'articolo 22 lettera a e sull'articolo 27 capoverso 1, mentre *Posta* reitera il parere espresso sull'articolo 22 lettera c. *HIN* obietta che il ruolo dell'emittente dello strumento d'identificazione è troppo vago. In ambito IHE, nel contesto dell'autenticazione e della regolamentazione degli accessi si parla di IDP, ATP e STS. Nella versione attuale non è invece chiaro se questi tre ruoli siano tutti integrati nella figura dell'emittente. Il XUA-token necessario per ogni transazione contiene dei dati che sono forniti da tutti e tre i ruoli: informazioni sull'autenticazione (IDP), attributo del professionista della salute (ATP) e le altre indicazioni necessarie per il token come ID, ruolo, ecc. (STS). Se questi tre ruoli venissero separati e l'emittente del SID fosse solo l'IDP, ne risulterebbe una lacuna di sicurezza, perché STS e ATP non sarebbero certificati e controllati sebbene forniscano dei dati rilevanti per la sicurezza. *HIN* propone di completare il ruolo dell'emittente di SID nell'articolo 30: «Ein Herausgeber des IDM muss alle notwendigen Aktoren (IDP, ATP und STS) zur Verfügung stellen, die nötig sind, eine gültige Authentisierung zu ermöglichen».

Capoverso 1: *Posta* approva espressamente il capoverso 1. Il Cantone *NW* scrive che l'organismo di certificazione verifica ogni anno per tutte le comunità se sono soddisfatte le condizioni di certificazione. Questo processo è troppo oneroso, tanto più che secondo l'articolo 34 i certificati rimangono validi per 3 anni. In questo periodo di validità triennale, si dovrebbe rinunciare a verifiche regolari una volta all'anno e sostituirle con dei controlli a campione. *ISSS* propone la seguente precisazione per la lettera b: «[…] Qualifikationen und anerkannte Zertifizierungen verfügt». La lettera c dovrebbe essere inoltre adeguata a complemento dell'articolo 11 come segue: «[…] zuverlässig in der Schweiz betrieben werden».

Capoverso 2: *Senesuisse* ripete il suo commento sull'articolo 22 lettera b e l'articolo 27 capoverso 1. *Posta* e *CURAVIVA* reiterano le loro posizioni sull'articolo 22 lettera a e l'articolo 27 capoverso 1. *Posta* aggiunge che l'interpretazione di questo capoverso non è chiara, perché fa riferimento all'autenticazione dei SID. Per migliorare la leggibilità dell'ordinanza, sarebbe preferibile raccogliere tutti i requisiti posti al SID in un unico articolo. Ammesso che abbia senso disciplinarlo a livello di ordinanza, *Posta* raccomanda di spostare il capoverso dopo l'articolo 22. *FMH* fa notare che le prescrizioni sulla protezione del SID sono già definite nell'articolo 22 lettera a con la norma ISO/IEC 29115:2013(E). Il capoverso 2 deve essere stralciato perché non è necessaria un'ulteriore tutela.

Capoversi 3 - 5: Secondo *Posta* non è chiaro se nel capoverso 3 i requisiti di certificazione si riferiscono all'emittente o all'organismo di certificazione. I requisiti menzionati nell'allegato 7 (art. 7) OCIP-DFI, nel capitolo 2, potrebbero essere citati direttamente qui, il che permetterebbe di stralciare i capoversi da 3 a 5. *FMH* è del parere che il DFI potrebbe disciplinare i dettagli della certificazione, ma solo in base alla norma ISO di cui all'articolo 22 lettera a e senza oltrepassare i requisiti di tale norma. Il capoverso 3 dovrebbe essere modificato come segue: «[…] Zertifizierungsvoraussetzungen gemäss Artikel 22 Buchstabe a». *CURAVIVA* e il Cantone *TG* ripetono a proposito del capoverso 4 la posizione già espressa sull'articolo 29 capoverso 3.

Sezione 2: Zertifizierungsverfahren

Art. 31 Ablauf

[1] In einem Voraudit prüft die Zertifizierungsstelle, ob der Gesuchsteller oder die Gesuchstellerin auf das Kontrollverfahren vorbereitet ist, und beurteilt und dokumentiert dessen oder deren Unterlagen.

[2] Im anschliessenden Zertifizierungsaudit überprüft sie anhand ihrer Begutachtungs- oder Prüfkriterien die Wirksamkeit der durch die Gesuchstellerin oder den Gesuchsteller getroffenen Massnahmen.

[3] Sie erteilt das Zertifikat, wenn Voraudit und Zertifizierungsaudit zum Ergebnis führen, dass die Gemeinschaft, die Stammgemeinschaft oder der Herausgeber von Identifikationsmitteln die jeweiligen Anforderungen nach den Artikeln 8–12, 8–20 oder 22–26 erfüllen.

Posta è del parere che la OAccD citata nell'articolo 27 capoverso 1 sia sufficiente per la certificazione e che l'articolo 31 debba essere pertanto stralciato. Mentre il Cantone *AG* approva le tappe di certificazione descritte*, FMH* critica i requisiti troppo elevati e ammonisce da un'eccessiva regolamentazione della procedura di certificazione. Concretamente chiede lo stralcio dell'articolo 31. *SQS* segnala che nella sezione 2 dell'OCIP, relativa alla procedura di certificazione, manca l'indicazione dei termini per la sospensione o la revoca definitiva. Se le comunità di riferimento e le comunità venissero certificate in base a una norma esistente, i termini sarebbero disciplinati nell'ambito di tale norma. Sono possibili due varianti, che dipendono dalla norma di certificazione scelta o dalla possibilità che l'OCIP stabilisca una propria procedura di certificazione per le certificazioni nell'ambito della cartella informatizzata del paziente. Una sospensione o una revoca della certificazione da parte dell'organismo di certificazione a causa di irregolarità o gravi divergenze constatate avrebbe un impatto diretto sull'autorizzazione degli ospedali o di altri istituti e quindi sulla loro possibilità di operare a carico dell'assicurazione malattie. Per questo motivo, la fissazione dei termini procedurali in caso di revoca o sospensione della certificazione deve rispettare le condizioni del diritto procedurale pubblico. Ciò parla a favore di una fissazione specifica dei termini nell'OCIP. Le due procedure relative alla sospensione e alla revoca delle certificazioni – da un lato secondo il diritto pubblico riguardante le condizioni di autorizzazione secondo la LAMal e dall'altro secondo le disposizioni sulla certificazione stabilite nelle norme ISO – non coincidono affatto nei termini e nelle vie legali. Per questo motivo è importante disciplinare i termini nell'ambito delle condizioni di certificazione nella sezione 2 OCIP e stabilire dei termini adeguati.
La variante a richiede l'aggiunta del seguente capoverso all'articolo 31: «Das Zertifizierungsverfahren von Stammgemeinschaften und Gemeinschaften richtet sich nach der Verordnung über die Datenschutzzertifizierungen (VDSZ) vom 28. September 2007, soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält». Nella variante b si tratta invece di completare la sezione 2 «Procedura di certificazione» del capitolo 6 OCIP aggiungendo delle disposizioni sui termini per l'eliminazione di gravi divergenze nonché la sospensione e la revoca. *OFAC* ricorda la sua esperienza con i processi simultanei di certificazione ISO 27001 e OCPD sin dal 2009. La sovrapposizione delle norme ISO 29115 e dei requisiti specifici per le eID dei fornitori di prestazioni in campo sanitario nonché la conformità al profilo di protezione dell'eID rappresentano un volume normativo e di certificazione (nei giorni di audit), che deve essere ripartito su un arco di tempo da definire. Auspica quindi delle disposizioni transitorie in questo campo.

Art. 32 Meldung an das BAG

[1] Die Zertifizierungsstelle teilt dem BAG jedes erteilte und erneuerte Zertifikat sowie Sistierungen oder Entzüge von Zertifikaten innert angemessener Frist mit und stellt die für den Eintrag in den Abfragedienst für die zertifizierten Gemeinschaften und Stammgemeinschaften nach Artikel 39 notwendigen Daten zur Verfügung.

[2] Das BAG veröffentlicht ein Verzeichnis der erteilten Zertifikate.

CURAVIVA, *Insos* e il Cantone *TG* ripetono i loro pareri sull'articolo 20 capoverso 2 lettera a. *Posta* approva espressamente l'articolo 32.

Art. 33 Überwachung

[1] Die Zertifizierungsstelle hat jährlich zu überprüfen, ob die Zertifizierungsvoraus-setzungen weiterhin erfüllt sind.

[2] Stellt die Zertifizierungsstelle im Rahmen ihrer Überwachungstätigkeit wesentliche Abweichungen von den Zertifizierungsvoraussetzungen fest, beispielsweise betreffend die Erfüllung von Bedingungen oder Auflagen, so informiert sie das BAG.

CDS, *ZAD* e 11 Cantoni[67] segnalano che l'organismo di certificazione verifica ogni anno se sono soddisfatte le condizioni di certificazione di ogni comunità. Questo processo è troppo oneroso, tanto più che secondo l'articolo 34 i certificati rimangono validi per 3 anni. In questo periodo di validità triennale, si dovrebbe rinunciare a verifiche regolari una volta all'anno e sostituirle con dei controlli a campione. La stessa proposta è avanzata da *K3* e *VZK*. Il Cantone *ZG* aggiunge che le verifiche dovrebbero essere svolte anche in caso di sospetto o segnalazione. Analogamente, il Cantone *AI* propone la seguente formulazione per il capoverso 1: «Die Zertifizierungsstelle hat stichprobenweise oder bei Verdacht zu überprüfen, ob die Zertifizierungsvoraussetzungen weiterhin erfüllt sind» e *Insel* raccomanda il seguente testo: «Bei begründetem Verdacht, dass die Zertifizierungsvoraussetzungen nicht mehr eingehalten werden, kann das BAG eine Überprüfung durch die Zertifizierungsstelle anordnen». *FMH* prevede che la verifica annua causi elevati oneri e propone pertanto un termine minimo di tre anni. Secondo *Posta* sarebbe sufficiente una verifica ogni 2 anni. Per la certificazione dei SID è invece opportuna la cadenza annuale. *BFH* chiede perché, al momento della verifica annuale, non si rinnovi il certificato per un ulteriore anno. Inoltre ritiene che non abbia senso svolgere una verifica il terzo anno quando il certificato scade ed è necessaria comunque la ricertificazione. Il Cantone *AG* auspica una distinzione più precisa, nel rapporto esplicativo, fra il controllo annuo e la ricertificazione triennale. Chiede anche una precisazione e migliore distinzione dei termini «Überwachung», «Zertifizierung» e «Rezertifizierung». *LUKS* e *SSIM* considerano eccessiva la verifica annua di un certificato che ha una validità di soli 3 anni e chiedono pertanto lo stralcio del capoverso 1. *DSBAG* e *privatim* si dicono invece favorevoli alla verifica annua per motivi di protezione dei dati.

HIN fa notare che la grande quantità di requisiti per la certificazione (punti di misurazione) può essere verificata solo con un onere molto elevato. Di conseguenza propone di distinguere fra criteri obbligatori e facoltativi. Il capoverso 2 dovrebbe essere modificato come segue: «Das BAG erstellt eine Liste aller Anforderungen und klassifiziert diese nach MUSS und SOLL-Kriterien. Wesentliche Abweichungen betreffen MUSS-Kriterien […]». *SQS* scrive che il registro delle comunità di riferimento e delle comunità certificate è tenuto dall'UFSP. Secondo l'articolo 36, l'UFSP può adottare delle misure se sussiste un rischio per la protezione o la sicurezza dei dati della cartella informatizzata del paziente. Chiede di aggiungere il seguente capoverso all'articolo 33: «Das BAG kann von der Zertifizierungsstelle oder von der Gemeinschaft sowie der Stammgemeinschaft jederzeit die für die Zertifizierung oder Rezertifizierung relevanten Dokumente einfordern».

Art. 34 Geltungsdauer

Das Zertifikat wird für jeweils drei Jahre ausgestellt.

BFH e il Cantone *AG* ripetono il loro parere sull'articolo 33 capoverso 1 e *FMH* il suo commento sull'articolo 28. *VAKA* è sorpresa della diffidenza dimostrata nei confronti delle future comunità e comunità di riferimento. Evidenzia che l'onere di dover sostenere una certificazione ogni 3 anni è intollerabile. Anche *K3* e *VZK* considerano troppo onerosa la ricertificazione ogni 3 anni. Secondo *Posta*, sarebbe adeguata una durata di 5 anni per le comunità e di 3 anni per i SID. Sulla stessa falsariga, 6 Cantoni[68] propongono la seguente formulazione per l'articolo 34: «[…] une durée de cinq ans». Complessivamente 10 partecipanti[69] chiedono il rilascio di un certificato valido 5 anni.

Art. 35 Meldung wesentlicher technischer oder organisatorischer Anpassungen

[1] Gemeinschaften, Stammgemeinschaften und Herausgeber von Identifikationsmitteln müssen der Zertifizierungsstelle wesentliche technische oder organisatorische Anpassungen melden.

[2] Die Zertifizierungsstelle entscheidet, ob diese Anpassung durch eine Überwachung, eine Rezertifizierung oder eine ausserordentliche Rezertifizierung geprüft wird.

67 BL, GL, LU, OW, UR, SH, SZ, ZG, TG, ZH, FR

68 GE, FR, VS, VD, JU, NE

69 VAKA, K3, VZK, Posta, GE, FR, VS, VD, JU, NE

VAKA e *Posta* chiedono una precisazione sulla parola «wesentlich». *VAKA* desidera anche degli esempi. *HIN* e *BINT* segnalano che il limite di ciò che è «wesentlich» deve essere molto elevato altrimenti gli organismi di certificazione vengono sommersi di notifiche. A questo proposito rimandano all'osservazione di *HIN* sull'articolo 33. Il Cantone *AG* avverte che gli adeguamenti delle infrastrutture IT possono causare facilmente verifiche e ricertificazioni onerose. Bisogna tenere conto del principio di proporzionalità.

Art. 36	Schutzklausel
Liegt eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vor, so kann das BAG:	
a.	Gemeinschaften und Stammgemeinschaften vorübergehend den Zugang zum elektronischen Patientendossier verweigern;
b.	den Gebrauch bestimmter elektronischer Identifikationsmittel verbieten;
c.	eine ausserordentliche Rezertifizierung anordnen.

K3 e *VZK* segnalano che l'ipotesi di un'esclusione di una comunità di riferimento o di una comunità non deve essere neppure contemplata, perché avrebbe conseguenze imprevedibili. Con la possibilità di negare anche solo provvisoriamente a una comunità l'accesso alla cartella informatizzata del paziente si disconosce l'importanza di quest'ultima. Occorre trovare altri modi e mezzi per assicurare il rispetto dei requisiti sulla gestione di una cartella informatizzata del paziente. È inammissibile chiudere un intero sistema. Sarebbe ipotizzabile per esempio una sorta di «istituto collettore», incaricato di rilevare le funzioni e i dati. *FMH* scrive che la disponibilità dei dati dei pazienti è un fattore centrale per la diffusione della cartella informatizzata del paziente. Anche *FMH* propone una sorta di «istituto collettore» in caso di cessazione dell'esercizio di una comunità. Il Cantone *NW* considera problematica la clausola di salvaguardia. Un'esclusione potrebbe avere come conseguenza che, p. es. in un caso di emergenza, gli ospedali non abbiano più accesso ai dati necessari. Ciò pregiudicherebbe la sicurezza dei pazienti. Per questo motivo l'articolo va riveduto. Il Cantone *SG* chiede un chiarimento su quali diritti i pazienti possono far valere e nei confronti di chi, nel caso in cui l'UFSP neghi provvisoriamente l'accesso a una comunità e i dati dei pazienti non siano più disponibili. 6 Cantoni[70] segnalano che l'UFSP non può negare a una comunità l'accesso alla cartella informatizzata del paziente, perché è la comunità a gestirla. L'UFSP può invece bloccare l'accesso di una comunità ai servizi centrali e ad altre comunità. Questi partecipanti propongono la seguente formulazione per la lettera a: «[…] l'accès aux services centraux et aux autres communautés». *Tessaris* osserva che in singoli casi, oltre a negare l'accesso, bisognerebbe prevedere anche la possibilità di un accesso condizionato a determinate misure di protezione, affinché il professionista della salute possa accedere alla cartella informatizzata del paziente per motivi terapeutici. Propone quindi la seguente aggiunta alla lettera a: «[…] verweigern, wobei einer Gesundheitsfachperson zum Zweck einer medizinischen Behandlung im Einzelfall der Zugang zum elektronischen Patientendossier einer bestimmten Patientin oder eines Patienten unter Auferlegung besonderer Sicherheitsvorkehrungen gewährt werden kann». 6 partecipanti[71] chiedono di verificare se una tale disposizione facoltativa permetta di raggiungere lo scopo prefissato. In presenza di una grave minaccia per la protezione o la sicurezza dei dati della cartella informatizzata del paziente, l'UFSP deve poter agire. *DSBAG*, *KDSBSON*, *privatim* e i Cantoni *BE* e *ZG* propongono la seguente formulazione dell'articolo 36: «[…] des elektronischen Patientendossiers vor, nimmt das BAG insbesondere eine oder mehrere der folgenden Handlungen vor: a. verweigert den Gemeinschaften und Stammgemeinschaften vorübergehend den Zugang zum elektronischen Patientendossier; b. verbietet den Gebrauch bestimmter elektronischer IDM; c. ordnet eine ausserordentliche Rezertifizierung an».

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

[71] DSBAG, KDSBSON, privatim, AG, BE, ZG

Sezione 3: Sanktionen

Art. 37

[1] Die Zertifizierungsstelle kann die Gültigkeit eines Zertifikats aussetzen oder ein Zertifikat entziehen, namentlich wenn sie im Rahmen der Überwachung (Art. 33) schwere Mängel feststellt. Ein schwerer Mangel liegt insbesondere vor, wenn:

a. wesentliche Voraussetzungen der Zertifizierung nicht mehr erfüllt sind; oder
b. ein Zertifikat in irreführender oder missbräuchlicher Art und Weise verwendet wird.

[2] Bei Streitigkeiten über die Sistierung oder den Entzug richten sich die Beurteilung und das Verfahren nach den zivilrechtlichen Bestimmungen, die anwendbar sind auf das Vertragsverhältnis zwischen Zertifizierungsstelle und zertifizierter Gemeinschaft oder Stammgemeinschaft oder zertifiziertem Herausgeber von Identifikationsmitteln.

[3] Besteht der begründete Verdacht, dass eine zertifizierte Gemeinschaft oder Stammgemeinschaft oder ein zertifizierter Herausgeber von Identifikationsmitteln die Zertifizierungsvoraussetzungen nicht einhält, so kann das BAG:

a. eine Überprüfung durch die Zertifizierungsstelle anordnen;
b. die Gültigkeit des Zertifikats aussetzen;
c. das Zertifikat entziehen.

Il Cantone *SG* reitera il suo parere sull'articolo 36. *VAKA* critica il fatto che in caso di revoca del certificato di una comunità o anche di deconnessione temporanea di una comunità dalla rete non esiste oggi una disposizione su «comunità collettrici» o loro società. La procedura, l'organizzazione e la gestione di un «istituto collettore» devono essere completamente rivedute e ridefinite. *RPB* aggiunge che sarebbe ipotizzabile uno scenario simile all'articolo 8, ma in forma «morbida». *SQS* auspica l'aggiunta di un capoverso all'articolo 37 per disciplinare le conseguenze di una sospensione o una revoca della certificazione, per tutelare l'interesse dei fornitori di prestazioni e dei pazienti all'accesso alla cartella informatizzata del paziente.

Riguardo al primo capoverso, 7 partecipanti[72] sono contrari a una disposizione «facoltativa» in caso di gravi irregolarità. In questo caso l'organismo di certificazione dovrebbe essere obbligato a sospendere la validità del certificato o a revocarlo. Questo capoverso deve essere modificato in tal senso. Sul secondo capoverso, *CDS* e 11 Cantoni[73] fanno notare l'incertezza del rapporto giuridico fra l'organismo accreditato e le imprese interessate. Il primo svolge compiti amministrativi che pongono interrogativi sul controllo statale, la protezione giuridica e il rispetto dei diritti fondamentali. Sostenere che la procedura segue le disposizioni del diritto civile che si applicano al rapporto contrattuale non è esatto in termini assoluti. Il capoverso 2 deve essere pertanto modificato. Riguardo al terzo capoverso, *DSBAG*, *privatim* e Cantoni *AG*, *BE* e *FR* scrivono che qui si applica la procedura amministrativa visto che l'UFSP è l'autorità decisionale (art. 1 PA, RS 172.021). In questo contesto bisognerebbe verificare se la procedura amministrativa è in grado di garantire i necessari margini di manovra in termini di tempestività, efficacia, ecc. *SQS* fa notare che la LCIP non autorizza l'UFSP a intervenire attivamente nel processo concreto di autorizzazione e ad assumere il ruolo di organismo di certificazione. L'autorizzazione concessa all'UFSP dall'articolo 37 capoverso 3 viola il principio di legalità ed è incompatibile con un'ordinanza d'esecuzione. Inoltre, nei casi che richiedono un'azione tempestiva, l'UFSP può intervenire in virtù dell'articolo 36. L'articolo 37 capoverso 3 lettere b e c deve essere quindi stralciato.

3.1.7 Capitolo 7: Abfragedienste

Sezione 1: Allgemeines

Art. 38

[1] Die Abfragedienste enthalten:

a. die Referenzdaten über:
   1. die Gemeinschaften und Stammgemeinschaften,
   2. die Gesundheitseinrichtungen und deren Gesundheitsfachpersonen, die Daten des elektronischen Patientendossiers bearbeiten dürfen;
b. die Metadaten (Art. 9 Abs. 3 Bst. b);

[72] DSBAG, KDSBSON, privatim, AG, BE, FR, ZG
[73] BL, GL, LU, OW, UR, NW, FR, SZ, TG, ZG, ZH

c. die Austauschformate (Art. 9 Abs. 3 Bst. c);

d. die für das elektronische Patientendossier registrierten Objektidentifikatoren (OID).

[2] Das BAG stellt den Aufbau, den Betrieb und die Weiterentwicklung der Abfragedienste sicher.

K3 e *VZK* scrivono che i servizi di ricerca di dati di cui all'articolo 38 segg. contengono diversi dati utili per la comunicazione fra i professionisti della salute e le strutture sanitarie, e chiedono se questi registri possono essere impiegati anche per la comunicazione orientata. Nel Cantone di Zurigo l'uso dell'infrastruttura è previsto anche per la comunicazione primaria fra due fornitori di prestazioni. Auspicano pertanto che sia consentito l'uso dell'MPI per la comunicazione orientata alla connessione fra fornitori di prestazioni. *OFAC* scrive che, sulla scorta della sua lunga esperienza nell'esercizio informatico di questo tipo di servizio a livello nazionale e tenuto conto della criticità di queste applicazioni dal punto di vista della disponibilità, sicurezza, protezione dei dati, ecc., raccomanda vivamente che le società che proporranno dei servizi centralizzati debbano essere anch'esse certificate (p.es. ISO20000, ISO27001, OCPD). Le organizzazioni che operano e gestiscono i servizi centralizzati devono essere sottoposte quantomeno agli stessi requisiti di certificazione e organizzazione delle comunità. Secondo *OFAC* questo principio dovrebbe essere iscritto nell'OCIP e rientrare nei requisiti delle gare di appalto.

Sezione 2: Inhalt

Art. 39 Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften

[1] Der Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften enthält folgende Daten:

a. ihre Bezeichnung;

b. ihre GLN;

c. ihre OID;

d. ihre Zertifikate zur sicheren Authentifizierung gegenüber anderen Gemeinschaften und Stammgemeinschaften;

e. die Internetadresse ihres Zugangspunktes.

[2] Das BAG prüft diese Daten und trägt sie im Abfragedienst der Gemeinschaften und Stammgemeinschaften ein.

Posta critica il termine «Zertifikat» e vorrebbe sostituirlo con «Authentifizierungszertifikat».

Art. 40 Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen

Gemeinschaften und Stammgemeinschaften tragen im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen folgende Daten ein:

a. zu Gesundheitseinrichtungen und Gruppen von Gesundheitsfachpersonen:

1. die Bezeichnung und die Adresse,
2. die GLN,
3. die OID;

b. zu Gesundheitsfachpersonen:

1. die Personalien,
2. die GLN,
3. die Bezeichnung und die Adresse der Gesundheitseinrichtung oder der Gruppe von Gesundheitsfachpersonen, der sie angehört.

PH CH ripete le sue osservazioni sull'articolo 8. *VAKA* chiede se esistono degli «use case» in cui possa succedere che varie comunità adeguino in modo diverso le stesse registrazioni dell'HPD. I professionisti della salute possono essere attivi in più comunità e appartenere a molte organizzazioni diverse. Questi accavallamenti devono essere possibili. *H+* è favorevole a che l'UFSP stabilisca un servizio nazionale di ricerca di dati. *Posta* osserva che il termine «Gesundheitseinrichtung» è utilizzato per la prima volta in questo articolo. Nei capitoli sull'autorizzazione si parlava invece solo di «Gruppen». Si chiede se una struttura sanitaria può essere anche un gruppo. Bisogna definire chiaramente i termini e specificare se i gruppi sono amministrati o meno nel servizio di ricerca di dati. Inoltre è necessario chiarire cosa succede se due comunità vogliono modificare le stesse registrazioni e chi deve assumere la responsabilità in tali casi. Riguardo alla lettera a numero 3, *Posta* chiede inoltre se l'obiettivo dell'ordinanza è che ogni struttura sanitaria in Svizzera debba procurarsi oltre al GLN anche un OID. In questo caso i gruppi verrebbero descritti in modo tale da poter essere sia globali che individuali. Questa decisione è lasciata

al paziente. Un identificatore univoco non ha senso in questo scenario «use case» perché lo stesso gruppo può avere diversi membri a seconda del contesto. Il GLN è sufficiente come identificatore. Questo punto va chiarito e la formulazione del capoverso 3 deve essere modificata come segue: «OID als eindeutiger Identifier innerhalb der OID der Gemeinschaft».

Lettera b: sui numeri 1 e 3 *HL7* e *IHE* chiedono un elenco esaustivo dei dati personali richiesti. Il numero 3 potrebbe essere formulato come segue: «die GLN und falls vorhanden die OID, sowie die Bezeichnung […]».*Posta* constata che, secondo la lettera a numero 2, i professionisti della salute devono indicare i GLN di un gruppo o di un'organizzazione già registrata. Queste indicazioni devono essere fornite già sotto la lettera a numero 1. *ASPS* e *Spitex* fanno notare che l'assegnazione di numeri GLN al personale infermieristico è iniziata da poco e lungi dall'essere completata. L'assegnazione di un GLN a ogni addetto alle cure deve essere indicata come obbligatoria.

Sezione 3: Übertragung an Dritte

Art. 41 Leistungsvertrag

[1] Das BAG kann den Aufbau und den Betrieb der Abfragedienste mittels Leistungsvertrag an Dritte übertragen.

[2] Der Leistungsvertrag regelt insbesondere:

a. die zu erreichenden Ziele;
b. die Anforderungen an den Datenschutz und die Datensicherheit;
c. den Umfang und die Modalitäten der Entschädigung durch den Bund;
d. die Folgen einer Nichterfüllung;
e. die Modalitäten für eine periodische Berichterstattung.

[3] Der beauftragte Dritte ist verpflichtet, das BAG umgehend über wesentliche Änderungen zu informieren.

CMC, *BüAeV*, *GAeSO* e *KAeG SG* scrivono che il testo non disciplina in base a quali criteri viene determinato l'importo dell'indennità. Dall'articolo 42 si può supporre che i costi di terzi siano accollati alle comunità o alle comunità di riferimento. Per mantenere questi costi a un livello ragionevole, l'indennità a terzi non deve essere stabilita o negoziata in base ai criteri di economia privata, bensì nel rispetto del principio dell'equivalenza. I suddetti partecipanti chiedono di inserire il seguente capoverso: «Die Entschädigung des Dritten, bestehend aus allfälligen Gebühren für die Erbringung von Leistungen gemäss Artikel 19 Absatz 2 EPDG sowie einer zusätzlichen Entschädigung des Bundes, darf den Aufwand, welcher anfiele, wenn das BAG den Aufbau und den Betrieb der Abfragedienste selber vornehmen würde, nicht übersteigen.» *KAeG SG* auspica anche l'aggiunta della seguente frase alla fine del nuovo capoverso: «Eine Beteiligung durch die Ärzteschaft ist ausgeschlossen».

Art. 42 Gebühren

[1] Von den Gemeinschaften und Stammgemeinschaften wird pauschal eine jährliche Gebühr von 13 500 Franken erhoben.

[2] Im Übrigen gelten die Bestimmungen der Allgemeinen Gebührenverordnung vom 8. September 2004.

FMH ripete il suo commento sugli articoli 28 e 34. 20 partecipanti[74] fanno notare che il capoverso 1 prevede un emolumento di CHF 13 500, mentre il rapporto esplicativo parla di CHF 20 000. *KSOW* chiede come è stata calcolata la cifra di CHF 13 500 oppure se si tratti effettivamente di CHF 20 000. Secondo *VGIch* e *Medgate* questa discordanza deve essere eliminata. Il Cantone *BE* chiede di precisare le restrizioni previste nelle CTO per le comunità e comunità di riferimento. 17 partecipanti[75] affermano che è contradditorio da un lato sostenere con aiuti finanziari la costituzione di comunità e dall'altro aumentare i costi di esercizio delle comunità attraverso un emolumento, esigendo praticamente il rimborso di una parte degli aiuti finanziari. Anche altri 9 partecipanti[76] ritengono insensato un emolumento annuo a fronte degli aiuti finanziari della Confederazione. Anche *LUKS* e *STSAG* rimandano agli aiuti finanziari e chiedono la soppressione dell'emolumento. *BRH* mette in questione l'emolumento annuo per la costituzione e l'esercizio dei servizi di ricerca di dati sull'arco di 10 anni, perché equivale alla

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

restituzione di una parte degli aiuti finanziari. Preferisce invece un conguaglio con gli aiuti finanziari versati e una correzione dell'importo dell'emolumento. *LUKS* scrive che la Confederazione dovrebbe finanziare i servizi centrali di ricerca di dati e *STSAG* ricorda che la LCIP prevede già un dovere di partecipazione degli istituti, al quale non si può ora aggiungere anche un obbligo di finanziamento. I Cantoni *NW*, *ZG* e *ZH* nonché *ZAD* considerano questo emolumento del tutto ingiustificato, tanto più che dall'ordinanza non risulta quali prestazioni debba indennizzare. Anche nel rapporto esplicativo non si trovano delle spiegazioni al riguardo. Secondo 6 Cantoni[77] la Confederazione dovrebbe assumere i costi operativi d'interesse generale, soprattutto quelli di funzionamento dei servizi centrali. Anche *OFAC* sostiene che questi costi debbano essere assunti interamente dalla Confederazione e non dalle comunità. Il Cantone *AR* desidera sapere quali costi sono coperti da questo emolumento e a chi vengono versati tali fondi. *VAKA* è del parere che, nel momento in cui nessuna comunità futura ha un modello aziendale per il finanziamento dell'esercizio, non è possibile chiedere degli emolumenti per dei servizi centrali. Secondo *UDC* sarebbe nell'interesse sia delle comunità sia delle autorità che i flussi finanziari venissero semplificati, per esempio fissando gli aiuti finanziari in modo tale da poter rinunciare all'emolumento.

In generale 25 partecipanti[78] chiedono esplicitamente lo stralcio dell'articolo 42. *HIN* parte dal presupposto che si costituiranno comunità molto diverse. Chiede che gli emolumenti vengano riscossi in funzione delle dimensioni e propone la seguente formulazione per l'articolo 42 capoverso 1: «[…] wird pauschal eine grössenabhängige, jährliche Gebühr von maximal CHF 13'500 erhoben». *BFH* scrive che anche qui sarebbe opportuno prevedere una ponderazione più equilibrata con un importo di base e una parte variabile, p. es. in funzione del numero di persone appartenenti a una comunità. Ciò vale soprattutto per le comunità di riferimento. Gli importi fissi non sembrano adeguati.

Art. 43	Aufsicht
[1] Das BAG ist zuständig für die Aufsicht über Dritte, denen der Betrieb eines Abfragedienstes übertragen ist.	
[2] Die Aufsicht umfasst insbesondere:	
a.	die periodische Prüfung, ob die Vorgaben nach Artikel 41 Absatz 2 eingehalten werden;
b.	die periodische Einforderung von Berichten;
c.	die Kontrolle der Einhaltung des Leistungsvertrags vor Ort.

Die *SSIM* fa notare che gli emolumenti sono citati nella sezione 3: «Trasferimento di compiti a terzi», bisognerebbe però precisare che valgono in generale.

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

[78] 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 OCIP-DFI

Nell'OCIP-DFI gli allegati 5b, 5c e 8 sono redatti in inglese. I pareri su questi tre documenti sono stati pertanto presentati essenzialmente in inglese e inseriti senza traduzione nel presente rapporto.

3.2.1 Art. 1 Patientenidentifikationsnummer (allegato 1)

Art. 1	Patientenidentifikationsnummer
Der Aufbau der Patientenidentifikationsnummer und das Vorgehen zur Kontrollzifferprüfung bei der manuellen Erfassung der Patientenidentifikationsnummer nach Artikel 4 Absatz 2 OCIP sind in Anhang 1 festgelegt.	

Articolo 1: Il Cantone *FR* suggerisce che sarebbe utile chiarire cosa si può o non si può fare con il NIP.

Allegato 1

Stiftung refdata, *GS1*, *SSIM* e *ICTS* ribadiscono per l'allegato 1 le posizioni espresse sull'articolo 4 OCIP. *ICTS* chiede inoltre che nell'ambito dell'identificazione del paziente e della chiave d'identificazione impiegata a riguardo, si applichi il principio di preferire gli standard internazionali, evitando nel limite del possibile soluzioni sviluppate appositamente per la Svizzera. *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* considerano positivo che venga creato un NIP specifico per la cartella informatizzata del paziente e che non si utilizzi come numero d'identificazione il NAVS13, come era intenzione inizialmente.

OFAC scrive che non c'è nulla da dire sull'algoritmo di controllo del numero d'identificazione. *BINT*, *HL7* e *IHE* ritengono che si tratti di una procedura usuale che corrisponde a uno standard e che secondo loro soddisfa i requisiti. Anche per *medshare* l'allegato 1 va bene.

3.2.2 Art. 2 Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (allegato 2)

Art. 2	Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften
Die technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ) für Gemeinschaften und Stammgemeinschaften nach Artikel 29 Absatz 2 OCIP sind in Anhang 2 festgelegt.	

Articolo 2: *SQS* ritiene che l'allegato 2 non sia una «condizione di certificazione», ma una «direttiva tecnica e organizzativa per le comunità e comunità di riferimento», le quali sottostanno all'obbligo di certificazione secondo l'articolo 11 capoverso 1 lettera a LCIP e devono quindi essere certificate. Non rientra nelli compiti della certificazione dei sistemi di gestione verificare il rispetto corretto delle direttive tecniche. Nel quadro della certificazione ISO/IEC 27001:2013, il team di verificatori deve controllare l'applicazione nel corso della certificazione del sistema di gestione attraverso Control A.18. per questo motivo, l'articolo 2 dovrebbe leggere: «Die technischen und organisatorischen Voraussetzungen (TOV) für Gemeinschaften und Stammgemeinschaften, die der Zertifizierungspflicht nach Artikel 11 Absatz 1 EPDG unterstehen, sind gemäss Artikel 29 Absatz 2 EPDV in Anhang 2 festgelegt»». *SQS* vuole inoltre aggiungere il seguente capoverso nell'articolo 2: «Die Mindestanforderungen an ein Datenschutzmanagementsystem richten sich nach Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 19. März 2014 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten».

Allegato 2

1. Gestione (art. 8 OCIP)

6 partecipanti[79] considerano le esigenze del numero 1 troppo complesse e chiedono quindi di semplifi-

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

carle. La maggior parte di tali esigenze risultano già dall'articolo 8 OCIP. Quelle che non vi sono contenute dovrebbero piuttosto essere indicate come regole generali astratte (esempio: numero 1.3 sulla gestione del personale ausiliario)

1.1 Gestione delle strutture sanitarie (lett. a e c):

6 Cantoni[80] sottolineano che il termine «gestion» nella traduzione francese è inopportuno e dovrebbe essere sostituito con «administration» (traduzione più vicina al tedesco «Verwaltung»).

1.1.1: IG *eHealth* e *Posta* desiderano una definizione del termine «Gesundheitseinrichtung» (struttura sanitaria), chiarendo in particolare se un medico indipendente, un terapeuta o una levatrice possano entrare in una comunità solo come «collaboratori» di una struttura sanitaria. Alla stessa stregua anche *Tessaris* critica che il termine «Gesundheitseinrichtung», introdotto all'articolo 8 capoverso 1 OCIP, non sia stato definito chiaramente in nessun punto.

1.1.2: Riguardo al numero 1.1.2.1, *FMH* scrive che la LCIP non disciplina i processi nell'ambulatorio medico, in ospedale, ecc. In questa disposizione si può disciplinare solo qualcosa sull'impiego della cartella informatizzata del paziente. IG *eHealth* e *Posta* evidenziano che i requisiti al numero 1.1.2.2 possono essere soddisfatti solo se i servizi forniscono i processi e i mezzi tecnici necessari. Tali requisiti non sono descritti in nessun punto. Propongono pertanto che i requisiti vincolanti per i servizi debbano essere formulati secondo l'articolo 40 nell'ordinanza (o allegati).

Sul numero 1.1.2.3 *CDS* e 10 Cantoni[81] scrivono che la formulazione «für alle mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachperson» potrebbe suggerire che ogni professionista della salute di una struttura sanitaria, senza alcuna eccezione, debba poter entrare nella HPD. Le strutture sanitarie devono poter essere libere di limitare la selezione dei professionisti della salute a quelli che si avvarranno della cartella informatizzata del paziente. Il numero 1.1.2.3 dovrebbe pertanto leggere come segue: «der Prozess «Eintritt von Gesundheitsfachpersonen» für jene mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen ausgelöst wird, welche die Gesundheitseinrichtung für den Zugriff aufs elektronische Patientendossier vorsieht». Su questo numero, *VGIch* scrive che in base al rapporto esplicativo dovrebbe essere possibile delegare il processo d'ingresso alle strutture sanitarie. Ai fini pratici, la disposizione dovrebbe essere interpretata nel senso che la struttura sanitaria può determinare chi entra attivamente. L'elevata fluttuazione registrata negli ospedali richiede un certo buon senso nell'interpretazione di questo requisito. Le CTO devono essere adeguate in tale direzione. Il Cantone *AR* vorrebbe che le indicazioni al numero 1.1.2.3 vengano integrate nelle ordinanze. *Posta* chiede come un professionista della salute possa entrare se la struttura sanitaria non è membro della comunità. Sarebbe opportuna una formulazione più chiara. Secondo *KSSG*, il numero 1.1.2.3 prevede che tutti i professionisti della salute entranti debbano essere comunicati. Ciò contraddice le dichiarazioni fatte nelle sedute informative, nelle quali è stato più volte dichiarato che solo alcuni professionisti della salute per settore specifico/clinica godono di tale diritto e devono essere repertoriati. L'articolo deve essere concretizzato in tale senso.

1.1.3: *SUVA* sostiene che l'archiviazione dei documenti in una struttura sanitaria corrisponde all'archiviazione nel sistema primario. Con l'obbligo di eliminare i documenti nell'archivio documenti della struttura sanitaria, i documenti vengono distrutti per sempre. Ciò non può essere l'obiettivo della cartella informatizzata del paziente. Indipendentemente dalla cancellazione della cartella informatizzata del paziente o dall'uscita di un istituto da una comunità, i documenti dovrebbero rimanere nei sistemi primari. L'obbligo di cancellazione deve essere eliminato. *SUVA* chiede lo stralcio completo del numero 1.1.3 incl. 1.1.3.1 fino a 1.1.3.2.3 o quantomeno una precisazione. *Posta* scrive riguardo al numero 1.1.3.1 che tali requisiti non possono essere soddisfatti se un fornitore di prestazioni lavora in più istituti o aderisce a più comunità. Se p. es. un medico ha uno studio a Nyon ed è al contempo un medico indipendente che lavora in una clinica a Ginevra, verrebbe registrato in due HPD. Alla SUVA ci sono dei medici

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

che lavorano per 7 istituti. La formulazione dovrebbe quindi essere modificata. Rispetto alle disposizioni dell'1.1.3.2, il Cantone *TI* ricorda che i dati sono inseriti da un professionista della salute per garantire al paziente una continuazione delle cure ottimale. I dati non appartengono dunque all'istituto che lascia la comunità, ma sono di proprietà del paziente. I dati non andrebbero quindi mai cancellati, ma eventualmente migrati per garantire al paziente una cartella più completa possibile. In ogni caso, la cancellazione non può avvenire senza avere informato il paziente in anticipo. *SSIM* sostiene che, in caso di uscita di una comunità, il paziente interessato deve avere la possibilità di aderire a un'altra comunità, e che questo principio deve essere precisato. Secondo *FMH* la maggior parte delle legislazioni cantonali prevedono che i dati del paziente debbano essere messi a disposizione del paziente in caso per esempio di decesso del titolare di un ambulatorio, mentre per la cartella informatizzata del paziente i dati vengono cancellati o la loro archiviazione viene demandata al paziente (vedi 1.1.3.2.3) e la procedura è stabilita dalla relativa comunità. Ciò è contrario agli interessi del paziente e alle regole fondamentali della documentazione medica. È inoltre inammissibile che un requisito di tale portata costituisca solo un criterio di certificazione nelle CTO e non venga definito come requisito funzionale a livello di ordinanza. È pertanto opportuno prendere le misure del caso.

6 Cantoni[82] sono del parere che in caso di cessazione dell'attività di una struttura sanitaria le cartelle informatizzate non debbano essere cancellate come previsto nei numeri 1.1.3.2.1 e 1.1.3.2.2, ma restare a disposizione dei pazienti e dei professionisti della salute. Inoltre, non sono gli istituti a essere gli autori dei documenti, ma i professionisti della salute. Entrambi i numeri devono quindi essere stralciati. *BFH* non capisce perché i documenti di una struttura sanitaria uscente debbano essere semplicemente cancellati. Anche se, secondo il numero 1.1.3.2.3, i pazienti devono essere informati per tempo, ci dovrebbe essere un processo chiaro che eviti la perdita dei documenti. Nel numero 1.1.3.2.3 si dovrebbe pertanto aggiungere che i documenti «da eliminare» vengano almeno trasferiti automaticamente negli «archivi dedicati interni alla comunità» per i documenti registrati dai relativi pazienti, come previsto dall'articolo 18 OCIP. *Economiesuisse* e *SBC* evidenziano che il paziente non deve in alcun caso perdere i dati se una struttura sanitaria abbandona lo spazio di fiducia LCIP. Ciò lederebbe la sovranità del paziente. I suddetti partecipanti propongono di inserire il testo seguente: «Die Gemeinschaften müssen sich organisieren für die weitere Speicherung von Dokumenten von Leistungserbringern, die die Gemeinschaft verlassen und die zu keiner anderen Gemeinschaft gehen». *Bleuer* sottolinea che i documenti appartengono al paziente e non possono quindi essere cancellati senza il suo esplicito consenso. È opportuno prendere le misure adeguate perché tutti i documenti della struttura sanitaria uscente rimangano archiviati nella cartella informatizzata del paziente (per l'utente non deve cambiare nulla in termini di accesso). Anche *medshare* considera che una cartella informatizzata del paziente appartiene al paziente dalla sua creazione fino al decesso del paziente e quindi nessun'altra persona ha il diritto di cancellarvi dei dati. Anche in caso di soppressione, il paziente deve avere il diritto di decidere se eliminare i dati o meno. La questione è fondamentale soprattutto in caso di una futura riapertura della cartella. Secondo *IG eHealth* e *Posta* il numero 1.1.3.2.1 non è logico. Se una struttura sanitaria esce da una comunità, è compito della nuova comunità registrare correttamente la struttura sanitaria. Gli identificatori della struttura sanitaria e dei professionisti della salute (GLN) rimangono validi, così come il collegamento con i documenti. È importante che una struttura sanitaria non possa trasferire i propri documenti in una nuova comunità, perché quando cambia l'ID dell'affinity domain cambia anche il collegamento dei documenti. Tutti i riferimenti negli audit logs sparirebbero e si perderebbe così la tracciabilità. Anche gli aggiornamenti dei metadati (vedi XDS.b) andrebbero persi, perché si dovrebbe eliminare anche il registry. Le iscrizioni nel registry indicherebbero infatti dei documenti non disponibili. Tale requisito deve pertanto essere stralciato. IG *eHealth* e *Posta* sono inoltre del parere che in caso di uscita di una struttura sanitaria, la cartella informatizzata del paziente non debba essere cancellata. *IG eHealth* propone che la struttura sanitaria uscente debba lasciare i dati nel repository, che passerebbe poi in mano alla comunità. *Posta* aggiunge che la richiesta di cancellazione prevista al numero 1.1.3.2.1 non è compatibile con lo scopo della legge. È contraria al principio della conservazione secondaria di dati e all'idea di fondo che la sovranità dei dati spetta al paziente. La comunità dovrebbe assicurare che anche dopo l'uscita di un professionista della salute o di una struttura sanitaria tutti i documenti continuino a essere disponibili. *Integic* è dell'avviso che la formulazione del numero 1.1.3.2.1 è incomprensibile; secondo il

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

paziente i documenti che lo riguardano si trovano nel suo (in un) archivio. Indipendentemente dalla struttura, nei casi previsti all'1.1.3 e 1.1.3.2 il paziente perde apparentemente dei dati, altrimenti non dovrebbe essere informato secondo il numero 1.1.3.2.3. I documenti medici appartengono al paziente. La cancellazione da parte di terzi – per un qualsivoglia motivo – è contrario alla legge. Manca la formulazione esplicita di un modello inteso a garantire la sovranità dei dati; le formulazioni proposte all'1.1.3.2.1 e 1.1.3.2.2 lasciano intendere che – almeno implicitamente – terzi possano decidere della conservazione dei documenti. Il numero 1.1.3.2.1 è pertinente solo se l'archivio è riservato alla cartella informatizzata del paziente. Nel rapporto esplicativo dell'OCIP sono menzionate delle eccezioni, ma non qui. *Pivatim* obietta che la mera cancellazione dei documenti non basta a distruggerli. I dati dovrebbero invece essere eliminati irrevocabilmente mediante procedure tecniche adeguate. Per il numero 1.1.3.2.1 propongono la seguente redazione: «[…] austretenden Gesundheitseinrichtung durch geeignete technische Massnahmen unwiderruflich vernichtet werden» (). Alla stessa stregua per il numero 1.1.3.2.2 propongono: «[…] austretenden Einrichtung verweisen durch geeignete technische Massnahmen unwiderruflich vernichtet werden». I Cantoni *LU*, *NW*, *SZ* e *ZH* ritengono problematico che i documenti registrati nella cartella informatizzata del paziente da una struttura sanitaria uscente debbano essere cancellati se l'istituto esce dalla comunità. Sarebbe opportuno chiarire se è il paziente o la struttura sanitaria ad avere la sovranità dei documenti. Non è lecito cancellare dati dalla cartella informatizzata del paziente contro la volontà del paziente. Il Cantone *ZG* scrive che l'uscita di una struttura sanitaria non deve comportare la cancellazione dei dati nella cartella informatizzata del paziente e ciò indipendentemente dal fatto che l'istituto aderisca a un'altra comunità o meno. È necessario inserire una disposizione che garantisca la permanenza dei dati del paziente nella sua cartella informatizzata anche quando l'istituto che ha inserito i dati esce dalla comunità o comunità di riferimento. *Tessaris* segnala che la cancellazione sicura di un documento nella cartella informatizzata del paziente, incluse tutte le copie di backup, è un processo oneroso. Bisogna chiedersi se è la comunità o la struttura sanitaria a esserne responsabile e ad accollarsi i costi. Il numero 1.1.3.2.1 dovrebbe essere modificato nel modo seguente: «[…] Gesundheitseinrichtung, einschliesslich Sicherungs- und Back-up Kopien, vollständig gelöscht werden und der Vollzug der Löschung überprüft und von der nach Ziff. 1.1.4 verantwortlichen Person unterschriftlich bestätigt wird».

IG eHealth critica nel numero 1.1.3.2.2 che tali registrazioni non dovrebbero nemmeno essere effettuate, stando all'articolo 9 capoverso 1 lettera c OCIP. Il rapporto esplicativo lascia intendere che vi potrebbero essere dei motivi tecnici, senza però precisare quali. *IG eHealth* raccomanda pertanto lo stralcio di tale eccezione. *HIN* obietta che il termine «rechtzeitig» (in tempo utile) al numero 1.1.3.2.3 lascia spazio a interpretazioni e propone, così come *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* la seguente redazione: «[…] rechtzeitig, d.h. mindestens einen Monat vor dem Austritt, informiert werden und ausdrücklich darauf hingewiesen werden, dass die Dokumentenablage der austretenden Gesundheitseinrichtung auf den Austrittszeitpunkt gelöscht werden». Sulla stessa falsariga, il Cantone AR considera che il termine «rechtzeitig» (in tempo utile) debba essere precisato. 6 Cantoni[83] desiderano formulare il numero 1.1.3.2.3 nel modo seguente: «l'information en temps utile des patients par les professionnels de soins concernés». *Tessaris* scrive che non è chiaro quali diritti e pretese spettino al paziente informato dell'uscita della struttura sanitaria. Propone la formulazione seguente: «[…] Patienten in textlich nachweisbarer Form rechtzeitig informiert und über die ihnen nun verfügbaren Optionen aufgeklärt werden».

1.1.4: *FMH* si lamenta che il numero 1.1.4 è troppo vago riguardo a molti processi e chiede pertanto una precisazione. *K3*, *VZK* e *VAKA* propongono lo stralcio del numero 1.1.4.2.2. *BFH* evidenzia che, in base all'articolo 8 lettera e OCIP, la composizione dei gruppi di professionisti della salute deve essere rintracciabile «jederzeit» (in ogni momento). Qui si scrive «vierteljährlich» (trimestralmente). Una gestione «in ogni momento» sarebbe molto difficile, se non addirittura impossibile. La scadenza trimestrale è più realistica, ma è in contrasto con l'ordinanza. *Tessaris* sottolinea che verificare e confermare almeno due volte all'anno l'attualità e la correttezza dei dati registrati nel servizio centrale di ricerca dei dati delle strutture sanitarie e dei professionisti della salute è un processo estremamente oneroso. Rimane inoltre vago chi deve effettuare tale verifica. 6 Cantoni[84] indicano che le comunità non hanno altri

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

mezzi per «verificare e confermare» i dati, se non le dichiarazioni degli istituti e dei gruppi. Propongono la seguente formulazione del numero 1.1.4: «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 Gestione dei professionisti della salute (lett. da a a d)

6 Cantoni[85] ribadiscono il loro parere espresso sul numero 1.1 anche per il numero 1.2.

1.2.2: *FMH* considera il numero 1.2.2.1 inapplicabile e ne chiede lo stralcio. Dal 1.2.2.3 risultano doppioni con l'OCIP. La verifica che si tratta di un professionista della salute deve avvenire da parte di servizi qualificati. È inoltre necessario distinguere i gruppi professionali. *FMH* richiede pertanto una regolamentazione chiara a livello di OCIP. Per il numero 1.2.2.4 *FMH* scrive che il SID deve essere registrato al momento dell'emissione: anche questo aspetto deve essere quindi disciplinato a livello di OCIP. *FMH* pone alcune domande sul numero 1.2.2.5 e richiede una regolamentazione generale dei processi a livello di OCIP. Per 6 Cantoni[86] il numero 1.2.2.4 è poco chiaro. Se uno strumento d'identificazione non è registrato, non può essere utilizzato. Bisogna chiarire la terminologia (identificazione o autenticazione?) e il significato di «garantir» al numero 1.2.2. I Cantoni *FR*, *GE*, *VS*, *VD* e *JU* scrivono inoltre che il MedReg non contiene necessariamente i dati più aggiornati. Di conseguenza tali dati non devono essere ripresi sistematicamente. È opportuno stralciare la relativa frase al numero 1.2.2.5. *IG eHealth* e *Posta* chiedono se i registri MedReg ecc. non facciano parte del servizio di ricerca HPI e se non dovrebbero essere collegati separatamente all'HPD. A ciò si aggiunge che non sono compatibili con la legge. Sono le comunità a essere competenti per i dati. I registri hanno un altro owner. Si pone l'interrogativo chi è competente in caso di dati contradditori e chi decide in caso di divergenze. È una questione da chiarire. Anche il personale ausiliario deve essere inserito nel servizio di ricerca di dati delle strutture sanitarie in modo da essere identificabile e riconoscibile per il paziente a livello intercomunitario. *Posta* scrive inoltre che il rilascio e l'amministrazione degli strumenti di autenticazione per i collaboratori delle strutture sanitarie non sono menzionati in questo punto e chiede se la comunità non li delega. *STSAG* auspica la garanzia che i servizi di ricerca di dati indicati al numero 1.2.2.5 possano avvalersi della massima automatizzazione possibile per il trattamento degli ingressi e delle uscite dei professionisti della salute. *Tessaris* desidera la seguente aggiunta al numero 1.2.2.5: «[…] von dort zu übernehmen und bei Änderung der Eintragungen in den betreffenden Registern nachzuführen». *SCH* critica che si creano delle interfacce con i registri professionali, con un conseguente e inutile incremento dei costi. Chiede pertanto lo stralcio della seconda frase del numero 1.2.2.5.

1.2.3: *6 Cantoni*[87] chiedono come questo accesso possa essere oggetto di controlli e se si tratta di verificare che il professionista della salute, che ha avuto accesso alla cartella informatizzata del paziente, fosse realmente autorizzato a farlo. Questa tappa viene verificata nel quadro dei test di penetrazione, ma non attraverso il «processo di gestione dei professionisti della salute». Il numero 1.2.3.2 deve quindi essere stralciato, mentre il numero 1.2.3.3 deve essere chiarito. SBC ritiene che la documentazione su un paziente non dovrebbe essere memorizzata per sempre in un supporto di sicurezza (file di backup) se il paziente non lo desidera, altrimenti sussiste il rischio di un utilizzo abusivo dei dati conservati nel backup, nonostante si pensasse di aver cancellato tutto. Ai fini legali i dati rimangono comunque sul sistema primario. *SBC* chiede il testo seguente: «Datensicherungsmedien, die älter als 2 Jahre sind, sollten gelöscht werden. Es soll dabei sichergestellt werden, dass alle aktuellen Daten in Datensicherungsmedien, die weniger als 2 Jahre alt sind, auch gesichert sind». Riguardo al numero 1.2.3, *Posta* chiede che cosa avviene con i fornitori di prestazioni aderenti a due comunità e come vengono gestiti i loro dati. Non è infatti chiaro se la serie di dati venga duplicata e, se sì, chi è responsabile della loro gestione. Per *IG eHealth* e *Posta* il requisito di cui al numero 1.2.3.3 non è plausibile. Un requisito deve

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

essere applicabile. A proposito del numero 1.2.3.1, *Tessaris* rimanda alla sua raccomandazione sui registri medici menzionati al numero 1.2.2.5. Per il numero 1.2.3.2, come indicato al numero 1.1.4.2, la verifica potrebbe risultare molto onerosa in funzione dei mezzi e delle procedure impiegati e autorizzati. Al numero 1.2.3.3 propone inoltre la seguente aggiunta: «Die Zugriffsrechte gemäss den in Artikel 1-3 EPDV festgelegten Kategorien und Optionen angepasst werden». *FMH* chiede sul numero 1.2.3.3 a cosa vengono adeguati i diritti di accesso.

1.2.4: I Cantoni *GE*, *VS*, *VD*, *JU* e *NE* segnalano che nella versione francese al numero 1.2.4.2 è stato ripetuto due volte di seguito «du patient» e che quindi se ne deve cancellare uno. *Tessaris* ricorda che i pazienti devono essere informati dell'ingresso e dell'uscita dei professionisti della salute e chiede l'aggiunta di un numero 1.2.4.4: «die Patientinnen und Patienten über den Eintritt sowie den Austritt einer Gesundheitsfachperson in die betreffende Gemeinschaft in textlich nachweisbarer Form informiert werden und ihre Optionen betreffend Zugriffsrechte ausüben können».

1.3 Gestione del personale ausiliario dei professionisti della salute

IG eHealth e *Posta* considerano che le disposizioni interne a una comunità non rientrano nel campo di applicazione della LCIP e che quindi non devono essere disciplinate. Si deve chiarire il campo di applicazione dell'OCIP e delle CTO. Per semplificare, *VAKA* propone che la gestione del personale ausiliario debba essere facoltativa e il numero 1.3 venga quindi stralciato. Secondo *Insel* la gestione del personale ausiliario è troppo onerosa, mentre *IG eHealth* chiede che il personale ausiliario debba essere gestito anche a livello intercomunitario per renderlo meglio visibile ai pazienti. *IG eHealth* chiede lo stralcio del numero 1.3.1, mentre *Insel* quello del numero 1.3. *HIN* esprime dubbi sulla portata del termine «personale ausiliario». Suppone che si riferisca ad assistenti di studio medico, infermieri e simili ed escluda implicitamente p. es. i cuochi di un istituto, il personale di pulizia, i collaboratori dell'amministrazione, ecc. Si chiede se non sia opportuno avere delle direttive. *STSAG* ritiene che si debba gestire solo il personale ausiliario che partecipa al trattamento dei dati e propone la seguente aggiunta al numero 1.3.1: «[…], sofern diese (die Hilfspersonen) in die Bearbeitung der Daten im elektronischen Patientendossier direkt eingebunden sind». Secondo *FMH* i processi per la gestione del personale ausiliario devono essere disciplinati in modo omogeneo nei requisiti di base a livello di ordinanza e non possono differire da comunità a comunità. È inoltre necessario specificare quali persone hanno accesso alla cartella informatizzata del paziente e chi ne assume la responsabilità. Riguardo al numero 1.3.2.1 propone una regolamentazione chiara a livello di OCIP. A proposito dei numeri 1.3.2 e 1.3.2.1 *BFH* sostiene che anche per il personale ausiliario si debbano definire dei metadati. È opportuno quindi designare amministratori e addetti al supporto che potranno richiedere e ricevere un accesso. *VGIch* teme che la gestione di singole persone, gruppi e personale ausiliario negli ospedali, così come viene richiesta attualmente, non sia fattibile o lo sia solo con un onere eccessivo, perché tale procedura non corrisponde alla prassi abituale e ben collaudata in vigore negli ospedali per l'impiego degli strumenti elettronici. L'ospedale deve essere considerato un «trusted domain». *KSSG* segnala che secondo l'ordinanza il personale ausiliario non deve essere sincronizzato con i servizi centrali e che quindi il paziente non può negargli l'accesso. Ciò rende la disposizione di autodeterminazione assurda e confonde il paziente che nei protocolli di accesso vede del personale ausiliario al quale non ha concesso esplicitamente il diritto di accesso. Anche il personale ausiliario deve essere inserito nell'HPD e sincronizzato con i servizi centrali. L'articolo deve essere cancellato. *KSSG* non approva neanche il numero 1.2.3.3 perché i diritti di accesso alla cartella informatizzata del paziente sono gestiti dai pazienti. Chiede quali processi amministrativi conducono a un adeguamento dei diritti di accesso ed è a favore dello stralcio di questo requisito. OFAC critica che il personale ausiliario non è registrato nei servizi di ricerca e quindi non può partecipare allo scambio fra le comunità. In alcune professioni sanitarie tutto il lavoro amministrativo nell'ambito della cartella medica è invece delegato al personale ausiliario. Ciò significa che quando una buona gestione della cartella richiede delle interazioni con altri professionisti della salute, il personale ausiliario non sarà più autorizzato a farlo. Sarebbe un passo indietro rispetto a oggi. Secondo *OFAC* l'autorizzazione ad avere uno scambio intercomunitario può essere valutata e concessa solo dal professionista della salute responsabile dell'ausiliario. In base all'articolo 2 lettera b LCIP il personale ausiliario deve essere registrato nel servizio centrale di ricerca e ottenere per delega i diritti concessi dal

paziente ai professionisti della salute. Altrimenti avverrà in pratica quanto segue: i professionisti della salute daranno al personale ausiliario il loro SID assieme alla password – con i problemi che ne conseguiranno.

1.4 Identificazione e autenticazione (art. 8 lett. d)

1.4.1 / 1.4.2: *HIN* indica che al numero 1.4.1 sono menzionati esplicitamente solo i professionisti della salute e al numero 1.4.2 anche il personale ausiliario. Ipotizza che anche il personale ausiliario abbia bisogno di un'identità propria ed è importante che anche il personale ausiliario possa utilizzare solo il SID di cui all'articolo 30 OCIP. Il numero 1.4.1 dovrebbe essere completato nel modo seguente: «Für den Zugriff von Gesundheitsfachpersonen und Hilfspersonen auf das elektronische Patientendossier [...]». *IG eHealth* e *Posta* temono che i login degli ospedali non siano più ammessi. IG *eHealth* aggiunge che il capoverso disciplina solo i requisiti del SID per l'accesso e chiede quali esigenze si applicano per le scritture in una cartella. *IG eHealth* chiede che anche i SID delle organizzazioni conformi alla legislazione cantonale siano accettati per l'accesso alla cartella informatizzata del paziente. Analogamente, *Posta* segnala che bisogna accettare i SID delle organizzazioni perché queste devono rispettare anche le prescrizioni di altre leggi. La certificazione dei SID in seno a un'organizzazione non rientra nell'OCIP. È inoltre opportuno chiarire se un'autenticazione a un unico fattore non sia sufficiente per i sistemi che consentono solo una visualizzazione protetta da scrittura del dossier medico. *Tessaris* chiede le seguenti modifiche al numero 1.4.2: «Gemeinschaften und Gesundheitseinrichtungen müssen sicherstellen, dass die eindeutigen Parameter der IDM von Gesundheitsfachpersonen und Hilfspersonen zuverlässig mit der registrierten Identität der jeweiligen Person in der Gemeinschaft bzw. der Gesundheitseinrichtung verbunden wird». *FMH* vede delle ridondanze nel numero 1.4.2 e propone una regolamentazione chiara a livello di OCIP.

1.4.3: Riguardo al numero 1.4.3 *privatim* rinvia ai suoi commenti nelle osservazioni generali sull'OCIP. *HIN* sostiene esplicitamente l'autenticazione forte a 2 fattori. *STSAG* considera inaccettabile inserire dei requisiti per i sistemi primari in un'ordinanza sulla cartella informatizzata del paziente, poiché gli istituti devono già osservare le disposizioni cantonali in materia. Visto il mancato rispetto della sovranità e della sicurezza dei dati dei sistemi primari, il numero 1.4.3 deve essere definitivamente stralciato. *K3* e *VZK* segnalano che i sistemi primari collegati sono probabilmente dei sistemi centrali utilizzati molto di frequente (Hospital Information System - HIS) ai quali si deve poter accedere rapidamente nell'attività corrente. Il numero 1.4.3 deve essere limitato in modo da essere applicato solo in caso di accesso alla cartella informatizzata del paziente da un sistema primario. *SSIM* e *FMH* constatano che nei numeri 1.4.3 / 1.4.3.1 si prescrivono delle esigenze in materia di sistemi primari e chiedono quindi di eliminare le disposizioni sull'autenticazione dei sistemi primari. *OFAC* osserva che le comunità non possono garantire nulla riguardo ai sistemi primari, perché non ne sono né proprietarie né responsabili. I sistemi primari non sono di responsabilità delle comunità.

Secondo *BHF*, dal numero 1.4.3.1 si potrebbe dedurre che i diritti di accesso si applichino anche ai documenti caricati, cioè ripresi nel sistema primario dalla piattaforma eHealth. Ci si chiede se s'intende che nel sistema primario è integrata una «finestra della cartella informatizzata del paziente» e che quindi non si lavora più nel sistema primario, ma che si visualizza esclusivamente un contenuto del browser sulla cartella informatizzata del paziente. La differenza sarebbe notevole e avrebbe delle ripercussioni dirette sui diritti di accesso, come già commentato a proposito dell'OCIP (art. 8, lett. e). Nella pratica non s'impiegano quasi mai tali procedure di autenticazione nei sistemi primari. Sono inoltre numerose le persone che non sono registrate nell'HPI perché non richiedono un accesso alla cartella informatizzata del paziente, ma che lavorano con i sistemi primari e potrebbero pertanto accedere ai documenti caricati. Ciò eluderebbe i presupposti della cartella informatizzata del paziente. Secondo *KSSG* il numero 1.4.3.1 comporterebbe che gli utenti dovrebbero usare un'autenticazione a due fattori per accedere a ogni applicazione che in qualche modo comunica con la cartella informatizzata del paziente, sia come fonte di documenti sia come fruitore di documenti. Le comunità devono garantire che tutti i sistemi tecnici, come p. es. i sistemi primari, utilizzino una procedura di autenticazione forte per accedere alla

cartella informatizzata del paziente (come attore IHE Document Consumer). *Posta* e *IG eHealth* sottolineano che il numero 1.4.3.1 indebolisce il numero 1.4.1. Bisogna rendere congruenti le CTO. *Posta* considera inaccettabile che da un lato si esiga l'impiego di SID rilasciati da emittenti certificati e dall'altro si accetti una procedura qualsiasi solo perché viene utilizzato un software diverso per l'accesso. Sempre riguardo al numero 1.4.3.1, *IG eHealth* e *Posta* desiderano una definizione del termine «Bearbeitung» (trattamento). A parere di *VGIch* il numero 1.4.3.1 sui sistemi primari collegati è in contraddizione con l'articolo 8 lettera d OCIP e le relative spiegazioni. L'articolo 8 lettera d e il rapporto esplicativo devono essere pertanto modificati.

VAKA ritiene poco chiara la richiesta formulata al numero 1.4.3.2 e sorprendente che in questo contesto vengano menzionati esplicitamente i sistemi primari. In funzione delle esigenze, le ripercussioni potrebbero rivelarsi enormi per i fornitori di prestazioni. L'esigenza deve essere formulata in modo più chiaro. 6 Cantoni[88] scrivono che la comunità non può garantire («garantir») che le migliaia di terminali impiegati siano affidabili, ma può solo informare i professionisti della salute. Il numero 1.4.3.2 deve essere stralciato. *Posta* e *IG eHealth* chiedono se l'esigenza indicata al numero 1.4.3.2 significa che tutte le strutture sanitarie destinate a collegare un sistema primario alla cartella informatizzata del paziente devono collegare il relativo sistema primario a un emittente di SID certificato. Ciò avrebbe ripercussioni sugli ospedali che si devono collegare. Tale requisito deve essere formulato in modo più chiaro. *Ahdis* critica la mancanza di indicazioni dettagliate sui terminali e chiede quindi una precisazione.

1.5 Gestione di gruppi di professionisti della salute (art. 8 OCIP lett. a, c, e e f)

FMH commenta al numero 1.5 che la prevista gestione di gruppi non è realizzabile e che deve quindi essere sostituita da una regolamentazione generale a livello di ordinanza. Il Cantone *ZH* ritiene che non sia né necessario né ammissibile dover informare i pazienti di ogni cambiamento nella composizione di un gruppo. Il termine «verhältnismässig» è inoltre inutile e poco chiaro. In ogni caso si dovrebbe rinunciare all'entità «gruppi di professionisti della salute». Chiede lo stralcio del numero 1.5.

6 Cantoni[89] sostengono che le comunità non possono essere responsabili dei gruppi di professionisti della salute. Esse possono solo prendere atto della loro composizione. Al numero 1.5.1 il brano di frase «sont responsable de la gestion» deve essere sostituito con «sont responsable de l'administration». I suddetti Cantoni aggiungono che il paziente non può accedere all'elenco completo dei professionisti della salute e del personale ausiliario di un gruppo o di una struttura. Già oggi ciò non avviene nella pratica. Inoltre, la composizione di una struttura o di un grande gruppo cambia quotidianamente. Non è possibile informare continuamente il paziente della composizione dei gruppi. Un ospedale è un esempio di struttura alla quale i pazienti possono concedere dei diritti. Frazionare la struttura in «gruppi ragionevoli» non ha alcun senso pratico. Il paziente dovrebbe concedere i diritti di accesso a una moltitudine di gruppi (p. es. radiologia, patologia), che non conosce. Chiedono pertanto di stralciare i numeri 1.5.2.1, 1.5.2.2 e 1.5.2.3. OFAC ritiene inapplicabili i requisiti al numero 1.5.2.2, poiché i gruppi sono soggetti a frequenti cambiamenti. Al numero 1.5.2.3 critica che una dimensione ragionevole non significa nulla di preciso. Riguardo al numero 1.5.2.1, *BFH* lamenta che il termine «jederzeit» non sia definito in modo preciso. Bisogna tenere conto del grande onere amministrativo che ciò comporta per una grande struttura sanitaria. Se «jederzeit» significa ogni ora/ogni giorno, questa disposizione creerebbe un onere supplementare notevole per i grandi istituti con medici assistenti che lavorano in diversi reparti, senza procurare vantaggi degni di nota. Anche il Cantone *AR* chiede che cosa s'intenda per «jederzeit nachvollziehbar» e desidera una precisazione. Dovrebbe inoltre essere precisato anche il brano di frase «die Grösse von Gruppen verhältnismässig bleiben» al numero 1.5.2.3. *Posta* scrive che, in caso di mancata definizione del termine «verhältnismässig», si atterrà ai desideri dei clienti. Anche *KSSG* considera il termine «verhältnismässig» impreciso e chiede lo stralcio del numero 1.5.2.3. I gruppi potrebbero essere suddivisi in settori specializzati. *SSIM* osserva che la dimensione dei gruppi dipende dalle dimensioni della struttura sanitaria e chiede una precisazione o lo stralcio. *STSAG* considera che i numeri 1.5.2.1 e 1.5.2.2 creano difficoltà inutili. Visto che il paziente può controllare gli accessi attraverso i protocolli,

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

non è comprensibile perché debba vedere tutti i potenziali professionisti della salute attribuiti a un gruppo di accesso. Inoltre il contenuto del numero 1.5.2.3 è già disciplinato attraverso i diritti di accesso ai sistemi primari. I numeri 1.5.2.1, 1.5.2.2 e 1.5.2.3 devono essere pertanto stralciati. Il Cantone *TI* considera che la gestione proposta dei gruppi di professionisti della salute (1.5.2.1 e 1.5.2.2) non è di facile attuazione. Nella pratica quotidiana il paziente non può accedere alle liste di tutti professionisti di strutture complesse (ospedali) che hanno accesso ai suoi dati. Questo tipo di gestione in tempo reale sarebbe troppo onerosa dove il turnover del personale è elevato. Entrambi i numeri devono quindi essere stralciati. *Privatim* segnala che i pazienti dovrebbero avere la possibilità di conoscere non solo la composizione attuale, ma anche i cambiamenti nella composizione dei gruppi (ingressi e uscite). Il testo dei numeri 1.5.2.1 e 1.5.2.2 dovrebbe essere formulato in modo più chiaro. *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* desiderano completare il testo del numero 1.5.2.2 in riferimento all'articolo 8 lettera f OCIP come segue: «[…] informiert werden können und informiert werden». *Insel* e *VGIch* segnalano che l'esigenza prevista al numero 1.5.2.2 non è attuabile in un ospedale e deve pertanto essere stralciata. Al numero 1.5.2.2 *Tessaris* propone la seguente aggiunta: «[…] in Gruppen von Gesundheitsfachpersonen und deren Austritt aus einer Gruppe von Gesundheitsfachpersonen informiert werden können». Il numero 1.5.2.3 dovrebbe essere completato come segue: «[…] verhältnismässig bleiben und im Regelfall die Zahl von Angehörigen der Gruppe nicht überschreiten».

2. Conservazione e trasmissione di dati (art. 9 OCIP)

2.1 Distruzione di dati (art. 9 cpv. 1 lett. a e b)

6 Cantoni[90] ribadiscono in riferimento al numero 2.1.1.1 quanto già espresso sull'articolo 20 OCIP, aggiungendo che i dati non dovrebbero essere cancellati. Sulla carta o nei sistemi primari non vengono cancellati e non vi è motivo che lo siano in un sistema secondario. Il vantaggio della cartella informatizzata del paziente consiste proprio nel proporre ai pazienti degli archivi duraturi. In materia sanitaria una limitazione a 10 anni non ha senso. Il paziente potrebbe essere interessato a dei trattamenti medici avvenuti 20 anni prima o durante la sua infanzia. Il Cantone *NE* ricorda che l'articolo 64 della legislazione sanitaria cantonale prevede effettivamente un limite di 10 anni per la conservazione della cartella, ma si tratta in questo caso di un limite minimo che non tiene ancora conto dell'«informatizzazione» della cartella. La questione dello spazio che occupano le cartelle cartacee nell'ambulatorio di un professionista della salute non si pone più negli stessi termini e alle stesse condizioni con la cartella informatizzata. In questo contesto non esistono più ostacoli logistici o tecnici che giustificherebbero la volontà del professionista della salute di non conservare più di 10 anni gli elementi della cartella del paziente nel suo interesse. *FMH* rinvia in questo contesto alle sue osservazioni sui relativi articoli dell'ordinanza. *BFH* segnala il divario fra le aspettative del paziente di disporre dei «suoi» dati nella «sua» cartella informatizzata e l'obbligo generale di conservazione vigente nel settore sanitario. Anche se il paziente viene informato e può chiedere una proroga di 10 anni (art. 9 cpv. 1 lett. a), ci si chiede perché debba prendere una decisione sulla conservazione dei suoi dati. Il paziente ha comunque la possibilità di cancellare in qualsiasi momento i dati. Se proprio si vuole un obbligo di distruzione, allora bisogna prevedere un trasferimento automatico nel repository per i documenti «privati». Volendo invece rinunciare a un obbligo di distruzione, il requisito al numero 2.1.1.1 deve essere stralciato. *Medshare* evidenzia in questo punto che esclusivamente il paziente decide da solo quando cancellare i documenti dagli archivi e dai registri. *STSAG* scrive che la scadenza di 10 anni di cui al numero 2.1.1.1 decorre dal termine del trattamento medico e si prolunga quindi automaticamente nei pazienti cronici. In alternativa, nel registry si potrebbero visualizzare solo i dati che non hanno più di 10 anni. *Tessaris* propone di formulare la cancellazione dei dati dei pazienti dopo 10 anni come «regola default». Per i dati sul decorso delle patologie croniche la durata di conservazione è di solito notevolmente più lunga. Chiede pertanto la seguente aggiunta al numero 2.1.1.1: «[…] erfassten Daten unter Vorbehalt einer festgelegten längeren Aufbewahrungsdauer nach 10 Jahren vernichtet werden». *OFAC* chiede cosa avviene dei dati che dopo 10 anni sono ancora rilevanti e rimanda alla LATer, la cui ultima revisione esige dai sistemi primari di archiviare per 30 anni i dati relativi all'impiego di prodotti sanguigni.

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

6 Cantoni[91] dichiarano in riferimento al numero 2.1.1.2 che, in caso di volontà del paziente di riattivare la sua cartella o per motivi medico-legali, non bisogna sopprimere subito la cartella, ma mascherarla per un certo periodo. *HIN* non capisce se in questa fattispecie bisogna cancellare anche i dati del login. Il testo parla di tutti i dati. Secondo l'articolo 20 capoverso 1 si devono invece sopprimere tutti i dati che non sono necessari all'adempimento dell'obbligo di tracciabilità e rendiconto. Al numero 2.1.1.2 si deve riprendere la stessa formulazione dell'articolo 20. *Posta* segnala che l'indice dei pazienti è un'infrastruttura che può essere riutilizzata più volte e chiede se sia consentito cancellare dall'indice dei pazienti solo le identità che appaiono nella cartella informatizzata del paziente. Le altre identità impiegate per altri processi (p. es. richieste di ricovero, visite specialistiche) rimarrebbero. L'impiego comune dell'infrastruttura è lecito ai sensi della LCIP. Le disposizioni che lo impediscono devono essere sostituite da altre che lo consentano nei limiti appropriati. L'indice dei pazienti dovrebbe rimanere un'eccezione e i dati dovrebbero essere cancellati se non servono ad altri scopi. *KSSG* considera che i requisiti per la conservazione dei dati, p. es. all'articolo 9 capoverso 1 lettera c OCIP e al numero 2.1.1.2.1, implicherebbero che le applicazioni che già si avvalgono di un registry non potrebbero più funzionare sull'infrastruttura esistente. Le disposizioni di esecuzione richiederebbero la creazione di un'infrastruttura separata per la cartella informatizzata del paziente e tutte le altre applicazioni, raddoppiando così i costi. Il numero 2.1.1.2.1 dovrebbe essere modificato in modo da tale da permettere una cancellazione logica e non fisica per l'applicazione «cartella informatizzata del paziente». Ciò consentirebbe di raffigurare nella stessa infrastruttura anche altre applicazioni. I requisiti previsti all'articolo 9 capoverso 1 lettera c OCIP e al numero 2.1.1.2.2 avrebbero altresì come conseguenza che il sistema di archiviazione esistente negli ospedali non possa essere impiegato come IHE Repository per la cartella informatizzata del paziente. Tali requisiti richiedono la creazione di un repository separato per i documenti inseriti dal paziente e quelli registrati dai professionisti della salute. Ciò significherebbe triplicare un'infrastruttura già costosa, che oltretutto conterrebbe dati ridondanti. Se lo scopo del numero 2.1.1.2.2 è di cancellare fisicamente i dati, non è possibile utilizzare i sistemi di archiviazione più convenienti (p. es. Centera). L'impatto in termine di costi si sentirebbe in particolare quando si devono registrare nella cartella informatizzata del paziente anche immagini radiologiche. Le tomografie computerizzate (TAC) e IRM pesano spesso diversi gigabyte e dovrebbero essere memorizzate in modo ridondante. L'articolo ha pertanto ripercussioni enormi sui costi di esercizio. Si chiede che tutti i dati possano essere memorizzati nello stesso repository fisico e che la separazione e la cancellazione dei dati per la cartella informatizzata del paziente avvengano a livello logico. I requisiti di protezione e di sicurezza dei dati verrebbero soddisfatti anche con una separazione logica. In riferimento al numero 2.1.1.2.3, *KSSG* ricorda che nel Cantone di San Gallo si impiega da diversi anni un indice dei pazienti per la comunicazione interospedaliera ed evidenzia i vantaggi di tale indice. Le attuali disposizioni di esecuzione impedirebbero l'utilizzo dell'attuale indice, poiché i pazienti potrebbero essere registrati nell'indice solo se hanno dato il loro consenso alla cartella informatizzata del paziente e dovrebbero essere cancellati se decidono di sopprimere la loro cartella informatizzata del paziente. Non sarebbe possibile costituire un secondo indice dei pazienti per la cartella informatizzata del paziente, poiché ne può esistere uno solo. L'attuazione delle attuali disposizioni di esecuzione degraderebbe il processo di cura. Si chiede di poter utilizzare l'indice dei pazienti per la cartella informatizzata del paziente oltre ad altri processi, senza però collegarlo all'ID della cartella informatizzata del paziente dell'UCC per i pazienti che non hanno dato il loro consenso. In caso di soppressione della cartella informatizzata del paziente si cancellerebbe semplicemente il collegamento con l'ID.

ISSS segnala che nei numeri 2.1.1.1 e 2.1.1.2 si dice che i dati devono essere cancellati, ma non è chiaro che cosa s'intenda esattamente, per esempio se è sufficiente la cancellazione (elettronica). Per disciplinare le esigenze in materia di distruzione dei dati, si propone di inserire un numero 2.1.1.3. Secondo *Tessaris,* l'obbligo di distruzione dovrebbe riferirsi in particolare anche ai file di sicurezza e ai backup, poiché si devono distruggere «tutti i dati».

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

2.2 Archivio di documenti (cpv. 1 lett. c)

Il Cantone *ZH* nonché *K3*, *VZK* e *ZAD* sottolineano che i requisiti di cui al numero 2.2 risultano già dalla LCIP e dall'OCIP e dovrebbero quindi essere stralciati. Il Cantone *AR* considera opportuno il requisito formulato al numero 2.2.1.1. *BINT*, *Integic* e *KSSG* scrivono invece che l'architettura di storage è in continua trasformazione e non dovrebbe essere fissata in un'ordinanza. 17 partecipanti[92] temono che una tale esigenza possa rivelarsi molto onerosa per i fornitori di prestazioni. *SSIM* e *FMH* criticano che per rispettare il numero 2.2.1.1, i fornitori di prestazioni devono creare un secondo archivio di dati ridondante, complicando così anche lo scambio bidirezionale di dati con la LCIP. *BFH* chiede se l'archivio di documenti possa funzionare in un ambiente virtualizzato. *SUVA* ritiene poco opportuno imporre alla comunità l'architettura dell'archivio di dati. Essendo un settore in rapida trasformazione, non ha senso disciplinarlo a livello di ordinanza. Nel complesso, 9 partecipanti[93] sono a favore dello stralcio del numero 2.2.1.1. *GKD* e 10 Cantoni[94] chiedono almeno una regolamentazione più semplice. L'impiego dell'archivio di documenti utilizzato anche per il SIC (*ZAD* parla nel suo parere di «sistema primario») dovrebbe essere ammesso, eventualmente con determinate prescrizioni tecniche. Il Cantone *ZH* sottolinea che gli eventuali requisiti tecnici per la sicurezza non devono essere talmente restrittivi da generare un incremento dei costi presso i fornitori di prestazioni. *HIN* afferma che qui basterebbe una separazione logica e propone la seguente redazione per il numero 2.2.1.1: «Dokumente des elektronischen Patiententendossiers jederzeit von anderen in der Datenablage gespeicherten Dokumenten getrennt werden können im Sinne einer kontrollierten logischen Trennung». Per *IG eHealth* e *Posta* non è chiaro cosa s'intenda con il termine «ausschliesslich», perché potrebbe sottintendere una duplice archiviazione. Quest'ultima sarebbe inopportuna perché farebbe raddoppiare i costi, sarebbe poco realistica da applicare e fortemente soggetta a errori. Propongono pertanto di stralciare il termine «ausschliesslich» al numero 2.2.1.1.

IG *eHealth* è del parere che al numero 2.2.1.2 s'intenda l'allegato 4 e non l'allegato 3 e che quindi l'errore dovrebbe essere corretto. *Posta* chiede se è permesso inserire nella cartella informatizzata del paziente dei documenti On Demand, visto che lo standard CDA-CH-MTPS si basa su documenti On Demand. Non bisogna inoltre dimenticare che le prescrizioni sono estremamente restrittive e impedirebbero qualsiasi adeguamento alle nuove tecnologie, cosa da evitare. Se il concetto di «zugelassenen Dateiformaten» si riferisce all'elenco di cui al numero 1.9 (MIME-Type del documento) dell'allegato 3, il Cantone *ZH* considera problematico limitare il numero dei formati di file ammessi. Innanzitutto non è sempre tecnicamente possibile convertire un documento in un formato ammesso e, in secondo luogo, non è probabilmente necessario. In particolare si dovrebbero supportare formati come PNG o SVG, ma anche documenti testuali. Per il resto, l'indicazione di formati come TIFF o XML è troppo poco precisa. Il numero 2.2.1.2 deve essere rielaborato o stralciato.

I Cantoni *GE*, *VD*, *VS*, *JU* e *FR* considerano il numero 2.2.1.3 troppo restrittivo. Oggi esiste il formato PDF/A-3, introdotto con la revisione della norma ISO 19005. Si potrebbe però anche utilizzare il formato PDF/X (ISO 15930). Queste norme evolvono continuamente. I dettagli tecnici non devono rientrare in un testo legislativo vincolante e quindi il numero in questione deve essere stralciato. IG *eHealth* afferma che limitarsi al formato PDF/A-1 o PDF/A-2 potrebbe comportare una conversione obbligata dei dati, che a sua volta potrebbe causare la perdita d'informazioni o d'integrità. Il sistema non dovrebbe procedere a una conversione del formato. Di conseguenza accetterebbe solo i dati in formato PDF/A-1 o PDF/A-2 e rifiuterebbe tutti gli altri formati. Gli utenti sarebbero riluttanti ad accettare tale limitazione. Il numero 2.2.1.3 deve pertanto essere stralciato. Secondo *Integic*, le indicazioni sul PDF/A-1 o PDF/A-2 non sono abbastanza precise, perché all'interno di questi due formati ci sono delle sotto-versioni con notevoli differenze in termini di requisiti e soprattutto di leggibilità. Il PDF/A-1a è per esempio destinato all'archiviazione nel lungo periodo e alle applicazioni accessibili, mentre il PDF/A-1b non lo permette. PDF/A-1 e PDF/A-2 devono piuttosto essere considerati come delle tecnologie evolutive che in parte si

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

sovrappongono, mentre le sotto-versioni disciplinano la semantica in modo più concreto[95]. *Integic* vuole una precisazione delle sotto-versioni ammesse di PDF/A-1 e PDF/A-2. Il Cantone *ZH* spiega che i formati PDF PDF/A-1 e PDF/A-2 sono stati sviluppati per l'archiviazione. Se s'impone l'impiego esclusivo di tali formati, molti documenti dovrebbero essere inutilmente convertiti. Per la cartella informatizzata del paziente non è necessario prescrivere tali formati e quindi il requisito deve essere stralciato. FMH chiede in riferimento al numero 2.2.1.3 se non si è già arrivati alla versione PDF/A-3. In un testo di legge non si dovrebbero mettere delle specificazioni così precise, soprattutto in un settore in continua evoluzione. *Posta* afferma che il numero 2.2.1.3 prevede un requisito inutilmente restrittivo. I dati devono essere cancellati dopo 10 anni. La maggior parte delle applicazioni non creano automaticamente il formato di archiviazione e *Posta* chiede quindi una definizione del comportamento richiesto dal sistema. Il sistema non deve procedere alla trasformazione del formato perché sussiste il rischio di perdita o cambiamento di dati potenzialmente rilevanti per il trattamento.

2.3 Gestione su richiesta del paziente (cpv. 2)

In riferimento al numero 2.3, *FMH* rimanda alle sue osservazioni sui relativi articoli dell'ordinanza. OFAC scrive che, oltre alla matrice dei gradi di riservatezza / diritti di accesso, si richiede una gestione flessibile («à la carte») dei tipi di documento per paziente. Oltre a essere assurdo dal punto di vista tecnico, è probabilmente pericoloso dal punto di vista medico tenere una cartella informatizzata del paziente incompleta, perché eventualmente i professionisti della salute, in situazioni di emergenza, potrebbero prendere delle decisioni mediche solo in base alla cartella informatizzata del paziente. Tale complessità sarebbe non solo inutile e irrealizzabile, ma anche potenzialmente pericolosa per la salute del paziente. *IG eHealth* e *Posta* criticano che l'esigenza formulata al 2.3.1.1.1 è poco chiara. La pubblicazione di documenti è compito dei professionisti della salute e non delle comunità. Di regola il paziente dà istruzioni ai professionisti della salute e non alle comunità. Queste non sono inoltre in grado d'interpretare il termine «bestimmte». Il requisito deve essere formulato in modo più chiaro perché nella versione attuale non può essere applicato. *KSSG* ritiene inapplicabile il numero 2.3.1.1.1. Se p. es. un paziente non vuole pubblicare nella sua cartella un test HIV che è parte di un'analisi completa di laboratorio (serie di analisi), può decidere o di pubblicare nella sua cartella informatizzata l'intero referto o di non pubblicarlo del tutto. Il numero in questione esige inoltre che, prima di pubblicare un documento, il medico chieda ogni volta il consenso del paziente. Si chiede di stralciare l'articolo 9 capoverso 2 lettera a OCIP e il numero 2.3.1.1.1 poiché il paziente può in qualsiasi momento modificare il grado di riservatezza in «dati segreti». Bisognerebbe inoltre definire meglio i termini «dati» e «documenti». *STSAG* considera esageratamente oneroso per le comunità il requisito del numero 2.3.1.1.1. In caso di bisogno, un paziente emancipato può assumere da solo tale compito. Poiché inoltre il servizio di riferimento per il paziente è la comunità di riferimento, tale compito dovrebbe semmai essere trasferito a quest'ultima. Si chiede lo stralcio completo del numero. Secondo 6 Cantoni[96] il paziente che non desidera far registrare i suoi dati nella cartella informatizzata, deve comunicarlo al professionista della salute. Poiché la comunità non può impedire la registrazione dei dati medici, chiedono lo stralcio del numero 2.3.1.1.1.

Gli stessi 6 Cantoni chiedono anche di stralciare il numero 2.3.1.1.2, visto che i dati medici non devono essere distrutti e che quindi non ha senso chiedere una proroga. Essi aggiungono che un paziente non dovrebbe avere la possibilità di cancellare i dati medici dalla sua cartella informatizzata. La cancellazione dei dati in un sistema secondario non ha inoltre alcun senso se i dati rimangono nel sistema primario. Il paziente che desidera mascherare i suoi dati può classificarli segreti. In caso di problemi medico-legali sarà importante sapere quando il paziente ha mascherato i suoi dati e se il professionista della salute ha avuto la possibilità di venirne a conoscenza. Anche il numero 2.3.1.1.3 deve essere stralciato. Ai numeri 2.3.1.1.1 – 2.3.1.1.3, *K3* e *VZK* deplorano la mancanza di una regolamentazione vincolante per i documenti che vengono trasmessi da un'altra comunità (attraverso XCA) alla cartella informatizzata del paziente. XCA consente solo un «accesso di lettura» senza autorizzazioni di scrittura, mutazione o cancellazione. La cancellazione completa richiede delle regole precise applicabili all'in-

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

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

sieme delle comunità svizzere, lo spazio di fiducia della cartella informatizzata del paziente. Tale osservazione vale anche per altri numeri. *K3* e *VZK* propongono pertanto di definire una regolamentazione in tal senso. In riferimento al numero 2.3.1.1.3, il Cantone *ZH* non ritiene necessario che il paziente possa richiedere la distruzione di dati nella cartella informatizzata del paziente. Questa deve rimanere completa perché solo così si garantisce la disponibilità dei dati, p. es. in caso di contenziosi legali. Il paziente può semplicemente classificare i dati con il grado di riservatezza «dati segreti». Il numero deve essere pertanto stralciato. *medshare* sottolinea riguardo al numero 2.3.1.1.2, che la cartella informatizzata del paziente appartiene al paziente dall'apertura fino al suo decesso e che solo lui è autorizzato a sopprimerla. Il numero deve essere stralciato. In riferimento al numero 2.3.2, *privatim* rimanda alle sue osservazioni generali sull'OCIP.

2.4 Applicazione dei gradi di riservatezza (cpv. 3 lett. a)

K3, *VZK*, *ZAD* e il Cantone *ZH* commentano che le condizioni risultano già dalla LCIP e OCIP. *VAKA* propone che il paziente debba avere la possibilità di non concedere autorizzazioni. OFAC dichiara che la traduzione in francese dei gradi di riservatezza è una vera catastrofe. Alcuni gradi portano la designazione di una categoria di dati definita all'articolo 3 LPD. Comunemente, la maggior parte dei dati appartiene a più categorie: i dati medici sono sia utilitari che sensibili. Non è logico in una cartella informatizzata del paziente che i dati medici si trovino solo al secondo grado e che siano superati da due gradi superiori. 6 Cantoni[97] chiedono che tutti i gradi e il loro impiego nella pratica vengano meglio definiti e completati da esempi concreti. A parere di *Integic*, il numero 2.4.1.3 implica che, a seconda dei parametri di accesso scelti, i professionisti della salute non possono più consultare i dati classificati «sensibili». Si dovrebbe esplicitare che per i professionisti della salute il cambiamento dei gradi di riservatezza richiede un'apposita autorizzazione o che la modifica costituisce un'autorizzazione. SQS segnala che le descrizioni dei 4 gradi di riservatezza sono tradotte nell'allegato 3 Metadati, 1.5. Grado di riservatezza. Il grado di riservatezza con il codice 30002 è descritto in inglese con «useful medical data» e in tedesco con «nützliche Daten». Gli altri codici hanno in inglese e in tedesco la stessa descrizione e bisogna quindi procedere alla stessa stregua anche qui. *STSAG* chiede di riformulare il numero 2.4.1 come segue: «Stammgemeinschaften müssen […]», e riguardo al numero 2.4.1.3 scrive che questa funzione deve essere automatizzata e realizzabile attraverso appositi servizi.

2.5 Attuazione della decisione di accesso (cpv. 3 lett. a)

FMH evidenzia che non si tratta di «una decisione di accesso della comunità di riferimento», ma di una richiesta di verifica alla quale bisogna dare una risposta positiva. In altri punti si è utilizzato il termine «Authorisierungsentscheid», decisione di autorizzazione. La terminologia deve essere riveduta e resa più omogenea. I Cantoni *GE*, *FR*, *VS*, *VD* und *JU* lamentano la mancanza di chiarezza al numero 2.5.1.1 e chiedono se le comunità devono informarsi presso le comunità di riferimento su quali diritti ha concesso il paziente e in quale forma. I diritti sono contenuti nel registro delle autorizzazioni collegato all'indice dei pazienti, al quale le comunità devono avere accesso. Si deve precisare e chiarire l'«use case».

2.6 Accesso di emergenza (cpv. 3 lett. a)

A proposito del numero 2.6 *FMH* rimanda alle osservazioni espresse sui relativi articoli dell'ordinanza. Il Cantone *ZH*, *K3*, *VZK* e *ZAD* considerano troppo complicate le esigenze previste in questo numero e chiedono quindi di semplificarle. *STSAG* ritiene che i compiti elencati al numero 2.6.1 debbano essere trasferiti alle comunità di riferimento. Il Cantone *TI* scrive che il requisito non è praticabile nella gestione di un caso d'urgenza. È necessaria una semplificazione della procedura per il tramite di una risposta preimpostata. L'operatore sanitario che effettua l'accesso deve motivare in seguito la forzatura del sistema. Sulla stessa falsariga, *SSIM*, *BINT*, *IG eHealth*, *SUVA* e *FMH* chiedono che al numero 2.6.1.1 il termine «vorgängig» venga sostituito da «nachträglich», permettendo così una motivazione a posteriori. Riguardo al numero 2.6.1.1, *medshare* sottolinea che in caso di emergenza, ogni minuto è prezioso per

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

il paziente. Per questo motivo le prestazioni mediche hanno indubbiamente la priorità sugli aspetti amministrativi. Il testo di legge deve essere modificato come segue: «innert 24 Stunden eine Begründung […]». *VAKA* vuole invece rinunciare a qualsiasi motivazione e chiede quindi di stralciare il numero 2.6.1.1.

USB si dichiara favorevole a un accesso di emergenza il più semplice possibile per i professionisti della salute. Propone a tal fine di fondere i numeri 2.6.1.1 e 2.6.1.2 con la seguente nuova redazione: «der Notfallzugriff in der Protokollierung als solcher dokumentiert ist und sich von den übrigen Zugriffen unterscheiden lässt». *IG eHealth* e *Posta* segnalano che il numero 2.6.1.2 renderebbe molto oneroso l'utilizzo della cartella informatizzata del paziente in caso di emergenza. È importante tenere conto della fruibilità. Chiedono che i professionisti della salute possano vedere in qualsiasi momento che il caso è stato dichiarato come emergenza e che gli accessi avvengono con un'autorizzazione di emergenza. Una prassi analoga è applicata ai documenti forniti dai pazienti. Neanche in quel caso il professionista della salute deve confermare ogni volta che la fonte dei dati è nota. Secondo *SCH* l'accesso di emergenza deve poter avvenire rapidamente visto che il professionista della salute interessato è già registrato. La registrazione più severa non comporta alcun vantaggio supplementare perché la persona è già identificata. Per questi motivi il numero 2.6.1.2. deve essere stralciato. *SUVA* è a favore di un accesso di emergenza rapido e non burocratico, con la possibilità di indicare la motivazione a posteriori. Il numero 2.6.1.2 dovrebbe di conseguenza leggere: «ein Notfallzugriff auch ohne nochmalige Bestätigung […]». *ISSS* chiede fra l'altro come si possono proteggere dagli abusi gli accessi di emergenza e come si presenta in dettaglio l'interazione manuale qui indicata. Il processo richiede una formulazione dettagliata.

SSIM desidera sostituire il termine «unverzüglich» al numero 2.6.1.3 con «nachträglich». *Posta* chiede a riguardo cosa significa «unverzüglich» e se si può scegliere anche la via postale. *FMH* dichiara che l'informazione sistematica a posteriori e un'eventuale motivazione in caso di sospetto di abuso costituiscono una soluzione sensata e sufficiente.

Integic vorrebbe che venissero specificate anche le condizioni quadro alle quali deve avvenire la presa di contatto. Riguardo al numero 2.6.1.4 *HIN* sottolinea che l'informazione può contenere dati degni di protezione e che deve avvenire naturalmente solo attraverso canali protetti in conformità con i requisiti sulla protezione dei dati. Propone dunque la seguente modifica o aggiunta: «[…] (z.B. SMS, E-Mail, etc.) und schützenswerte Daten enthält, muss datenschutzkonform via geschützte Kanäle erfolgen. Andernfalls darf nur die Angabe, dass ein Notfallzugriff erfolgte, mit Datum und genauer Uhrzeit enthalten sein sowie der Hinweis, dass die genauen Umstände des Zugriffs dem elektronischen Patientendossier entnommen werden können». Analogamente, *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* propongono la seguente redazione: «[…] übermittelt wird nur die Angabe, dass ein Notfallzugriff erfolgte, mit Datum und genauer Uhrzeit enthält sowie den Hinweis, dass die genauen Umstände des Zugriffs dem elektronischen Patientendossier entnommen werden können».

2.7 Verifica dell'amministrazione dei diritti (art. 9 cpv. 3)

BINT sostiene che il numero 2.7 potrebbe generare un onere illimitato visto che lo scenario e le funzionalità sono sconosciuti. 6 Cantoni[98] affermano che il quadro degli scenari di test deve potere essere scelto dal fornitore e dall'organismo di certificazione. In funzione del numero di test non è necessaria un'automatizzazione, che complicherebbe inutilmente la struttura. Questo tipo di dettagli non deve essere inoltre incluso in un ambito legislativo vincolante. Chiedono quindi lo stralcio del termine «automatisés» al numero 2.7.1. *Privatim* chiede a quali dati è possibile accedere nel quadro degli scenari di test automatizzati e chi è autorizzato a farlo. Desidera una precisazione e ricorda che è necessario evitare accessi non autorizzati ai dati. *SQS* domanda chi decide quando le funzionalità e le valutazioni delle regole possano essere considerate corrette e chiede di completare la disposizione con un numero 2.7.1.2. Propone inoltre di fissare o determinare i valori ammessi per la verifica e di definire chi è responsabile della fissazione di tali valori.

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

2.8 Metadati (cpv. 3 lett. b)

FMH rimanda in riferimento al numero 2.8 alle osservazioni espresse sui relativi articoli dell'ordinanza. *HIN* e *SQS* presumono che per «Metadaten» s'intenda l'allegato 3 e non l'allegato 4 e chiede quindi una correzione. Anche *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* commentano che i metadati si riferiscono all'allegato 4 dell'OCIP-DFI. Nell'allegato 4 si stabiliscono però i formati di scambio e non i metadati. Si presuppone quindi che in questo caso s'intenda l'allegato 3. IG *eHealth* e *Posta* criticano la formulazione rudimentale e minimalista del numero 2.8.1. Osservano che i metadati devono essere curati e chiedono che le CTO prescrivano come le comunità debbano attuare gli adeguamenti dei metadati in termini di velocità, completezza, ecc.

2.9 Profili d'integrazione (cpv. 3 lett. d)

FMH rimanda anche qui alle osservazioni espresse sui relativi articoli dell'ordinanza. SQS s'informa se esiste un solo regolamento di utilizzazione dell'UCC. La ricerca del regolamento di utilizzazione attraverso zas.admin.ch è stata infruttuosa. Sarebbe opportuno verificare ed eventualmente indicare una denominazione più precisa. 6 Cantoni[99] criticano che il numero 2.9 contiene dettagli tecnici, soggetti a possibili sviluppi, che non dovrebbero essere riportati in questa forma in ambito legislativo vincolante. L'articolo deve essere semplificato e si devono eliminare tutti i riferimenti a norme soggette a sviluppi. Il Cantone *ZH* si associa a tale richiesta e ribadisce che non è opportuno fare prescrizioni tecniche di tale portata. Secondo *medshare* non è possibile pretendere da tutti i partecipanti del settore di rispettare le regolamentazioni, mentre l'UCC ne è esonerato. Propone che l'UCC implementi IHE XCPD e che le comunità consultino presso l'UCC il NIP della cartella informatizzata del paziente attraverso IHE XCPD.

2.9.1/2.9.2 Interfacce standard con la banca dati d'identificazione dell'UCC: *VAKA* mette in guardia contro l'utilizzo di interfacce supplementari. I profili forniti da *IHE* sono già difficili da attuare. Alla stessa stregua di *K3* e *VZK,* vuole lo stralcio di interfacce supplementari. *Privatim* segnala che non sono i punti di accesso delle comunità, ma le comunità stesse a doverlo garantire. È opportuno rettificare il testo, poiché i punti di accesso non sono dei soggetti con obbligo di agire. 6 Cantoni[100] affermano che non serve ricordare delle tautologie, anche perché la comunità può dimostrare che dispone di prescrizioni, ma non che le rispetta. Chiedono pertanto lo stralcio del numero 2.9.2. La stessa richiesta è avanzata da *VAKA*, *K3* e *VZK*, i quali aggiungono che tali prescrizioni debbano essere assolutamente formulate nell'ambito delle presenti ordinanze e non spostate altrove.

2.9.3 Profili d'integrazione, adeguamenti nazionali dei profili d'integrazione e profili d'integrazione nazionali: *BINT* e *Integic* sostengono che dovrebbe essere necessaria una prova di conformità con i suddetti profili IHE. Senza Conformance Statements e prova del superamento di test IHE Connect-A-Thon, tale criterio non può essere certificato in modo serio. Tali prove devono quindi essere richieste per i profili IHE rilevanti. *Posta* considera poco chiaro il campo di applicazione del numero 2.9.3. Bisognerebbe applicare solo lo scambio fra le comunità e non all'interno di una comunità. Il numero in questione dovrebbe essere completato nel modo seguente: «[…] Informationsübertragung zwischen Gemeinschaften die Integrationsprofile […]».

2.9.4 Attori e transazioni dei profili d'integrazione – comunicazione intercomunitaria: *BINT* e *HIN* ritengono che gli accessi intercomunitari devono essere gratuiti. Se le comunità possono esigere tasse di roaming, la divulgazione e l'approccio federativo della LCIP non possono essere realizzati. Vi sarebbe inoltre il pericolo di situazioni di monopolio, visto che già esiste una limitazione in termini di gestore per il portale dei pazienti. Essi chiedono di completare il numero 2.9.4 come segue: «nach Anhang 5 der EPDV- EDI kostenlos unterstützen». *IG eHealth* e *Posta* evidenziano che il requisito indicato al numero 2.9.4.2 non dovrebbe essere necessario. Il numero 2.9.1 definisce le interfacce con l'UCC. L'UCC offre anche un WebService. Ricordano inoltre che SEDEX non è gratuito e chiedono chi debba sostenere tali

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

costi. Propongono di cancellare questo requisito. *BINT*, *Integic*, *IG eHealth* e *ahdis* sono favorevoli allo stralcio del numero 2.9.4.4. La Patient Location Query è esclusa esplicitamente nell'allegato 5 dell'OCIP-DFI. *BINT*, *Integic* e *ahdis* vorrebbero l'inclusione di un numero 2.9.4.5; Update Document Set Cross Community [ITI-xxx]. Essi scrivono che per modificare in un'altra comunità i gradi di riservatezza dei metadati di un documento è necessaria una transazione Cross Community. Vorrebbero poi creare anche un numero 2.9.4.6; On-Demand Documents Option (vedi ITI TF-2a, 3.18.4.1.2.5).

SQS fa rilevare che le verifiche tecniche di tale profondità non possono essere effettuate nell'ambito dell'audit di un sistema di gestione e non sono compatibili con l'essenza stessa dell'audit (prove a campione). I requisiti qui descritti sono dei criteri di prova obbligatori, che devono essere validati e protocollati nel quadro della messa in funzione dei sistemi/delle interfacce. Queste prove devono essere disciplinate al di fuori delle certificazioni vere e proprie, p. es. nell'ambito di una verifica tecnica. Nel corso della certificazione si deve verificare mediante dei controlli solo se tali verifiche sono state effettuate e se gli eventuali esiti sono stati trattati. La norma di certificazione non definisce invece quanto sia rilevante l'esito. Concretamente *SQS* chiede di completare i numeri 2.9.4 – 2.9.21 con una disposizione riguardante la prova delle avvenute verifiche tecniche delle premesse tecniche e ripete la richiesta per tutti i numeri rilevanti.

2.9.5/2.9.6 Attori e transazioni dei profili d'integrazione – comunicazione di identità autenticate: *KSSG* osserva in riferimento al numero 2.9.5 che non ritiene sufficiente XUA e che bisognerebbe optare per XUA++. *Ahdis* fa notare che al numero 2.9.6 manca una spiegazione di come un X-Service User ottiene l'assertion dal X-Assertion Provider e come deve essere la relazione nei confronti dell'User Authentification Provider.

2.9.9 Attori e transazioni dei profili d'integrazione – messa a disposizione dei documenti: *KSSG* chiede se sia obbligatorio archiviare i documenti nel repository mediante Provide and Register Document Set-b. Si potrebbero per esempio archiviare i documenti nel repository anche attraverso HL7 MDM e poi registrarli nel registry con la transazione Register Document Set. A San Gallo si procede così, poiché le fonti dei documenti non supportano sempre il Provide and Register Document Set-b. Nell'ambito dei prodotti medici è poco probabile che questo requisito venga sviluppato per il mercato svizzero. Il numero dovrebbe essere ampliato in modo da consentire altre varianti di memorizzazione di documenti nel repository.

2.9.10 Attori e transazioni dei profili d'integrazione – mutazione dei metadati dei documenti: *IG eHealth* e *Posta* chiedono chi può assumere il ruolo di «Document Administrator». Se si tiene conto dei diritti degli autori è chiaro che ogni autore è anche implicitamente un «Document Administrator» dei documenti da lui pubblicati. Se non si considerano invece i diritti degli autori, questo requisito non è attuabile. Essi aggiungono che Update e Delete Document sono delle funzioni forti e che bisogna quindi chiarire chi può esercitare tali funzioni. Chiedono pertanto una definizione a riguardo, nel caso in cui l'autore non riceva implicitamente tale funzione. *IG eHealth* rileva inoltre in riferimento al numero 2.9.10.1 che, secondo l'articolo 1 capoverso 1 OCIP, si deve sempre indicare un grado di riservatezza. Consiglia poi lo stralcio del numero 2.9.10.2, perché basta modificare i metadati.

2.9.11 Attori e transazioni dei profili d'integrazione – registro di documenti: *IG eHealth* e *Posta* osservano che la LCIP si focalizza sullo spazio di fiducia fra le comunità. Le transazioni XDS.b sono «out of scope». Sarebbe opportuno definire più chiaramente il campo di applicazione della LCIP, dell'OCIP e delle CTO. *Integic* sottolinea riguardo al numero 2.9.11.2 che il termine corretto è «Registry Stored Query» e che bisogna quindi correggerlo. Rileva inoltre delle incongruenze nelle transazioni menzionate. Sono indicate per esempio delle transazioni che gli autori devono poter eseguire o ricevere/elaborare. Le transazioni che devono essere eseguite a seconda dell'IHE Actor (quindi ricevere e inviare) sono lacunose. Per esempio, 2.9.12. dovrebbe supportare ITI-42, poiché questa transazione avviene da Document Repository a Document Registry, ma è indicata solo nel Document Registry (2.9.11). Queste incongruenze devono essere corrette.

2.9.12 Attori e transazioni dei profili d'integrazione – archivio di documenti: *Integic* ribadisce il suo parere espresso sul numero 2.9.11 e critica inoltre che manca completamente la transazione ITI-64, con il relativo profilo IHE XAD-PID Change Management, essenziale per i processi di clearing e per garantire la qualità dei dati nei registri dei link. Sarebbe opportuno aggiungere la transazione ITI-64. *KSSG* ribadisce il suo parere relativo al numero 2.9.9 anche per il numero 2.9.12.1.

2.9.15 Attori e transazioni dei profili d'integrazione – gestire l'indice dei pazienti: *BINT* ripete il commento effettuato sul numero 2.9.4 anche per il numero 2.9.15.3 e propone, alla stessa stregua di *Integic* e *ahdis*, di stralciare questo numero. Non è infatti necessaria una segnalazione di update per l'ID del paziente. La casistica di una tale applicazione non è evidente.

2.9.16 - 2.9.18 Attori e transazioni dei profili d'integrazione - autenticazione di sistemi e verbalizzazione delle transazioni IHE: *Integic* e *ahdis* chiedono lo stralcio del brano di frase «grouped with Any IHE Actor» dei numeri 2.9.16 e 2.9.17. Secondo *medshare* le Secure Applications e i Secure Nodes devono essere trattati allo stesso modo. I sottopunti del numero 2.9.17 e del numero 2.9.18 dovrebbero essere ripresi in entrambi i numeri. *IG eHealth*, *Integic* e *ahdis* chiedono di aggiungere un numero 2.9.18.2 «Maintain Time [ITI-1]». Ciò in base all'allegato 5 OCIP-DFI, punto 1.4.2.4 ATNA Secure Application.

2.9.22 – 2.9.24 Autenticazione con certificati validi: Riguardo ai certificati elettronici, provenienti dai servizi di certificazione di cui alla FiEle, OFAC afferma che la FiEle disciplina le condizioni alle quali i fornitori di servizi di certificazione che operano nel settore della firma elettronica possono essere riconosciuti, nonché i loro diritti e doveri. Tale legge definisce l'ambito che consente alle persone fisiche di firmare elettronicamente dei documenti. La FiEle è però limitata al settore della firma elettronica e non copre assolutamente il modo d'identificarsi o autenticarsi delle persone giuridiche e i loro diversi punti di accesso tecnici. L'esigenza di acquisizione dei certificati presso fornitori di servizi di firma elettronica non è dunque fondata e non offre alla cartella informatizzata del paziente nessuna garanzia supplementare rispetto ai servizi di certificazione esistenti sul mercato. *Posta* chiede, in riferimento al numero 2.9.22, se sono ammessi i certificati soft. *Medshare* ritiene che l'UCC debba essere trattato alla stessa stregua dei servizi centrali di ricerca di dati e propone la fusione con il numero 2.9.22.3, anche all'articolo 38 capoverso 1 OCIP. Al numero 2.9.23, *medshare* segnala che manca il riferimento ai documenti. Per il resto, *medshare* ribadisce il commento fatto al numero 2.9 anche riguardo al numero 2.9.24. CT (consistent time) è una premessa per ATNA. ATNA è il presupposto per gli altri profili IHE. *Medshare* scrive che sarebbe più opportuno che il CT utilizzasse come fonte l'ora della Svizzera.

2.9.25 Impiego coerente dell'ora svizzera: *SQS* chiede chi decide quali sono i sistemi rilevanti per l'elaborazione dell'informazione e su quali basi. Desidera inoltre sapere se p. es. uno smartphone o un tablet sono dei sistemi rilevanti. Affermazioni di questo tipo potrebbero essere interpretate e valutate in modo diverso nel quadro degli audit. Concretamente si vuole una descrizione esplicita del termine «relevantes informationsverarbeitendes System». *IG eHealth* e *Posta* chiedono invece perché non si fa riferimento in questo punto al profilo CT.

2.10 Dati verbalizzati (cpv. 3 lett. e), requisiti in materia di sistema di verbalizzazione

FMH rimanda alle osservazioni espresse sui relativi articoli dell'ordinanza, in particolare segnala però che la verbalizzazione degli accessi ha una rilevanza in materia di responsabilità civile anche per chi eroga le cure. Tale procedura deve servire obbligatoriamente a provare quale dati l'erogatore di cure ha visto al momento dell'accesso.

2.10.2: 7 partecipanti[101] chiedono cosa significhi «auf das erforderliche Mass» e come venga definito. *K3*, *VZK*, *ZAD* e il Cantone *ZH* chiedono lo stralcio di tale concetto. Il Cantone *ZH* vuole inoltre che dal protocollo emerga – contrariamente a quanto indicato al numero 2.10.2 – quali dati sono stati consultati. Altrimenti il paziente non è in grado di valutare se l'accesso è avvenuto in modo legale. Si deve garantire che il protocollo sia sempre completo, se si vuole instillare fiducia nel sistema. *IG eHealth* chiede di

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

inserire la nozione di «erforderliches Mass» nella definizione dei termini, altrimenti questa dimensione deve essere disciplinata in un regolamento di esercizio a livello nazionale. Il Cantone *ZG* propone dal canto suo una precisazione del termine. Secondo *medshare* il concetto di «Medizindaten» non è chiaro e deve essere precisato.

2.10.3: *IG eHealth* e *Posta* chiedono se è vero che basta poter provare una modifica a posteriori. Propongono di riformulare il numero 2.10.3.2 come segue: «[…] von Protokolldaten muss klar erkennbar sein». *Tessaris* scrive a proposito della modifica a posteriori dei dati verbalizzati che nella pratica potrebbe accadere che i dati verbalizzati si rivelino non corretti o incompleti. Bisogna pertanto prevedere la possibilità di correggerli o completarli. Una modifica a posteriori dei dati verbalizzati non dovrebbe essere ammessa. Le aggiunte, correzioni o modifiche di registrazioni nel protocollo devono essere designate come tali e corredate di informazioni sul loro autore nonché di marcatura oraria.

Bleuer osserva, in riferimento al numero 2.10.3.3, che la verbalizzazione della consultazione dei propri dati costituisce un'ingerenza nella sfera privata del cittadino e che quest'ultimo debba acconsentirvi espressamente. A parere del Cantone *ZH*, la cartella informatizzata del paziente dovrebbe essere impostata in modo che gli amministratori del sistema non abbiano accesso ai dati del paziente. Il criptaggio e l'amministrazione delle chiavi di criptaggio dovrebbero essere implementati in modo che né gli amministratori OS né gli amministratori DB possano leggere i dati criptati. Tutti i dati dovrebbero essere criptati. *Privatim* segnala ai numeri 2.10.3.3 e 2.10.3.4 che il paziente dovrebbe poter vedere se un amministratore del sistema ha avuto accesso ai dati della sua cartella informatizzata e chiede che la disposizione venga modificata in tal senso.

SQS evidenzia in riferimento al numero 2.10.3.4 che le limitazioni tecniche possono sempre essere aggirate con le apposite autorizzazioni. La problematica deve pertanto essere risolta a livello amministrativo. La limitazione dei diritti degli amministratori deve essere inserita in un'istruzione. Sulla stessa falsariga, *KSSG* afferma che i dati verbalizzati sono manipolabili fino alla loro archiviazione e che quindi tale disposizione è solo parzialmente attuabile. Il numero 2.10.3.4 deve quindi essere stralciato o modificato. Anche *SCH* critica l'attuabilità tecnica e propone di modificare il numero 2.10.3.4 come segue: «Systemlogs müssen revisionssicher aufbewahrt werden». *BFH* ritiene che gli amministratori di sistemi non dovrebbero poter cancellare o disattivare anche altre attività e chiedono di rettificare il numero 2.10.3.4: «[…] die Protokollierung von Aktivitäten zu löschen oder zu deaktivieren».

2.10.4: *Integic* considera che le registrazioni nel protocollo di cui al numero 2.10.4, siano un'ingerenza nella sfera privata del cittadino, se riguardano la consultazione dei propri dati. È il paziente a dover decidere a riguardo. Il parere di *SUVA* è dello stesso tenore: questa prescrizione viola la sfera privata del cittadino che dovrebbe essere libero di accedere ai propri dati quando e come vuole, senza che ciò sia visibile per un professionista della salute. Su questo punto si dovrebbe trovare un'altra soluzione compatibile con la LPD. 6 Cantoni[102] criticano la traduzione francese del numero 2.10.4.1.3 e propongono la seguente redazione: «configuration des autorisations ou gestion des autorisations».

Posta e *IG eHealth* chiedono, in riferimento al numero 2.10.4.2, se sia opportuno indicare ai pazienti nel log anche i tentativi di accesso rifiutati. Dubitano che sia necessario indicare nel log ogni ricerca con i relativi criteri, perché potrebbe dar adito a confusione, soprattutto se la ricerca è stata infruttuosa. Desiderano quindi una precisazione. Riguardo al numero 2.10.4.2.1 scrivono inoltre che l'elenco è focalizzato sulla visualizzazione da parte del paziente. Chiedono se è vero che il paziente possa andare a controllare a piacimento per qualsiasi professionista della salute quando questo ha effettuato un login o un logout, oppure se s'intende invece il login/logout del paziente. Si deve verificare la formulazione «Fokus», mentre sembra opportuna la verbalizzazione. Propongono inoltre la seguente aggiunta: «die eigene Authentifizierung […]». Al numero 2.10.4.2.3, *Posta* critica che vi potrebbero essere molte registrazioni, perché spesso i medici fanno ricerche non specifiche. La limitazione del numero dei risultati nei profili IHE è opzionale e manca una prescrizione che la renda obbligatoria. La valanga d'informazioni non migliora la sicurezza. La formulazione del numero dovrebbe essere completata e resa più coerente.

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

Medshare ritiene questo numero incomprensibile e dichiara che si possono cercare i documenti e non la cartella informatizzata del paziente. Si deve precisare cosa s'intende. Riguardo al numero 2.10.4.2.5 *medshare* desidera una precisazione o una motivazione. *KSSG* segnala che i logdata consultabili dal paziente sono generati dal profilo IHE ATNA, che però a suo parere non supporta tale requisito. Il numero 2.10.4.2.7 deve essere stralciato. La verbalizzazione di un nuovo SID può essere richiesta nei systemlog ma non nell'ATNA e quindi non è visibile per il paziente. Per il numero 2.10.4.2.7, *SCH* afferma che la registrazione di un nuovo SID è un processo che avviene isolatamente nell'Identity Provider. L'Identity Provider non è però necessariamente un componente IT della comunità, ma può essere esternalizzato a terzi. Il protocollo SAML imposto per la comunicazione dei portali con gli Identity Provider non prevede uno scambio di dati verbalizzati fra gli Identity Provider e i portali. L'informazione sulla registrazione di nuovi SID non è quindi disponibile nella comunità e non può pertanto essere registrata nei protocolli.

2.10.5: 6 Cantoni[103] osservano che se il risultato della ricerca non si riferisce a un solo paziente, la ricerca non necessita di una storicizzazione. Non è inoltre tecnicamente possibile rintracciare una stampa o impedire uno screenshot. I numeri da 2.10.5.1 a 2.10.5.3 devono dunque essere stralciati. *Integic* ribadisce il parere espresso sul numero 2.10.4. *SUVA* segnala che le sue osservazioni sul 2.10.4 valgono anche per questo punto, se si tratta di una ricerca del paziente nei propri dati. *Privatim* ritiene che sia poco chiaro se il paziente può vedere nel protocollo chi ha avuto accesso ai suoi dati. Si tratta in ogni caso di un'informazione importante e dovrebbe apparire nel protocollo. Di regola, la persona che accede dovrebbe essere nota al sistema, altrimenti il protocollo dovrebbe indicare che gli accessi sono stati effettuati da ignoti. Si chiede di specificare o completare la disposizione. Secondo *SSIM* e *FMH* la verbalizzazione della funzione di ricerca e dei parametri di ricerca è esagerata e dovrebbe essere stralciata. Gli accessi mediante create, read, update e delete sono loggati. *BFH* critica che al numero 2.10.5 si parla di indicazioni minime, mentre nei numeri 2.10.5.1 – 2.10.5.3 si utilizzano degli esempi ed «etc.». Chiede un elenco preciso degli attributi che come minimo devono essere ripresi nel protocollo. *Posta* chiede lo stralcio del numero 2.10.5.3 perché secondo lei è inattuabile.

2.10.6: *Tessaris* propone la seguente aggiunta al numero 2.10.6 vor: «Die Protokolldaten sind 10 Jahre, und im Falle einer längeren Dauer der Aufbewahrung von Daten im elektronischen Patientenregister bis zur Löschung der betreffenden Daten, aufzubewahren». Per motivi di maggiore chiarezza, *privatim* chiede di scrivere che i dati verbalizzati devono essere distrutti al termine di un periodo di 10 anni e di valutare una modifica redazionale in questo senso.

2.11 Collegamento del NIP con documenti (cpv. 3)

OFAC chiede come si possa ricostruire una cartella completa se non si memorizza il collegamento del NIP con i documenti e perché l'impiego del NIP è vietato nei sistemi primari. *Privatim* rinvia alle sue osservazioni generali sull'OCIP. Il Cantone *ZH* nonché *K3* e *VZK* scrivono che il divieto di collegare il NIP con i documenti non è attuabile. L'attribuzione di un caso interno avviene una volta sola, poi bisogna garantire di poter utilizzare sempre tale attribuzione. Il Cantone *ZH* aggiunge che una comunità non è in grado di garantire che il NIP non venga utilizzato nei sistemi primari. Il termine «persistent» deve essere sostituito da «dauerhaft». A tale richiesta si associano anche *K3*, *VZK* e *SBC.* In generale, il Cantone *ZH* chiede di riformulare o stralciare il numero 2.11.1. *SUVA* osserva che le comunità non possono assumere la responsabilità per le strutture aderenti e che quindi il numero 2.11.1 deve essere stralciato. Anche *SBC* e *BINT* chiedono lo stralcio. *BINT* aggiunge che le comunità devono assicurare che i sistemi primari non utilizzino i NIP attribuiti dall'UCC, ma fa notare che le comunità non sono in grado di farlo. Scrive inoltre che il requisito di questo numero deve essere precisato e chiede cosa bisogna mettere nei contratti, cosa viene controllato, da chi e che ne è della responsabilità civile. Dall'argomentazione separata sul NIP nella cartella informatizzata del paziente risulta inoltre la necessità di invertire la prescrizione: «Die PID ist in den Metadaten von Dokumenten persistent vorzuhalten», richiesta alla quale si associazione anche *Integic* e *Bleuer*. I Cantoni *GE*, *FR*, *VS*, *VD* e *JU* segnalano che la

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

comunità non può garantire il contenuto dei sistemi primari. Se un medico conserva il NIP con i documenti medici, la comunità non può saperlo. Essa può invece emettere delle raccomandazioni. Il termine «lieux de stockage» non è inoltre chiaro. Il MPI potrebbe trovarsi nello stesso luogo di archiviazione (data center) dei documenti, ma esserne separato fisicamente. È opportuno chiarire il numero 2.11.1, ma in termini di economicità non vi è nessun vantaggio a generare un NIP e non poterlo poi impiegare per identificare chiaramente un paziente.

A parere di *IG eHealth*, per rispettare il testo dell'ordinanza è fondamentale che le comunità debbano garantire che il NIP dell'UCC non sia memorizzato permanentemente nei luoghi di archiviazione o nei registri di documenti. Si oppone decisamente alla richiesta di mantenere in modo duraturo il NIP nei metadati. Se il NIP viene apposto su tutti i documenti, nel caso di un cambiamento voluto o necessario del nuemro, si perderebbero tutti i riferimenti, cioè un documento non potrebbe più essere collegato in modo univoco a un paziente in caso di cambiamento del NIP. Ciò risulta problematico dal punto di vista della protezione dei dati. Il metodo di collegare i documenti attraverso il MPI e chiavi locali è certo più complesso, ma consente il trattamento separato dei documenti, perché su ogni documento appare il nome e la data di nascita del paziente. *HIN* critica che in particolare la seconda parte del numero 2.11.1 è tecnicamente irrealizzabile. Il numero può essere in fondo copiato mediante memorizzazione intermedia / screenshot e poi inserito nel sistema primario. Bisogna inoltre rilevare l'apparente contraddizione con l'immagine 2 nell'allegato 5, «Nationale Anpassungen der Integrationsprofile». *HIN* vuole una menzione specifica che questi requisiti devono essere risolti soprattutto a livello organizzativo.

3. Portale di accesso per i professionisti della salute (art. 10 OCIP)

6 Cantoni[104] osservano che il grado di dettaglio menzionato al numero 3 corrisponde più a delle specifiche funzionali («come») piuttosto che a requisiti che dovrebbero essere contenuti in un'ordinanza («cosa»).

3.1 Conformità con le disposizioni di legge

ZAD, *K3*, *VZK* nonché i Cantoni *ZH* e *ZG* osservano che il portale di accesso deve essere conforme alle CTO. Nelle CTO non si può esigere che il portale di accesso debba rispettare le relative esigenze legali, poiché queste si applicano in ogni caso. Nessun servizio di certificazione è inoltre in grado di confermare che il portale di accesso rispetti tutte le esigenze legali. *VAKA* considera la prescrizione al numero 3.1.1 puramente declaratoria e per di più dà un'impressione di impotenza. 7 partecipanti[105] chiedono lo stralcio del numero 3.1.1, anche se *medshare* potrebbe accontentarsi di una menzione specifica dei requisiti. Secondo *privatim* lo scopo di tale disposizione non è chiaro. Se la si vuole rendere utile bisogna indicare quali requisiti legali deve rispettare in particolare il portale di accesso (non un elenco esaustivo).

3.2 Presentazione

Per *K3*, *VZK*, *ZAD* nonché i Cantoni *ZH* e *ZG,* le disposizioni del numero 3.2 non sono necessarie e dovrebbero essere stralciate. 8 partecipanti[106] rilevano che al numero 3.2.1.1 è stata dimenticata la parola «Gesundheitsfachperson» e che bisogna quindi aggiungerla: «ob ein Dokument durch eine Gesundheitsfachperson oder durch […]». Anche SQS osserva che la frase è incompleta e va quindi rettificata.

VAKA s'informa come bisogna interpretare la richiesta contenuta al numero 3.2.1.2, in particolare anche nell'ambito del personale ausiliario, e se questo agisce a nome dei professionisti della salute primari / da quali dipendono. Questa fattispecie deve essere chiarita con spiegazioni precise. Alla stessa stregua, *Posta* chiede come bisogna contrassegnare i dati pubblicati personalmente e se basta l'indicazione

[104] FR, NE, GE, VS, VD, JU
[105] ZG, ZH, ZAD, K3, VZK, VAKA, medshare
[106] CMC, BüAeV, GAeSO, KAeG SG, HIN, Medgate, privatim, pharmaSuisse

dell'autore. A riguardo affiora l'interrogativo di come interpretare «selbst» quando è coinvolto il personale ausiliario o altri membri dello stesso gruppo. Il punto deve essere concretizzato indicando che il personale ausiliario deve agire a nome del medico.

CDS e 9 Cantoni[107] segnalano a proposito del numero 3.2.1.3 che nel diritto di esecuzione e nel suo rapporto esplicativo affiorano termini e concetti come «Vernichtung», «Löschung» e «Annullierung» in riferimento ai dati della cartella informatizzata del paziente e si chiedono come distinguere tecnicamente tali concetti. CDS e 8 Cantoni[108] propongono di riprendere i concetti nelle spiegazioni e di differenziarli così da poterli impiegare in modo coerente. Anche il paziente dovrebbe capire qual è la differenza fra un documento annullato e uno cancellato. *SBC* chiede dal canto suo cosa significhi «annuliert» e desidera una spiegazione. Secondo *Posta* si dovrebbe chiarire se sia necessario mostrare al paziente i documenti annullati o se non sia sufficiente indicare la cancellazione nella history / nel log.

In riferimento ai numeri 3.2.1.3 e 3.2.1.4, *VGIch* scrive che per ogni documento si deve garantire un versionamento e che si parla di documenti «validi» e «annullati». Inoltre, secondo i «metadati», un documento può avere uno status di disponibilità «approvato» e «rifiutato». La terminologia deve essere chiarita ed eventualmente semplificata per consentire una migliore comprensione. *VAKA* osserva riguardo al numero 3.2.1.4 che il versionamento finisce in pratica per dar adito a confusione e chiede se sia necessario metterlo a disposizione del paziente. Propone di fornire al paziente solo la versione più attuale. Sulla stessa falsariga, *Posta* chiede se non sia più facile mostrare al paziente solo la versione più aggiornata e avanza una proposta in tal senso.

3.3 Assenza di barriere

VAKA è molto favorevole all'assenza di barriere. Poiché però essa genera già costi elevati per la realizzazione, diventerebbe ancora più onerosa se dovesse essere anche certificata. Le comunità e le comunità di riferimento provvederanno in ogni caso a rendere accessibili i portali di accesso. Questo requisito deve essere stralciato dalle CTO. Secondo *KSSG*, questo articolo esige che il portale di accesso e di conseguenza anche l'integrazione nei sistemi primari debbano essere accessibili. Implicitamente ciò significherebbe, per esempio, che tutto il SIC debba essere accessibile. Si chiede lo stralcio del numero 3.3 nel contesto del portale di accesso per i professionisti della salute. *SBV* critica che l'articolo si riferisce solo all'accessibilità del web e chiede che ne è delle applicazioni e se queste sono prese in considerazione nei documenti. Anche qui è necessario definire i requisiti dell'assenza di barriere. I Cantoni *ZG* e *ZH* considerano inutili le disposizioni sull'assenza di barriere e ne chiedono lo stralcio. I Cantoni *GE*, *VS*, *VD*, *JU* e *NE* segnalano che esistono professionisti della salute anziani che sanno utilizzare bene gli strumenti informatici, mentre medici più giovani sono talvolta molto reticenti a impiegarli. Chiedono poi di quali handicap si tratti: disturbi della vista o disabilità psichiche? Chiedono lo stralcio del numero 3.3.1.1. 6 Cantoni[109] aggiungono in riferimento al numero 3.3.1.2 che questa precisazione si riferisce a una norma che potrebbe evolvere e che non dovrebbe trovarsi in questa forma in un quadro legislativo vincolante. Mentre i Cantoni *GE*, *VS*, *VD*, *JU* e *NE* preferiscono stralciarlo, il Cantone *FR* è favorevole a una semplificazione. SQS ribadisce per il numero 3.3.1.2 l'osservazione fatta al numero 2.9.4 e chiede di completarlo con una disposizione sulla prova della verifica tecnica dei requisiti tecnici. Secondo *SBV* il livello di conformità AA di cui al numero 3.3.1.2 è insufficiente per i disabili della vista. Si devono soddisfare le condizioni di conformità stabilite nelle WCAG 2.0 e raggiungere il livello di conformità AAA.

3.4 Formati di dati: messa a disposizione

Secondo *K3*, *VZK*, *ZAD* nonché i Cantoni *ZG e ZH,* le disposizioni di cui al numero 3.4 non sono necessarie e devono quindi essere stralciate. Secondo *SCH* non è noto a priori quale tipo di formati il paziente o il fornitore di prestazioni intende memorizzare nella cartella informatizzata del paziente attraverso il

[107] BL, GL, LU, OW, UR, FR, NW, SZ, TG
[108] BL, GL, LU, OW, UR, FR, NW, SZ
[109] FR, NE, GE, VS, VD, JU

portale. In particolare non si può escludere che il paziente o il fornitore di prestazioni voglia utilizzare formati proprietari per i quali non sono disponibili dei programmi di conversione o esistono solo programmi con una conversione parziale. A ciò si aggiunge che la conversione in uno dei formati ammessi rappresenta un trattamento dei dati ai sensi della LPD. *Bleuer* segnala che è l'allegato 4 (e non il 3) a definire i formati di scambio, cosa da rettificare al numero 3.4.1.1.

A parere di 6 Cantoni[110], per motivi d'integrità dei dati è pericoloso che il portale converta un file fonte. È responsabilità dei professionisti della salute fornire il formato giusto. Ciò implicherebbe che il portale di accesso debba essere in grado di leggere tutta una serie di formati. Chiedono di stralciare il numero 3.4.1.2. *Bleuer* ricorda che in seguito alla conversione potrebbero affiorare errori che modificano il senso del testo e chiedono quindi di conservare sempre anche i formati originali. Se si lasciano i documenti nel formato originale diventa problematico limitare i formati a quelli ammessi. In ogni caso bisognerebbe ammettere tutti i formati usuali, fra cui in particolare ZIP e ISO. Il partecipante propone la seguente formulazione del numero 3.4.1.2: «[…] in eines der in Anhang 4 aufgeführten Formate umwandeln. Dokumente sind bei Umwandlung zusätzlich im Originalformat vorzuhalten». Analogamente, *BINT* e *Integic* chiedono che in caso di conversione si debbano archiviare i file anche nel formato originale. Ciò significa l'ammissione di oggetti anche come bitstream. *SUVA* osserva che la conversione non è compatibile con la sicurezza di revisione e si dichiara favorevole a lasciare i file nel formato originale. *Posta* chiede perché è necessario convertire anche formati usuali e chi si assume la responsabilità nel caso in cui la conversione automatica provochi una perdita di informazioni che possa condurre a un errore terapeutico. *K3* e *VZK* ritengono necessario vietare la conversione durante l'upload, perché durante la conversione si potrebbero falsificare dei contenuti, con una conseguente violazione dell'integrità dei dati. Il risultato sfuggirebbe al controllo dell'autore e il documento presenterebbe un contenuto diverso. La disposizione dovrebbe quindi essere modificata in modo da non consentire la conversione durante l'upload. Non si dovrebbero poter convertire i documenti e quindi il requisito deve essere stralciato. In riferimento al numero 3.4.1.2, *Integic* chiede inoltre quali modalità di conversione siano previste e come si debba gestire il caricamento di dati provenienti da fitness tracker o da applicazioni. Secondo *HIN* dovrebbe essere nell'interesse dei produttori di sistemi primari offrire le apposite possibilità di conversione. Il portale dovrebbe autorizzare solo determinati tipi di dati. Si chiede la seguente riformulazione del numero 3.4.1.2: «Dateien der im Anhang 3 definierten Formate entgegennehmen. Dateien in anderen Formaten müssen entweder automatisiert umgewandelt oder abgewiesen werden». Per precisare il numero 3.4.1.2, *medshare* desidera la seguente aggiunta: «[…] in ein gemäss 3.4.1.1 zugelassenes Format umwandeln».

3.5 Formati di dati: consultazione

K3, *VZK*, *ZAD* nonché i Cantoni *ZG e ZH* considerano superflue le disposizioni di cui al numero 3.5 e chiedono pertanto di stralciarle. *Posta* vuole sapere perché alcuni tipi di documenti correnti come Word, non sono supportati.

3.5.1: Riguardo al numero 3.5.1.2, *privatim* rimanda alle spiegazioni fornite nel quadro delle osservazioni generali sull'OCIP. *SBC* segnala che il «bulk download» consente una lacuna di sicurezza e che il numero 3.5.1.3 deve quindi essere stralciato. *Integic* chiede se in caso di «bulk download» l'utente sia tenuto a inserire una verifica per ogni documento o se debba farlo una sola volta in blocco. Il punto dovrebbe essere chiarito o completato. In riferimento al numero 3.5.1.5, *BINT*, *Integic* e *IG eHealth* evidenziano che il concetto di umanamente leggibile non è un problema di scaricamento ma di presentazione. Chiedono se non s'intenda piuttosto un «rendering» a livello di server. In tal caso il punto dovrebbe essere esplicitato. Anche *SUVA* desidera una precisazione del concetto di «menschenlesbar». A parere di *KSSG* non si può partire dal presupposto che il portale sappia gestire ogni tipo di dati strutturati, ma solo i formati di scambio indicati nell'allegato 4 dell'OCIP-DFI. Il numero 3.5.1.5 dovrebbe essere adeguato in modo da consentire solo i formati di scambio previsti nell'allegato 4 dell'OCIP-DFI. 6 Cantoni[111] vogliono stralciare il numero 3.5.1.1 e riformulare i numeri, 3.5.1.2, 3.5.1.3 e 3.5.1.5 come

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

segue: «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 sottolinea in riferimento al «bulk download» di cui al numero 3.5.1.3 che una gran parte dei dati relativi al paziente esce dalla comunità e sfugge a qualsiasi controllo. Tale disposizione è inoltre in totale contraddizione con il concetto di «Patient Empowerment».

3.5.2: *Medshare* segnala che la parola «erlaubte» presenta un errore di battuta. *K3* e *VZK* lamentano la scarsa precisione della redazione. Sulla stessa falsariga, *SQS* domanda chi definisce i limiti massimi ammissibili e chiede di precisare le competenze per la definizione dei limiti massimi ammissibili. Secondo *Integic*, *BINT* e *IG eHealth*, non è ammissibile fissare un limite assoluto. Si dovrebbe avere la possibilità di riconoscere e consultare semplicemente altri documenti disponibili. Per *Posta* l'argomentazione a favore dei «rate limit» non è comprensibile. Il paziente ha deciso che il professionista della salute ha accesso alla cartella informatizzata del paziente. Un limite artificiale non sembra quindi adeguato. A parere di *Bleuer* vi è il rischio che i documenti vengano consultati in modo incompleto. Il numero 3.5.2 deve quindi essere stralciato. Anche *SUVA* è a favore dello stralcio e ricorda che tale disposizione comporterebbe un'incompletezza dei dati del paziente. In caso di dati aggiunti personalmente dal paziente, questa disposizione significherebbe un'ingerenza nella sua sfera privata perché il paziente non avrebbe la possibilità di trasmettere i dati desiderati. *HIN* ritiene che i rate limit dovrebbero (poter) essere definiti dalle comunità. Il numero 3.5.2 dovrebbe essere completato come segue: «[…] auslösen. Die rate limits werden von den Gemeinschaften definiert».

4. Protezione e sicurezza dei dati (art. 11 OCIP)

ISSS vuole un nuovo numero 4.25 per garantire che i dati del paziente, dopo la distruzione, non rimangano archiviati per sempre. Chiede il seguente testo: «4.25 Datensicherung (Backups): Datensicherungen sind spätestens nach 2 Jahren zu vernichten, sofern keine gesetzlichen oder regulatorischen Anforderungen etwas Anderes verlangen. Im Falle belegbar betrieblicher Notwendigkeit kann diese Dauer auf maximal 3 Jahre ausgedehnt werden». SQS segnala che tutto il numero 4 contiene gran parte degli elementi della norma ISO/IEC 27001:2013 e dei Controlli dell'allegato A. Sarebbe più opportuno rinviare all'ISO/IEC 27001:2013 incl. allegato A e descrivere solo gli elementi aggiuntivi specifici per l'OCIP. Un elemento di questo tipo potrebbe essere la notifica all'UFSP degli eventi rilevanti per la sicurezza. Nell'allegato s'impiegano inoltre dei termini non corrispondenti all'ISO/IEC 27001:2013. Concretamente si propone la separazione degli elementi contenuti nella norma ISO/IEC 27001:2013 e nei Controlli dell'allegato A dalle aggiunte specifiche per l'OCIP nonché l'impiego della terminologia dell'ISO/IEC 27001:2013. *FMH* afferma che nell'ambito della protezione dei dati ci si debba riferire alle norme e alle good practice in vigore e non elaborare nuove disposizioni. Come *SSIM* anche *FMH* chiede di riformulare tutto il numero 4. A parere di *Tessaris*, le onerose condizioni tecniche e organizzative previste nel numero 4, non potranno essere interamente sostenute da una comunità con risorse di personale e di mezzi limitate, come un ambulatorio con un solo medico o un piccolo ambulatorio collettivo che desidera introdurre e gestire la cartella informatizzata del paziente. Queste piccole strutture dovranno pertanto ricorrere a terzi («organizzazioni di esercizio»). Se tali organizzazioni forniscono prestazioni per le comunità, dovrebbero anche soddisfare i requisiti di cui all'articolo 11 OCIP e al numero 4, altrimenti vi sarebbe una lacuna nel dispositivo di garanzia della protezione e della sicurezza dei dati.

4.1 Requisiti per terzi

Privatim approva questa regolamentazione per motivi di protezione dei dati. Sebbene tali aspetti siano già disciplinati nelle LPD cantonali e federali, ai fini di una maggiore chiarezza e completezza è opportuno riprenderli nelle CTO.

4.2 Responsabile della protezione e della sicurezza dei dati (cpv. 1)

4.2.1: *HIN* si rallegra che la norma ISO 27001 sia menzionata in modo esplicito. *SQS* segnala che

l'ISO/IEC 27001:2013 non descrive un sistema di gestione della protezione e sicurezza dei dati, ma un Information Security Management System (ISMS). Il sistema di gestione della protezione e sicurezza dei dati dovrebbe basarsi sulla norma ISO/IEC 27001 o soddisfarla. Più adatte alla descrizione di un sistema di gestione della protezione e sicurezza dei dati sono invece le «Direttive del 14 giugno 2014 sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere» rilasciate dall'IFPDT (Direttive sulla certificazione dell'organizzazione e della procedura), che vengono applicate in caso di certificazione ai sensi dell'articolo 11 LPD. *SQS* propone le seguenti due varianti per il numero 4.2.1: «Gemeinschaften müssen ein Informations- und Managementsystem betreiben, wie in der Norm ISO/IEC 27001:2013 beschrieben wird, das: […]» und «Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben, wie in den Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 14. Juni 2014 des EDÖB beschrieben wird, das: […]». I Cantoni *ZH e ZG*, *ZAD*, *K3* e *VZK* considerano il numero 4.2.1 non opportuno e ne chiedono lo stralcio. OFAC scrive che i sistemi di gestione della protezione dei dati (SGPD) e i sistemi di gestione della sicurezza dell'informazione (SGSI) funzionano perfettamente insieme, ma non devono essere confusi. Entrambi i sistemi dovrebbero essere gestiti separatamente. Alla stessa stregua di *SQS,* segnala inoltre che la norma ISO/IEC 27001:2013 non definisce i sistemi di gestione della protezione dei dati e quindi la frase dovrebbe essere riformulata.

4.2.2 / 4.2.3: *ISSS* afferma che attraverso i numeri 4.2.2.3.1 – 4.2.2.3.3 e 4.2.2.3.5 si dovrebbero richiedere esplicitamente anche i componenti per le discipline specifiche dell'ICT, come ad esempio la sicurezza contro gli attacchi, contro le interruzioni dell'esercizio e il backup dei sistemi e dei dati. Ciò aumenterebbe la consapevolezza e fungerebbe da base per i Management Review / audit / certificazioni. Ai suddetti numeri propone le seguenti aggiunte: numero 4.2.2.3.1: «Hardware (Inventar der Datenspeicher, Server, Backup-Systeme, Sicherheitsfunktionen); numero 4.2.2.3.2: Software (Inventar von Betriebs- und EPD-Anwendungssystem, Endpoint Protection, Backup, Monitoring, Update- und Patch-Management); numero 4.2.2.3.3: Datenbestände (Beschreibung zu Datenhaltung, Datenorganisation, Datensicherheit, Berechtigungen); numero 4.2.2.3.5: Prozesse (zu Datenschutz- und Datensicherheitsmanagementsystem, insbesondere auch zu Ausfallszenarien, Recovery, Tests, Audits, Verantwortlichkeiten). Riguardo al numero 4.2.2.3, *Posta* chiede se l'inventario comprende tutti i sistemi primari collegati o se nella fattispecie si tratta solo dei componenti centrali. Desidera che il campo di applicazione delle CTO venga definito in modo chiaro. SQS critica che le disposizioni di cui ai numeri 4.2.2 e 4.2.3 non collimano con quelle dell'articolo 11 OCIP. O si deve completare l'articolo 11 OCIP o adeguare i due numeri. In riferimento al numero 4.2.2.3, *SQS* ritiene che nell'ISO/IEC 27001:2013 l'inventario non riguardi solo gli strumenti di esercizio. La norma parla di asset / valori dell'organizzazione, fra cui rientrano per esempio i collaboratori. L'organizzazione strutturale non è definita in modo abbastanza esauriente. Si propone pertanto il seguente testo: «Ein aktuelles Inventar der folgenden Werte der Organisation». Anche il numero 4.2.3 deve essere modificato di conseguenza: «[…] an den Werten der Organisation sind zu […]».

4.3 Responsabile della protezione e della sicurezza dei dati (cpv. 1 lett. a)

20 partecipanti[112] chiedono di rinunciare alla designazione di un responsabile della protezione e della sicurezza dei dati. 14 partecipanti[113] aggiungono che tale responsabile non aumenta la sicurezza. I costi per la creazione di una funzione di questo tipo sono inoltre molto elevati. *ZAD*, *CDS* e 8 Cantoni[114] evidenziano che le CTO non coincidono con le spiegazioni sull'articolo 11 OCIP, dove si parla di un responsabile indipendente dal punto di vista tecnico e organizzativo. Il Cantone *AR* ritiene che, in caso di sufficiente capacità, questa funzione potrebbe essere affidata al responsabile della protezione dei dati, evitando di dover assumere un'altra persona. 6 partecipanti[115] vogliono lo stralcio del numero 4.3.

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

In riferimento al numero 4.3.1.1, il Cantone *SZ* considera inopportuno che i responsabili della protezione e della sicurezza dei dati debbano esercitare la loro funzione in modo indipendente. Alla stessa stregua di *K3*, *VZK*, del Cantone *ZG* e di *ZAD*, il Cantone *SZ* chiede inoltre che cosa s'intenda di preciso. Per *privatim* sarebbe auspicabile che al numero 4.3.1 si aggiungesse un altro punto che esiga per il responsabile della protezione e della sicurezza dei dati di disporre delle conoscenze tecniche necessarie. Al numero 4.3.1.2 si dovrebbe inoltre precisare che per risorse s'intendono sia quelle in termini di tempo che di finanze. *VGIch* considera il numero 4.3.1.2 troppo poco specifico e chiede una precisazione mediante criteri chiari. *Medshare* desidera completare il numero nel modo seguente: «[…] erforderlichen Ressourcen und Entscheidungskompetenzen verfügt», mentre il Cantone *BS* preferisce la seguente redazione: «[…] erforderlichen Kompetenzen und Ressourcen verfügt».

4.4 Monitoraggio di incidenti di sicurezza (cpv. 1 lett. b)

KSSG osserva che la creazione di un Security Information and Event Management System (SIEM) è molto onerosa e praticamente impossibile da realizzare entro i 3 anni di periodo di transizione. Il numero 4.4 deve essere reso più flessibile oppure si devono prolungare le scadenze. A parere di *VGIch*, il SIEM deve limitarsi a quelle parti tecniche e organizzative dell'infrastruttura di una comunità intese a mettere a disposizione la cartella informatizzata del paziente, e non deve essere applicato alle estensioni (separate logicamente) destinate a fornire una comunicazione orientata né all'infrastruttura e organizzazione delle strutture aderenti. 6 Cantoni[116] dichiarano che un SIEM non può essere applicato ai sistemi primari dei professionisti della salute e desiderano dunque la seguente aggiunta al numero 4.4.1.1: «[…] de la communauté à l'exclusion des système primaires, qui détecte […]». Secondo *ISSS* si dovrebbe prevedere, ai fini dell'applicazione pratica, che le persone incaricate debbano assolvere una formazione, un corso o certificato. Il numero 4.4.1.3 deve pertanto essere completato come segue: «[…] adressiert werden. Speziell sind mittels Sensibilisierungsmassnahmen, Schulungen oder Erfahrungsaustausch mit anderen Verantwortlichen die beauftragten Personen innerhalb der Gemeinschaft angemessen und wiederkehrend zu unterstützen».

Posta critica che il numero 4.4.2.2 è formulato in modo molto vago. Per una comunità e anche per chi effettua un audit è infatti difficile valutare cosa sia inusuale o meno. Non è inoltre chiaro cosa sia una mutazione critica secondo il numero 4.4.2.3. Entrambi i numeri dovrebbero essere concretizzati.

4.5 Gestione degli incidenti di sicurezza (cpv. 1 lett. b)

VAKA, *K3 e VZK* chiedono quale sia la differenza fra una procedura formale e una normale. *Medshare* segnala che al numero 4.5.1.1 manca il rinvio all'OCIP e che bisogna quindi inserirlo. *FMH* e *SSIM* auspicano una precisazione del numero 4.5.1.1, perché non ha senso notificare tutto. In questo punto *Posta* lamenta la mancanza di una descrizione precisa del campo di applicazione e chiede di colmare questa lacuna. *ISSS* propone la seguente riformulazione del numero 4.5.1.1 per motivi di conformità con il Regolamento generale sulla protezione dei dati dell'UE (UE-RGPD): «formale Verfahren für das Melden von Datenschutz- und Datensicherheitsereignissen an die betroffenen Patientinnen / Patienten gemäss Ziffer 4.13 definiert haben». *SQS* considera che non sia competenza né compito di un servizio di certificazione, ricevere notifiche di eventi relativi alla protezione e sicurezza dei dati e controllarne la soluzione. Nel numero 4.5.1.1 si dovrebbe pertanto cancellare il servizio di certificazione come livello di escalation. *Medshare* desidera che il numero 4.5.2.2.1 venga precisato come segue: «[…] Sperren des Zugangspunktes und Zugangsportals der Gemeinschaft […]».

4.6 Protezione da software maligni (cpv. 1 lett. b)

ZAD e i Cantoni *NW*, *TI* e *ZH* criticano che la disposizione di cui al numero 4.6 è troppo dettagliata. Dovrebbe essere stralciata e sostituita da principi generali e astratti da inserire nell'OCIP. Sul numero 4.6.1.1 *Posta* ripete la richiesta avanzata al numero 4.5.1.1.

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

4.7 Gestione delle lacune di sicurezza (cpv. 1 lett. b)

I Cantoni *NW* e *ZH* nonché *ZAD* ribadiscono il parere espresso sul numero 4.6. A differenza del commento fatto al numero 4.6, *ZAD* propone però una semplificazione invece dello stralcio. Accanto ai Cantoni *NW* e *ZH,* anche *K3* e *VZK* sono a favore dello stralcio del numero 4.7. Essi affermano che la disposizione è corretta nel principio, ma che è troppo dettagliata. *ISSS* vuole dei numeri supplementari con la seguente redazione: «4.7.4 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens vierteljährlich automatisierte Schwachstellen-Scans durchführen» e «4.7.5 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens jährlich einen Penetration-Test durch einen unabhängigen Anbieter durchführen lassen». *VAKA* caldeggia la proposta di cui al numero 4.7, ma ritiene relativamente oneroso verificare in qualsiasi momento le lacune di tutti i software, anche perché spesso si tratta di software «closed source» le cui lacune di sicurezza di solito sono sconosciute.

4.8 Gestione dei dati e dei sistemi degni di protezione (art. 1 lett. c e d)

K3, *VZK*, *ZAD* nonché i Cantoni *NW* e *ZH* ritengono troppo dettagliata la disposizione e bassa la sua utilità pratica. Chiedono pertanto una semplificazione del numero 4.8.

4.8.1: 6 Cantoni[117] ricordano che ciò fa parte dell'obbligo di diligenza che i professionisti della salute devono osservare già oggi. *Bleuer* ritiene che non si possa definire a priori la rilevanza del trattamento. *VAKA* dichiara che la decisione di cui al numero 4.8.1 viene presa dai professionisti della salute e deve essere valutata ad hoc. *KSSG* chiede come sia possibile soddisfare tale prescrizione, se non esistono direttive sui dati rilevanti per il trattamento. Anche *BINT* e *Integic* si domandano come interpretare in questo contesto il termine «behandlungsrelevant» e ricordano che la sua interpretazione è soggetta a forti trasformazioni. Anche *SSIM* considera la definizione «behandlungsrelevant» troppo poco precisa e ne chiede una concretizzazione, come già espresso nel parere sul disegno di legge del 2011. Anche *VGIch* sostiene che non sia chiaro quali dati/documenti vengano considerati rilevanti per il trattamento. Mentre complessivamente 9 partecipanti[118] chiedono lo stralcio totale del numero 4.8.1, *Integic* e *KSSG* si accontenterebbero di una precisazione. *VGIch* propone che l'UFSP fornisca un template non vincolante in modo da favorire una best practice per la messa a disposizione dei documenti da parte degli ospedali. OFAC chiede come le comunità possano garantire qualcosa che riguarda le strutture sanitarie aderenti. Chi assicurerebbe il controllo sul lungo termine, come e con quale diritto? I compiti delle comunità sono descritti in modo esauriente all'articolo 10 LCIP. Le strutture sanitarie, indipendentemente dalla loro adesione, sono soggette al diritto svizzero sulla protezione dei dati. È inoltre opportuno notare che il diritto al quale sono soggette le strutture sanitarie dipende anche dalla loro forma giuridica.

4.8.2 – 4.8.4: *Posta* ribadisce il parere espresso al numero 4.5 anche in riferimento al numero 4.8.2. 6 Cantoni[119] chiedono un chiarimento, perché nella versione francese il termine «sensible» utilizzato al numero 4.8.2 non ha lo stesso senso che negli articoli 1 e 2 OCIP o nella LCIP. *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* osservano che qui viene utilizzato di nuovo il termine «schützenswerte Daten», senza aver fornito una definizione. Poiché ciò potrebbe causare delle incertezze giuridiche, chiedono di aggiungere una definizione legale. *Integic* desidera un chiarimento perché a suo parere il numero 4.8.3.8.1 implica che per ogni attore IHE debba essere utilizzato un certificato client. Riguardo allo stesso numero *KSSG* scrive che la memorizzazione del certificato TLS-Client non è sicura nell'inventario e che tali certificati dovrebbero invece essere conservati in un luogo protetto. Propone quindi o di stralciare il numero o di riformularlo. L'inventario dovrebbe contenere solo il nome del certificato client, ma non il certificato stesso. 6 Cantoni[120] ricordano che una comunità non può tenere un inventario con migliaia di sistemi primari, né fornire indicazioni sul certificato TLS installato su questi sistemi, e chiedono dunque di stralciare il numero 4.8.3.8. *SQS* critica che la frase al numero 4.8.4.3 non è comprensibile. Non si capisce

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

di quale conferma si tratti. È quindi necessaria una precisazione o una riformulazione. Per limitare il rischio di abusi, *ahdis* propone di precisare al numero 4.8.3.8.1 «die Serial ID, HASH des TLS-Clientzertifikats» al posto di «TLS-Clientzertifikat». Riguardo al sistema primario come attore IHE, OFAC critica che nell'elenco mancano le interfacce fra la comunità e il resto del mondo. Non è obbligatorio che il trasporto e lo scambio fra i sistemi primari e la comunità avvenga secondo il protocollo IHE. In generale tutte le interconnessioni fra la comunità e terzi dovrebbero far parte dell'inventario in qualità d'interfacce.

4.9 Requisiti in materia di protezione e sicurezza dei dati per le strutture sanitarie affiliate e i loro professionisti della salute nonché per i loro terminali (lett. e)

HIN si rallegra dei requisiti posti ai terminali. *SSIM* e *FMH* criticano che i requisiti previsti per le strutture sanitarie aderenti e i loro professionisti della salute violano la sovranità dei sistemi primari. Chiedono la revisione di tutta la sezione e in particolare lo stralcio dei numeri 4.9.1.2.3, 4.9.2 e 4.9.3. A parere di *VGIch,* il SIEM deve limitarsi a quelle parti tecniche e organizzative dell'infrastruttura di una comunità che servono a mettere a disposizione la cartella informatizzata del paziente, e non deve essere applicato alle estensioni (separate logicamente) destinate a fornire una comunicazione orientata né all'infrastruttura e organizzazione degli istituti aderenti. Un numero a sé stante dovrebbe prescrivere una separazione esplicita. OFAC osserva che le comunità non possono garantire qualcosa che riguarda le strutture aderenti, di cui non sono né proprietarie né responsabili. Il ruolo della comunità nei confronti delle strutture aderenti si limita a descrivere i requisiti tecnici e organizzativi delle loro interfacce.

4.9.2 / 4.9.3: Terminali sicuri per i professionisti della salute: *BINT* scrive che attraverso il numero 4.9.2 la responsabilità viene trasferita agli aderenti, cosa di per sé accettabile. Questo requisito non può essere però né imposto né sanzionato, oltre a superare l'ambito di competenza della LCIP, e va quindi stralciato. *ISSS* preferirebbe un testo corredato di una lista di esempi e propone quindi la seguente formulazione: «[…] Endgeräte sicherzustellen (z.B. auch speziell eingeschränkt für Internet-Nutzung, Visual- oder Audio-Aufnahmen, Datentransfers, Synchronisationen), die von den Gesundheitsfachpersonen […]».*Posta* osserva in riferimento ai numeri 4.9.2 e 4.9.3 che le comunità non possono controllare né validare i singoli computer collegati. Questo requisito non è realizzabile; le comunità devono definire i requisiti di sicurezza per gli utenti nelle loro condizioni generali. *Integic* dichiara quanto segue nel suo commento sul numero 4.9.3: «Personenspezifische Benutzer und definitives Verbot / Verweigerung von Sammel- oder Gruppenbenutzerzugängen» e chiede di completare il numero in questo senso. A parere di *VGIch,* il numero 4.9.3 costituisce un'ingerenza nelle competenze di esercizio degli ospedali e deve quindi essere stralciato. È infatti sufficiente un contratto fra comunità e struttura sanitaria. Per *K3*, *VZK*, *ZAD* e il Cantone *ZH* si tratta di punti scontati, che sono già rispettati nella pratica. Il numero 4.9.3 deve essere stralciato o altrimenti semplificato attraverso una disposizione generale e astratta da inserire nell'OCIP. *VAKA*, *K3* e *VZK* segnalano che un firewall non è un elemento sul terminale del professionista della salute e propongono di stralciare il testo in questione o di adeguare il titolo del capoverso. OFAC scrive che il rapporto fra comunità e strutture sanitarie aderenti è di natura meramente contrattuale. Se l'UFSP decide di assoggettare i professionisti della salute a disposizioni e norme severe sulla sicurezza dell'informazione e la protezione dei dati, ciò non dovrà avvenire attraverso la cartella informatizzata del paziente, perché nella LCIP non vi è una base legale a riguardo.

4.10 Requisiti in materia di protezione e sicurezza dei dati per il personale (cpv. 1 lett. f)

ZAD e i Cantoni *NW* e *ZH* ribadiscono il parere espresso sul numero 4.6, al quale si associano anche *K3* e *VZK* per il numero 4.10.

4.10.1: *ÄTG* e *HÄ CH* evidenziano che la protezione dei dati e una corretta gestione dei dati sensibili rappresentano già oggi un compito importante per i professionisti della salute. Nella realizzazione degli obiettivi previsti per le comunità è però importante fare in modo che le esigenze vengano raggiunte con buon senso, oculatezza e un onere tollerabile in termini di tempo e finanze (vantaggio marginale). *Posta* chiede se si tratta qui dell'esercizio dei sistemi della LCIP, come amministrazione, engineering, helpdesk, ecc. e desidera una concretizzazione.

4.10.2: In riferimento al numero 4.10.2.1, 6 Cantoni[121] sono del parere che le comunità non possano garantire che le persone siano competenti o assumano la loro responsabilità. Non spetta alla comunità accollarsi la responsabilità di valutare le conoscenze degli utenti. Questo numero deve essere stralciato. CDS e 6 Cantoni[122] considerano che il requisito di cui al numero 4.10.2.3 non possa essere applicato. L'obbligo contrattuale al segreto professionale per le persone che accedono ai dati della cartella informatizzata del paziente non è giuridicamente perseguibile come quello riservato ai medici. Altri 7 partecipanti[123] sono dello stesso avviso e aggiungono che il segreto professionale dei medici è disciplinato dal diritto federale ed eventualmente anche dal diritto cantonale. Né le comunità né le comunità di riferimento posseggono competenze regolamentari a riguardo. *K3*, *VZK* e *ZAD* vorrebbero chiarire in quale misura i collaboratori delle comunità e comunità di riferimento possano essere considerati personale ausiliario ai sensi dell'articolo 321 del codice penale svizzero (CP). Il Cantone *ZH* osserva a riguardo che i collaboratori delle comunità e comunità di riferimento non sono contemplati dall'articolo 321 CP e che senza un adeguamento del CP, il medico non sarebbe punibile solo se il paziente ha dato il consenso giuridicamente valido ai sensi dell'articolo 321 numero 2 CP. Sulla stessa falsariga, *SQS* chiede cosa s'intende per obbligo analogo al segreto professionale medico. Il segreto professionale del medico rientra nei segreti professionali dell'articolo 321 CP. La lista delle professioni interessate è esaustiva e riguarda, nel caso dei medici, solo i loro ausiliari, mentre gli operatori informatici non sono tenuti al segreto professionale medico. Il numero 4.10.2.3 deve essere precisato o riformulato come segue: «[…] erlangen könnten, müssen entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet sein. Die vertragliche Schweigepflicht muss alle Daten des Patientendossiers betreffen, welche im Rahmen der Berufsausübung den Personen bekannt werden und sie muss unbefristet über die Berufsausübung und über Ende des Auftrags hinaus gelten». *Tessaris* scrive a riguardo del 4.10.2.3 che le persone che non sono assoggettate al segreto professionale medico e di conseguenza non sono sanzionate in caso di sua violazione (p.es. impiegati di organizzazioni di esercizio secondo il numero 4.1.1) dovrebbero essere obbligate a mantenere la stretta confidenzialità con misure adeguate (obbligo di riservatezza scritto). Si propone pertanto la seguente redazione: «Personen, die Zugang zu Daten des Patientendossiers erhalten, müssen durch geeignete Massnahmen, insbesondere Unterzeichnung einer Vertraulichkeitsverpflichtung, zur Geheimhaltung der bei Ausübung ihrer Tätigkeit für die Gemeinschaft wahrgenommenen Informationen über Patientinnen oder Patienten angehalten werden». *ISSS* propone la seguente precisazione al numero 4.10.2.3: «[…] analogen Verpflichtungen (wie z.B. einer vertraglichen Geheimhaltungspflicht) unterliegen». Per il Cantone *AR* si dovrebbe chiarire e precisare al numero 4.10.2.3 quali persone sono contemplate, chi è competente e cosa significhi «bewusst» in questo contesto. Complessivamente 14 partecipanti[124] sono favorevoli allo stralcio del numero 4.10.2.3. *Tessaris* dichiara in riferimento al numero 4.10.2.4, che i requisiti sulla gestione del personale dovrebbero riguardare la protezione e la sicurezza dei dati e propone la seguente formulazione: «auf die Anforderungen an Datenschutz und Datensicherheit ausgerichtete Prozesse […]».

4.10.3: Per *SSIM* il numero 4.10.3 e i sottonumeri sono eccessivi e devono essere stralciati. Il Cantone *ZH* ribadisce il parere espresso sui numeri 4.6 e 4.10. *Posta* desidera che al numero 4.10.3 si inserisca un rinvio preciso ad altre leggi in modo da poter consultare le prescrizioni concrete. *IG eHealth* si chiede se non venga violato il principio dell'uguaglianza giuridica quando sul piano federale si richiede un tale livello di protezione, mentre su scala cantonale il livello di protezione per il trattamento degli stessi dati medici è nettamente inferiore. Consiglia pertanto di armonizzare il punto con i requisiti cantonali. Secondo il Cantone *BS* i numeri 4.10.3.1 e 4.10.3.2 dovrebbero essere precisati, per chiarire che i professionisti della salute non rientrano nella «Liste der Schlüsselpersonen» e non devono essere sottoposti a un controllo di sicurezza relativo alle persone (CSP) ai sensi della legge militare. Il controllo di sicurezza relativo alle persone previsto nella legge militare dovrebbe invece essere eseguito dalle comunità di riferimento senza grosse difficoltà. Propone la seguente aggiunta al numero 4.10.3.1: «[…] Liste aller

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

Personen, welche keine Gesundheitsfachperson nach articolo 2 lettera b LCIP sind, führen, die […]». *Privatim* considera la disposizione del numero 4.10.3.1 opportuna nell'ottica della protezione dei dati, ma poco chiara riguardo alle persone che tale elenco deve comprendere. Nella categoria delle persone chiave non possono certo rientrare tutti i professionisti della salute autorizzati ad accedere alla cartella informatizzata del paziente. La disposizione deve pertanto essere precisata. 6 Cantoni[125] chiedono un chiarimento del numero 4.10.3.1 mediante esempi concreti.

A parere di 15 partecipanti[126] non è comprensibile come una comunità o comunità di riferimento possa effettuare un «PSP nach Militärgesetz». 6 partecipanti[127] aggiungono che anche in termini di contenuto non è opportuno esigere tale controllo. *Insel*, *Integic* e *KSSG* criticano che questa esigenza è sproporzionata rispetto ad altri istituti, mentre *STSAG* definisce eccessivamente oneroso quanto prescritto al numero 4.10.2.3. *Bleuer* dichiara a riguardo che tale esigenza costituisce un'ingerenza eccessiva nei diritti della personalità dei lavoratori interessati e dubita dell'esistenza di una base giuridica o della legalità di tale disposizione, opinione che sottoscrive anche *Integic*. *SQS* afferma che per un CSP è necessaria una base legale, anche perché i risultati devono essere comunicati a destinatari specifici definiti in leggi speciali. Manca una sufficiente base legale per questa disposizione, ossia secondo il principio di legalità non basta richiedere tale prova in un allegato di un'ordinanza di un dipartimento. *SUVA* segnala che il CSP non è previsto né nella legge militare né nell'ordinanza sul CSP (OCSP). Ci si chiede quale legittimità legale possa avere un controllo così severo e se non sia un'esigenza eccessiva. Una tale disposizione non è più compatibile con il diritto oggi in vigore e neanche necessaria viste le possibilità offerte dal diritto in materia di protezione dei dati. Anche *SCH* critica il carattere sproporzionato della disposizione e ritiene che spetti alle comunità d'interesse fare raccomandazioni sul controllo dell'integrità delle persone che accedono ai dati del paziente. *Tessaris* afferma che il CSP previsto nella legge militare e nella legge federale sulle misure per la salvaguardia della sicurezza interna (LSMI) non può essere applicato alle persone chiave secondo la LCIP. In base a tali leggi, il CSP presuppone la consultazione del casellario giudiziale e la rilevazione di dati sulla sfera privata della persona controllata, quindi un'ingerenza nei diritti fondamentali che deve essere giustificata da una legge formale. *KSSG* osserva che l'applicazione di tale requisito entro la scadenza prevista di 3 anni è irrealistica. *BINT* critica che il CSP impedirebbe l'impiego di lavoratori stranieri. *VGIch* ritiene che il numero 4.10.3.2 sia eccessivo e violi la parità di trattamento con i professionisti della salute. Tale condizione infrange inoltre formalmente e materialmente i principi legali in vigore.

Complessivamente 26 partecipanti[128] chiedono lo stralcio del numero 4.10.3.2. 6 Cantoni[129] ritengono che l'OCSP non sia adeguata in questo contesto. Come alternativa, *SCH* propone il seguente testo: «diese Personen eine adäquate Integritätsprüfung durchlaufen haben», mentre *Tessaris* potrebbe accettare che si constati se queste persone sono state sottoposte a un CSP ai sensi della legislazione federale o cantonale o eventualmente che si richieda lo svolgimento di un CSP. *VAKA* desidera una riformulazione del numero 4.10.3.2. Il Cantone *BS* propone la seguente aggiunta al numero in questione: «[…] PSP in Anlehnung an das Militärgesetz […]». *HIN* sottolinea che al numero 4.10.3.2 manca un verbo (probabilmente «dafür sorgen, dass»), e quindi il testo deve essere corretto. *ISSS* chiede se si deve effettuare il CSP solo all'inizio o se la procedura deve essere ripetuta periodicamente. Avanza la seguente proposta redazionale: «diese Personen vor Aufnahme ihrer Tätigkeit und in begründeten Fällen auch während ihrer Tätigkeit eine PSP nach […]». Tessaris scrive in riferimento numero 4.10.3.3 che le comunità non dispongono delle competenze per prevedere delle procedure «offiziell festgelegte» e che quindi tale brano di frase all'inizio del numero deve essere stralciato.

[125] FR, NE, GE, VS, VD, JU
[126] CDS, BL, GL, LU, OW, UR, AR, SZ, NW, TG, ZG, ZH, ZAD, K3, VZK
[127] K3, VZK, ZAD, ZH, NW, ZG
[128] 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
[129] FR, NE, GE, VS, VD, JU

4.11 Requisiti in materia di protezione e sicurezza dei dati per terzi (cpv. 1 lett. f)

K3, *VZK*, *ZAD* nonché i Cantoni *ZH* e *NW* chiedono di verificare la necessità delle disposizioni riportate al numero 4.11. in caso affermativo, si dovrebbe sondare la possibilità di sostituirle con regolamentazioni generali e astratte nell'OCIP. OFAC vorrebbe sapere perché al numero 4.11 non si fa riferimento ai requisiti dell'articolo 10*a* LPD. *Posta* considera opportuno il registro di terzi di cui al numero 4.11.1 e chiede quale sia lo scopo del visto apposto dal responsabile della sicurezza dei dati. La formulazione è troppo vaga. Il termine «IT-Infrastrukturkomponenten» dovrebbe essere definito in modo più preciso, altrimenti bisognerebbe inserire nell'elenco anche Intel, Samsung, Microsoft ecc. Chiede quindi di stralciare la richiesta di visto e la formulazione «unter Umständen». In riferimento al numero 4.11.2, *SQS* evidenzia che la prima frase dovrebbe essere completata nel modo seguente: «Gemeinschaften müssen sicherstellen, dass kein Datenzugriff […]». *Tessaris* segnala degli errori di ortografia al numero 4.11.2 e chiede cosa s'intende in questo contesto per «Intermediäre» rispetto a «Dritte». *Posta* vorrebbe conoscere la differenza fra il numero 4.11.3 e il numero 4.11.4. Secondo *privatim* i contratti di cui al numero 4.11.5 dovrebbero assolutamente contenere le seguenti clausole: disposizioni secondo cui i terzi devono garantire che vengano autorizzati ad accedere ai dati solo i collaboratori che ne hanno veramente bisogno per adempiere al loro compito; una dichiarazione di confidenzialità per i collaboratori che li vincoli al segreto professionale anche oltre il termine del loro contratto di lavoro; divieto di trasferire i dati a terzi senza il consenso della comunità. La disposizione al numero 4.11.5.4 dovrebbe inoltre precisare chi ha diritto alla verifica periodica: i gestori della comunità o il responsabile della protezione dei dati della comunità? Sarebbe poi opportuno disciplinare che la comunità è autorizzata ad avvalersi di terzi competenti per effettuare tale verifica. *Privatim* desidera una riformulazione dei numeri da 4.11.5.5 a 4.11.5.7 e consiglia di evitare i rapporti di subappalto. Più persone sono coinvolte nelle procedure, più diventa difficile mantenere una visione d'insieme e il controllo. La disposizione dovrebbe pertanto essere modificata in modo da consentire solo in via eccezionale i rapporti di subappalto e solo previo consenso della comunità (un consenso puntuale e non generale).

4.12 Controllo e verifica dei servizi (cpv. 1 lett. f)

K3, *VZK*, *ZAD* e il Cantone *ZH* ribadiscono il parere espresso sul numero 4.11. *SQS* ripete l'osservazione fatta sull'articolo 11 capoverso 2 OCIP e sul numero 4.12.1 e propone di stralciare che il servizio di certificazione funge da centro di notifica per tutti gli eventi considerati rilevanti per la sicurezza.

4.13 Obbligo di notifica degli incidenti di sicurezza (cpv. 2)

K3, *VZK*, *ZAD* e il Cantone *ZH* ribadiscono il parere espresso sul numero 4.11 e 4.12, mentre *FMH* ripete il commento fatto sul numero 4.5.1.1. *SQS* non approva che il servizio di certificazione assuma il ruolo di centro di notifica per eventi di sicurezza. In questo punto non si dovrebbe neanche definire una procedura di notifica da parte delle comunità. Propone di cancellare il servizio di certificazione come centro di notifica e di stralciare il brano di frase «die Zertifizierungsstelle und» dal numero 4.13.1. *ISSS* segnala che in base a prescrizioni in altri contesti, p. es. nell'UE-RGPD, anche i pazienti devono essere informati di eventi rilevanti per la sicurezza se questi comportano per loro un potenziale rischio. Il numero 4.13.1 deve essere completato con la seguente frase: «[…] Zudem müssen Gemeinschaften formale Verfahren für das unverzügliche Melden von Vorfällen an die betroffenen Patienten, durch welche die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Patienten zur Folge hat, definiert haben».

4.14 Sicurezza di esercizio (cpv. 3)

4.14.1: *HIN* osserva riguardo al numero 4.14.1.1.1 che si tratta giustamente di un'autenticazione forte a 2 fattori. Sempre a riguardo, *SQS* chiede di precisare a partire da quando un'autenticazione a 2 fattori possa essere considerata forte. In riferimento al numero 4.14.1.1, *KSSG* scrive che l'applicazione di un'autenticazione a 2 fattori nei sistemi operativi, in particolare nelle banche dati e altri componenti

tecnici, è esagerata e solo difficilmente realizzabile. Ciò comporterebbe l'obbligo di applicare un'autenticazione a 2 fattori per tutti gli utenti dell'Active Directory e per ogni scopo (anche al di fuori della cartella informatizzata del paziente), una richiesta estremamente costosa e impraticabile. L'autenticazione a 2 fattori non è fattibile per tutte le banche dati. Il numero 4.14.1.1 deve quindi essere stralciato. *STSAG* teme che i numeri 4.14.1.1 e 4.14.1.3 – 4.14.1.10 implichino un onere eccessivo e chiede lo stralcio completo di tali disposizioni. 10 partecipanti[130] segnalano che al numero 4.14.1.1.2 la frase è incompleta e che manca almeno una parola. Il testo deve essere corretto. *HIN* propone concretamente di inserire in questo punto il termine «System». A parere di 6 Cantoni[131] è difficile garantire che un sistema sia in grado di impedire l'esportazione di dati del paziente, se l'accesso privilegiato consente di accedere ai dati del paziente. Questo accesso privilegiato presuppone il segreto professionale. I suddetti Cantoni chiedono lo stralcio del numero 4.14.1.1.3. *ISSS* considera il numero 4.14.1.2.3 non attuabile in pratica. Se il fornitore deve garantire l'infrastruttura e così anche il suo esercizio continuo, gli accessi non possono essere attivati solo se necessario. I Service Level Agreements (SLA) non possono così essere rispettati (cfr. 4.23.1.2). Il numero deve essere stralciato. *ISSS* propone la seguente precisazione al 4.14.1.4: «[…] diese verschlüsselt, örtlich getrennt und sicher aufbewahrt sind». In riferimento al numero 4.14.1.5 ritiene poco chiaro lo scopo di tale disposizione e del doppio controllo. Presuppone che la password non debba essere nota a una sola persona. È indispensabile spiegare come procedere in concreto, altrimenti è preferibile stralciare il numero. Riguardo ai numeri 4.14.1.4 e 4.14.1.5, *KSSG* considera eccessivo il principio del doppio controllo per il criptaggio dei backup e dell'accesso al materiale chiave, perché comporterebbe la creazione di un'infrastruttura di backup separata per la cartella informatizzata del paziente e quindi costi enormi. I numeri dovrebbero essere riformulati in modo da prescrivere la conservazione sicura dei backup. Spetterebbe ai provider IT decidere come risolvere concretamente la questione. *HIN* segnala che quanto richiesto al numero 4.14.1.7 avviene automaticamente non appena un fornitore assume l'esercizio dell'infrastruttura IT e che i backup vengono effettuati periodicamente. È irrealistico pensare di poter separare la memoria perché ciò implicherebbe un'attività manuale. Il numero in questione può pertanto essere stralciato. Anche *VAKA* sostiene lo stralcio di tale numero poiché ritiene eccessiva la richiesta (separazione della rete in caso di backup). Analogamente, *Posta* ritiene esagerata la richiesta di separazione della rete. I backup sono già criptati e la chiave è protetta secondo il principio del doppio controllo. *SCH* ricorda a riguardo che di solito le architetture cloud non prevedono più dei sistemi di memorizzazione con backup che debbano essere staccati dalla rete dopo essere stati copiati, perché la conservazione viene considerata sicura con i criteri di sicurezza previsti nell'ISO 27001 (criptaggio, doppio controllo in caso di accesso, ecc.). Anche *SCH* si dichiara favorevole allo stralcio. *HIN* ritiene necessaria una precisazione al numero 4.14.1.11 sui metodi di cancellazione, in analogia al numero 2.1. Propone pertanto la seguente aggiunta: «[…] vorgängig alle Daten kontrolliert und dokumentiert, vollständig und unwiderruflich gemäss aktuellen Best Practice Regeln gelöscht werden». *Privatim* considera il numero 4.14.1.11 troppo impreciso dal punto di vista della protezione dei dati e propone quindi il seguente testo: «Patientendaten auf Datenträgern, die nicht mehr benötigt werden, unwiderruflich gelöscht und die Datenträger anschliessend korrekt entsorgt werden». *SQS* evidenzia che la disposizione di cui al numero 4.14.1.12 è già contenuta al numero 2.9.25 e deve pertanto essere stralciata.

4.14.2 / 4.14.3: *ISSS* chiede in riferimento al numero 4.14.2.5, se per tutti i sistemi sia veramente necessario tenere dei componenti dedicati in una zona separata della rete e propone la seguente riformulazione: «[…] mittels geeigneter Trennung isoliert sein (bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich)». *STSAG* critica che quanto richiesto al numero 4.14.2 risulterebbe troppo oneroso e chiede lo stralcio di tutti i sottonumeri. 6 Cantoni[132] sostengono che le esigenze previste al numero 4.14.3 sono molto onerose e costose. È dunque opportuno ammettere un periodo massimo di 5 anni ai fini della certificazione. *KSSG* chiede come attuare la disposizione di cui al numero 4.13.3.4, se basta adottare un Change Management o bisogna introdurre un automatismo (applicazione). *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* ripetono al numero 4.14.3.10 il parere espresso sul numero 4.8.2. *SCH* osserva in riferimento

[130] CMC, BüAeV, GAeSO, KAeG SG, HIN, Posta, privatim, medshare, Medgate, SQS
[131] FR, NE, GE, VS, VD, JU
[132] FR, NE, GE, VS, VD, JU

al numero 4.14.3.10 che la stampa di dati e documenti è un'azione manuale che nell'esercizio del sistema non è collegata al sistema di protocollo integrato. È quindi impossibile o molto oneroso automatizzare il processo di stampa e renderne sicura la tracciabilità.

4.15 Acquisto, sviluppo e manutenzione dei sistemi (cpv. 3)

KSSG considera irrealizzabile la sorveglianza delle imprese di sviluppo da parte delle comunità e chiede lo stralcio completo del numero 4.15. Anche *K3*, *VZK*, *ZAD* e il Cantone *ZH* si associano a tale richiesta perché considerano superflua tale disposizione. *Integic* ritiene molto difficile attuare i punti del numero 4.15.2 quando ci si avvale di imprese esterne, perché sarebbe necessario anche il loro coinvolgimento. Poiché ciò è praticamente impossibile bisogna rivedere il testo. A parere di *CDS* e di 8 Cantoni[133], non è possibile far funzionare degli ambienti di test senza dati del paziente quando si tratta di ambienti d'integrazione e consolidamento. Attraverso mezzi tecnici e organizzativi è necessario garantire che i dati dei pazienti contenuti in un ambiente di test della cartella informatizzata del paziente siano protetti alla stessa stregua dei dati contenuti nell'ambiente produttivo. *KSSG* è della stessa opinione. Si propone la seguente formulazione del numero 4.15.2.5: «die Datenschutz- und Datensicherheitsanforderungen, welche die Datenhaltung betreffen, auch für Patientendaten in Konsolidierungs- und Integrationsumgebungen gelten. In anderen Test- und Entwicklungsumgebungen dürfen sich keine Patientendaten befinden.» *KSSG* aggiunge nella sua osservazione che agli ambienti d'integrazione sono collegati anche gli ambienti d'integrazione dei sistemi primari. In tali sistemi d'integrazione si vogliono esplicitamente effettuare dei test con dati reali. Si deve stralciare il numero riferito agli ambienti d'integrazione. Il Cantone *AR* interviene sul numero 4.15.2.5 sottolineando che in caso d'impiego di dati reali dei pazienti in un ambiente di test, la procedura deve soddisfare le direttive della protezione dei dati. *H+* scrive che per il test dei software, si dovrebbero poter utilizzare i dati dei pazienti nel quadro della legislazione in materia di cartella informatizzata del paziente. Anche *VGIch* considera che dovrebbe essere autorizzato l'utilizzo di dati dei pazienti per gli ambienti d'integrazione e consolidamento, a condizione che vengano rispettate le prescrizioni sulla protezione e sicurezza dei dati dei sistemi produttivi. *SQS* ritiene più realistica e preferibile la seguente redazione del numero 4.15.2.5: «In Testumgebungen dürfen sich keine echten bzw. nur anonymisierte oder pseudonymisierte Patientendaten befinden». *VAKA* e *Posta* chiedono lo stralcio del numero 4.15.2.6. *VAKA* osserva che non è chiaro cosa venga sorvegliato da chi. *Posta* si domanda come funziona questo requisito in caso di software acquistati e cosa ha a che vedere l'organizzazione di esercizio con lo sviluppo di software. Tale richiesta potrebbe creare problemi per la certificazione. *OFAC* segnala una contraddizione fra i numeri 4.15.1 e il 4.15.5. La validazione finale di una nuova versione prima della produzione necessita di un test di non regressione, realizzabile solo con dati reali. Si possono adottare delle misure per evitare che i test di validazione non creino vulnerabilità e siano severamente controllati alla stessa stregua dei sistemi produttivi. Si tratta di una questione di Change Management piuttosto che di una prescrizione legale. Il principio è di poter sempre provare il giusto equilibrio fra la qualità dei test effettuati e il rispetto della sfera privata del paziente.

4.16 Criptaggio nella comunicazione (cpv. 3)

SSIM e *FMH* chiedono il criptaggio di tutta la comunicazione e memorizzazione dei dati. *STSAG* considera esagerata la procedura richiesta all'interno della comunità secondo il numero 4.16.1 e vorrebbe stralciare il brano di frase in questione.

4.17 Memorizzazione di dati criptata (cpv. 3)

Insel chiede riguardo al numero 4.17, se per «besonders schützenswerte Daten» s'intendono tutti i dati dei pazienti o solo quelli sensibili e chiede una definizione più precisa. *SSIM* e *FMH* ribadiscono il parere espresso al numero 4.16, mentre *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* ripetono per il numero 4.17.1 le osservazioni fatte sui numeri 4.8.2 e 4.14.3.10. 6 Cantoni[134] confermano quanto osservato al numero

[133] BL, GL, LU, OW, UR, FR, BS, SZ
[134] FR, NE, GE, VS, VD, JU

4.8.2 anche per il numero 4.17. 13 partecipanti[135] dichiarano che o si devono criptare tutti i dati o nessuno. Non è comprensibile perché si debbano criptare solo i «dati particolarmente degni di protezione». Lo stesso vale per la richiesta di memorizzare con misure criptografiche solo i dati classificati «segreti» e «sensibili». Tale requisito non consente certo di risparmiare, perché bisogna in ogni caso spendere per creare le possibilità di criptaggio. Il numero 4.17.1 deve pertanto essere modificato. Alla critica sull'impossibilità di risparmiare costi si associano anche i Cantoni *TG* e *AI*, che chiedono il criptaggio di tutti i dati. *VAKA* non considera opportuna l'aggiunta «und integritätsgeschützt», poiché i dati sono già criptati, e vuole lo stralcio del brano di frase. Si dice inoltre sorpresa delle indicazioni sul criptaggio end-to-end contenute nel rapporto esplicativo. L'argomentazione non è plausibile e la formulazione «wird vorderhand verzichtet» suona come una minaccia. *VAKA* non è fondamentalmente contraria alle nuove tecnologie, ma si stupisce che si metta in risalto una tecnologia che non è mai stata discussa nelle istanze di eHealth Suisse, anche perché rimangono molti punti da chiarire a riguardo. *Tessaris* dichiara che si dovrebbero considerare «particolarmente degni di protezione» i dati contenuti nella cartella informatizzata del paziente che si riferiscono alla salute e alla terapia medica del paziente («informazioni rilevanti per la terapia»). Accanto a questi ci sono dati come l'indirizzo, informazioni amministrative, metadati che servono all'amministrazione e alla gestione della cartella informatizzata del paziente nonché alla trasmissione dei dati rilevanti per la terapia. Per motivi pratici e per evitare problemi di definizione, si potrebbe decidere di criptare sia i dati del paziente rilevanti per la terapia che i metadati. T*essaris* propone la seguente redazione: «Die Daten des elektronischen Patientendossiers, mit Ausnahme der Metadaten, müssen mit geeigneten und dem Stand der Technik entsprechenden kryptographischen […]», o altrimenti: «Die auf die Behandlung der Patientinnen und Patienten bezogenen Daten des elektronischen Patientendossiers müssen […]».

4.19 Sicurezza di comunicazione: gestione di reti (cpv. 3)

ISSS propone un nuovo numero 4.19.1.4 con la seguente formulazione: «nicht autorisierte WLAN-Zugriffspunkte erkannt und identifiziert werden», segnala però che tale requisito supplementare, a seconda dell'interpretazione, potrebbe già essere contenuto nel numero 4.19.1.2.

4.20 Sicurezza di comunicazione: servizi di rete (cpv. 3)

4.20.1: 6 Cantoni[136] chiedono cosa siano i «services d'information, d'utilisateurs et systèmes d'information» e desiderano degli esempi concreti di tali servizi. *VAKA* prega di verificare se i requisiti contenuti al numero 4.20.1.1 non siano già previsti nell'ATNA e, se è così, chiede di sopprimere il numero. *SQS* ripete l'osservazione fatta al numero 2.9.3 anche per i numeri da 4.20.1.1.2.1 a 4.20.1.1.5. Ritiene inoltre necessario completare i numeri da 2.9.4 a 2.9.21 con una disposizione sulla prova di una verifica tecnica delle premesse tecniche. *SCH* segnala in riferimento ai numeri 4.20.1.1.2.1 e 4.20.1.1.2.2 che i certificati EV sono criticati anche dagli esperti di sicurezza, perché offrono solo apparentemente una maggiore sicurezza dei certificati TLS pubblici, ma al contempo sono più costosi e onerosi dal punto di vista amministrativo. La protezione effettiva di un certificato tradizionale e di uno EV può essere uguale o addirittura inferiore nel certificato EV. Si chiede pertanto lo stralcio di «Extended-Validation» da entrambi i numeri. *ISSS* si dichiara favorevole all'inserimento di un nuovo numero 4.20.1.1.6 che leggerebbe: «ausschliesslich die für die Systemfunktion notwendigen Dienste, Protokolle und Daemons aktiviert sind».

4.20.2 / 4.20.3: *EHS* e *VGIch* obiettano che il numero 4.20.2.1 impedirebbe lo sfruttamento di sinergie della comunicazione orientata e non orientata attraverso una piattaforma eHealth e quindi genererebbe costi inutili perché promuoverebbe l'impiego di sistemi proprietari per la comunicazione orientata. Basterebbe una chiara separazione logica. Il numero dovrebbe essere modificato nel modo seguente: «Es werden Massnahmen getroffen, dass die Komponenten (Repository, Registry, Patientenindex) für die sichere Anwendung sowohl gerichteter wie ungerichteter Kommunikation gemäss EPDG/EPDV genutzt werden können», proposta sostenuta anche da *Insel*. *ISSS* considera che il termine «separiert» impiegato al numero 4.20.2.1 lascia troppo margine d'interpretazione e propone la seguente aggiunta: «[…]

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

aufweisen. Bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich». *VAKA* vorrebe invece lo stralcio di alcuni parti del testo, in modo da riformulare come segue il numero 4.20.2.1: «Dokumentenregister, Dokumentenablage, Berechtigungssteuerung und Patientenindex netzwerktechnisch von allen anderen Systemen separieren». Riguardo al numero 4.20.3.1 *SCH* scrive che le cosiddette zone demilitarizzate (DMZ) costituiscono solo una delle possibilità di proteggere le reti attraverso un pilotaggio scaglionato degli accessi con l'aiuto di firewall. Esistono altre strategie, utilizzate oggi soprattutto nelle architetture con cloud. Riguardo al numero 4.20.3.2, *SQS* chiede su quale base o prescrizione bisogna documentare / gestire un WAF e quali aspetti dell'implementazione tecnica del WAF debbano essere presi in considerazione. Un WAF esiste come hardware-appliance, software-plug-in su un webserver o come addon per firewall di rete o loadbalancer. I requisiti di documentazione per l'infrastruttura HW/SW del portale di accesso dovrebbero essere formulati in modo generico. Il numero deve pertanto essere completato o riformulato.

4.21 Scadenza delle sessioni di rete («Session Timeout»)

Per maggiore chiarezza, *privatim* desidera una riformulazione delle disposizioni e chiede inoltre di valutare se 2 ore di inattività non sia un periodo troppo lungo per i professionisti della salute: «Netzwerksitzungen, die während einer definierten Zeitperiode inaktiv sind (nicht bedient werden), sind vom System automatisch zu beenden. Die Inaktivitätsperiode beträgt bei Patienten 20 Minuten und bei Gesundheitsfachpersonen 1 Stunde». *VGIch* ribadisce la sua posizione già illustrata al numero 4.9.3. *Insel* osserva che per i pazienti una durata di sessione talmente breve potrebbe essere percepita come una notevole limitazione della fruibilità e propone di seguire le disposizioni in materia di online banking. Il paziente potrebbe definire la propria scadenza di sessione e assumersi personalmente il rischio della sua scelta. *K3*, *VZK*, *ZAD* e il Cantone *ZH* ritengono poco opportuno prescrivere cifre assolute per il logout automatico e considerano sufficiente una regolamentazione generale astratta. Il numero 4.21 dovrebbe quindi essere stralciato e sostituito con una disposizione nell'OCIP(-DFI). Anche *SQS* pensa che non abbia molto senso definire il timeout delle sessioni e contesta la prescrizione di un intervallo di 2 ore per i professionisti della salute. Il riferimento orario deve essere soppresso, oppure bisogna indicare una durata massima. Il timeout dopo massimo 20 minuti dovrebbe essere applicato a tutti. *FMH*, *SSIM* e *STSAG* considerano la definizione di session timeout poco adatta a un'ordinanza e chiedono dunque lo stralcio del numero 4.21. Sempre a questo riguardo, *Bleuer* attira l'attenzione sul rischio di una consultazione solo parziale dei documenti e chiede di stralciare questo numero o almeno di allungare i tempi. *BINT* vuole la soppressione del numero 4.21 perché potrebbe condurre a dati incompleti dei pazienti. Quando si tratta dei propri dati ciò costituisce inoltre un'ingerenza nella sfera privata. Si chiede perché questo aspetto venga disciplinato a livello di ordinanza e perché i tempi previsti per i pazienti siano più corti. *ISSS* ritiene giusto prevedere una scadenza della sessione, ma considera più opportuno definirla altrove, inserendo un rinvio in questo punto. In caso di una modifica della scadenza, non bisognerebbe dover cambiare l'intero allegato. Inoltre sarebbe forse più opportuno parlare in generale di sessioni (e non sessioni di rete), perché gli stessi principi si applicano anche ai posti di lavoro offline. Propone la seguente redazione del numero 4.21.1: «[…] definierten Inaktivitätsperiode automatisch beendet werden» e la seguente per il numero 4.21.2: «[…], wenn während der Inaktivitätsperiode keine Interaktion des Benutzers mit dem elektronischen Patientendossier stattfand». *SCH* sottolinea che dalle esperienze raccolte con il portale della salute di Swisscom risulta che le sessioni di breve durata sono considerate poco fruibili, soprattutto quando alla scadenza della sessione l'utente è obbligato ad autentificarsi con 2 fattori. La limitazione della durata di sessione è una misura oggi abitualmente adottata per evitare il session hijacking. Tuttavia, poiché l'ordinanza già esclude la possibilità di scaricare in massa documenti della cartella informatizzata del paziente, un eventuale danno sarebbe limitato solo a singoli pazienti e a un numero limitato di documenti. Non si può escludere che informatici innovativi sviluppino in futuro altre procedure per impedire il session hijacking e aumentare la fruibilità. *SCH* propone di chiedere ai gestori delle comunità di dimostrare che per evitare il session hijacking adottano misure adeguate e secondo lo stato della tecnica. 6 Cantoni[137] rilevano in riferimento al numero 4.21.1 che 2 ore sono troppo corte per un professionista della salute e che sarebbe meglio prevedere 4 ore

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

(mezza giornata). Bisogna evitare che il medico sia obbligato a riconnettersi troppo spesso. Chiedono pertanto di modificare la durata e di chiarire il concetto «les sessions dans le réseau». *SUVA* non capisce perché le sessioni di rete inattive debbano scadere dopo un periodo di inattività di 20 minuti quando gli utenti sono i pazienti e di 2 ore quando sono i professionisti della salute. Ciò rappresenta una grave violazione della sfera privata. Una tale disparità non è inoltre né legale né equa. Il numero 4.21.1 deve essere o stralciato o altrimenti prevedere la stessa durata per tutti.

4.22 Memorizzazione temporanea (cpv. 3)

KSSG fa notare che dovrebbe essere possibile un coaching di tali dati in modo da consentire una performance accettabile della cartella informatizzata del paziente e, in caso di interruzione dei Services CPI centrali, il funzionamento ininterrotto della cartella informatizzata del paziente.

4.23 Disponibilità (cpv. 3)

In riferimento al numero 4.23.1.2, *ISSS* critica l'insoddisfacente formulazione «vertraglich vereinbarte Verfügbarkeit über die Zeit von mindestens 98%». Se si prende come parametro un anno, ciò corrisponderebbe a un'interruzione di 7 giorni. Sarebbe preferibile una soluzione con un periodo predeterminato e/o con una durata d'interruzione definita in cifre assolute, Chiede pertanto di aggiungere il seguente brano di frase: «[…] Last aufweisen, wobei die maximale Ausfalldauer am Stück 48h nicht überschreiten darf». Una precisazione del numero 4.23.1.2 è richiesta anche da *Posta*, che desidera sapere in particolare che cosa s'intende per «sowie unter Last». Tali requisiti dovrebbero inoltre essere soddisfatti anche dai sistemi esterni che sono rilevanti per la comunità. *Posta* domanda pertanto di inserire al punto giusto dell'ordinanza questo impegno per l'UCC e per i servizi centrali. Riguardo al numero 4.23.1.3 *HIN* osserva che non esiste una protezione completa contro gli attacchi DoS senza terminali specifici. Non si capisce perché menzionare esplicitamente questa minaccia e altre no. *HIN* parte dal presupposto che le diverse norme (ISO ecc.) implichino una protezione secondo lo stato dell'arte delle risorse Internet. Come alternativa propone l'introduzione di Service Level Agreement per le richieste intercomunitarie e il portale pazienti / professionisti della salute, nonché di stralciare il numero 4.23.1.3. Riguardo allo stesso punto, *Tessaris* osserva che è impossibile realizzare la richiesta di protezione assoluta contro gli attacchi DDoS, ma che si dovrebbe invece esigere di impiegare tutti i mezzi disponibili secondo lo stato della tecnica per contrastare tali attacchi. Propone la seguente formulazione: «[…] des elektronischen Patientendossiers nach dem Stand der Technik gegen sog. DDoS Angriffe geschützt sind». *STSAG* considera troppo oneroso il requisito del numero 4.23.1.4 e chiede pertanto di sopprimerlo.

4.24 Supporti di memoria dei dati soggetti alla giurisdizione svizzera (cpv. 4)

Privatim rimanda alle osservazioni fatte sull'articolo 11 capoverso 4 OCIP. Il Cantone *AR* si dichiara favorevole alla memorizzazione dei dati sotto giurisdizione svizzera. *CDS* e 8 Cantoni[138] criticano le prescrizioni relative all'assoggettamento della cartella informatizzata del paziente alla giurisdizione svizzera, perché temono che non consentano di raggiungere lo scopo prefisso. Il numero 4.24 deve essere completamente riveduto. Anche *ZAD* nonché i Cantoni *ZG e ZH* sono favorevoli a una revisione completa del numero in questione perché ritengono che la formulazione «juristische Personen, die unter Schweizer Recht sind» sia inconsueta e poco chiara. Lo stesso vale per «für die Erbringung der Leistung ausschliesslich unter Schweizer Recht handeln.» Un'impresa che non opera solo in Svizzera non potrebbe soddisfare questo requisito. Ci s'interroga sullo scopo di tale frase. Anche la formulazione «Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erbringen» non è chiara. I suddetti partecipanti chiedono cosa succede di un'impresa i cui server si trovano e sono amministrati in Svizzera, ma che per alcuni servizi si rivolge a fornitori all'estero (una realtà per la maggior parte delle imprese di una certa dimensione). *ZAD* e Cantone *ZH* considerano inoltre necessario verificare se la condizione che si debba trattare di un'impresa svizzera sia compatibile con le disposizioni sugli acquisti pubblici (in particolare: rispetto dell'accordo sugli appalti pubblici e degli accordi bilaterali).

[138] BL, GL, LU, OW, UR, FR, NW, SZ

In riferimento al numero 4.24.1.1, *CMC*, *BüAeV*, *GAeSO*, *KAeG SG* e *HIN* criticano la mancanza di chiarezza della formulazione secondo la quale è necessario garantire che l'esercizio dei supporti di memorie dei dati della cartella informatizzata del paziente debba essere effettuato da persone giuridiche «unter Schweizer Recht sind». Probabilmente significa che queste persone giuridiche devono essere soggette al diritto svizzero. Essi propongono le seguenti alternative: «Schweizer Recht unterstehen» o «in der Schweiz domiziliert sind». In merito al numero 4.24.1.2, *SCH* dichiara che in base all'allegato le prestazioni devono essere fornite interamente in Svizzera. Vista la supremazia tecnologica di alcuni Paesi, il coinvolgimento di soli operatori informatici svizzeri è poco probabile. La limitazione di fornire tutte le prestazioni sul territorio svizzero obbligherebbe le comunità ad autorizzare ogni singolo trattamento di dati all'estero. Questa procedura non è necessaria a garantire il rispetto del diritto svizzero, anzi pregiudica la stabilità della fornitura di prestazioni. Anche in caso di memorizzazione di dati in centri di calcolo svizzeri da parte di imprese svizzere, è nell'interesse del cliente consentire il trattamento dei dati da parte di subfornitori o collaboratori residenti all'estero. Si dovrebbe piuttosto esigere che la prestazione principale debba essere essenzialmente fornita in Svizzera. *SCH* propone pertanto la seguente formulazione per il numero 4.24.1.2: «die Hauptleistung ist im Wesentlichen innerhalb der Schweizer Landesgrenzen zu erbringen».

SWICO chiede la soppressione del numero 4.24.1.3. Secondo *Tessaris* questa disposizione destinata alle comunità che sono in gran parte di diritto pubblico viola l'articolo 3 e l'articolo 23 numero 2 dell'accordo sugli appalti pubblici (RS 0.632.231.422) perché non si può presupporre in buona fede che la protezione e la sicurezza dei dati nell'esercizio della cartella informatizzata del paziente di una comunità possa essere fornita solo da un'impresa che sia maggioritariamente di proprietà svizzera. Anche *Tessaris* si associa quindi alla richiesta di stralcio di questo numero. *EHS* er *VGIch* fanno notare riguardo ai numeri 4.24.1.3 e 4.24.1.4 che le persone giuridiche in Svizzera sono soggette al diritto svizzero, indipendentemente dai rapporti di proprietà. Il bando di concorso per una piattaforma di eHealth indetto da un'organizzazione svizzera responsabile in ambito eHealth è soggetto alle regole GATT/WTO e in questa fattispecie i fornitori stranieri con una filiale in Svizzera sarebbero autorizzati a partecipare alla gara di appalto, ma non potrebbero gestire una tale piattaforma. Considerano pertanto inammissibili entrambi i numeri perché violano il diritto sovraordinato. Le CTO non devono comprendere disposizioni di questo tipo. 6 Cantoni[139] chiedono riguardo al numero 4.24.1.4, se ciò significa che le persone giuridiche devono lavorare solo in Svizzera. Il numero deve essere riformulato. *Posta* s'informa in questo contesto se tale prescrizione si riferisce alla prestazione stipulata nei contratti. Se non è così e se vale in generale, un fornitore che effettua prestazioni anche all'estero sarebbe escluso. Tale approccio è sbagliato e colpirebbe anche la Posta. La traduzione in francese ha un significato diverso dal tedesco; la questione deve quindi essere chiarita.

5. Punto di contatto per i professionisti della salute (art. 12 OCIP)

13 partecipanti[140] ribadiscono il commento fatto al numero 4.10.2.3 anche per il numero 5.1.2.2. *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* si dicono favorevoli alla creazione di un service-desk. Manca purtroppo però una regolamentazione su chi deve assumere i costi di gestione del service-desk e degli aiuti al service-desk. Non devono essere a carico dei professionisti della salute, che devono già sostenere un'elevata spesa per l'introduzione della cartella informatizzata del paziente. I suddetti partecipanti chiedono la seguente aggiunta al numero 5.1.1: «[…] im Umgang mit dem elektronischen Patientendossier kostenlos unterstützt». *STSAG* preferirebbe limitare la disposizione di cui al numero 5.1.1 alle sole comunità di riferimento e sostituire il termine «Gemeinschaft» con «Stammgemeinschaft». 6 Cantoni[141] fanno notare al numero 5.1.2.2 che i datori di lavoro scelgono già con cura i loro collaboratori e questi ultimi sono legati al segreto professionale. Non serve a nulla ricordarlo. Il numero in questione deve pertanto essere stralciato. I Cantoni *GE*, *VS*, *VD*, *JU* e *FR* scrivono inoltre in riferimento al numero 5.1.2.4, che la documentazione non è tecnicamente possibile con i software disponibili sul mercato e

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

che quindi bisogna sopprimere il brano di frase «et que l'accès est documenté automatiquement». Riguardo al numero 5.1.2.4 *HIN* sostiene la richiesta di documentare l'accesso a distanza. Non è invece d'accordo sull'obbligo di documentazione automatica e quindi chiede di stralciare la parola «automatisch». *Posta* s'informa come debba avvenire l'informazione o il consenso per l'accesso a distanza e come si debba procedere alla documentazione.

6. Informazione del paziente (art. 14 OCIP)

A parere di *K3*, *VZK*, *ZAD* nonché dei Cantoni *ZG e ZH* le disposizioni del numero 6 sono già previste nella LCIP e nell'OCIP per cui possono essere eliminate.

6.1.2 / 6.1.3: 6 Cantoni[142] osservano che i punti da spiegare ai pazienti sono troppo lunghi e complicati per essere capiti. Dall'esperienza dei Cantoni romandi, fondata su oltre diecimila pazienti, emerge che il tempo di concentrazione e disponibilità di un paziente non supera i 15 minuti. Bisogna dunque spiegare solo gli elementi essenziali. Secondo le loro stime, basate sulla prassi, ci vorrebbero altri 30 minuti per spiegare tutti i punti indicati al numero 6.1 a una persona di età media e mentalmente sana. Per una comunità con 100 000 pazienti ciò significherebbe 4 500 000 minuti, ossia 9 375 giorni/uomo o 42 anni/uomo. Con 10 collaboratori (ossia 1 milione di franchi di salari all'anno), ci vorrebbero 4 anni. Essi chiedono di mantenere in primo luogo solo i seguenti punti: 6.1.2.5, 6.1.3.5, 6.1.4.1-2-5, 6.1.5.2. Il paziente dovrebbe poi avere la possibilità di informarsi su altri aspetti. *VAKA*, *K3* e *VZK* fanno notare che le informazioni previste al numero 6.1.2.1 sarebbero troppo complesse per un paziente normale e devono quindi essere stralciate. Riguardo al numero 6.1.2.3, *VAKA* aggiunge che ogni comunità di riferimento lo fa nel proprio interesse e che non deve quindi essere prescritto. Il numero deve essere quindi stralciato. *KSSG* fa osservare riguardo al numero 6.1.3.2 che la comunità di riferimento può sì informare il paziente su questi punti, ma non ha nessuna possibilità di garantirne il rispetto. *OFAC* ritiene necessario precisare che si parla di una cartella informatizzata del paziente unica, conforme alla LCIP e custodita da una comunità di riferimento certificata che utilizza un unico NIP generato dall'UCC. Non si prendono in considerazione le cartelle pilota cantonali che non sono certificate secondo i requisiti della LCIP e non utilizzano un NIP unico rilasciato dall'UCC. A proposito del numero 6.1.3.4, *SPO* chiede cosa s'intenda per conseguenze legate al cambiamento di comunità di riferimento. Se si tratta dei processi indicati ai numeri 8.4.2.2 e 8.4.2.3, non è necessaria una modifica, altrimenti bisogna elencare le diverse conseguenze. *VAKA*, *K3* e *VZK* vedono nel numero 6.1.3.5 una contraddizione con la richiesta di conservare la dichiarazione di revoca e chiedono un adeguamento. Per il numero 6.1.3.6, *IG eHealth* osserva che la cartella informatizzata del paziente può essere soppressa ai sensi dell'articolo 20 capoverso 1 OCIP. In questo caso il NIP viene annullato nella banca dati d'identificazione dell'UCC. Una volta revocato il consenso alla tenuta di una cartella informatizzata, il paziente ha però la possibilità di riaprire una cartella. Al momento della riapertura gli viene attribuito un nuovo NIP. *IG eHealth* apprezza la possibilità per un paziente di aprire più volte una cartella informatizzata, sarebbe però opportuno avvertirlo prima della soppressione della sua cartella che i dati memorizzati in tale cartella vanno persi e che in caso di apertura di una nuova cartella è obbligato a registrare nuovamente i documenti desiderati nella nuova cartella informatizzata del paziente.

6.1.4 / 6.1.5: 6.1.4 / 6.1.5: *Posta* prega di chiarire al numero 6.1.4.6 come ottenere l'autorizzazione all'accesso a distanza e come documentarlo. Il Cantone *ZH* e *ZAD* ritengono problematico prevedere che i collaboratori del service-desk abbiano un accesso a distanza ai terminali dei pazienti. Per motivi di sicurezza, un accesso a distanza corretto non dovrebbe essere possibile senza la partecipazione del paziente. Una comunità di riferimento non può garantire che sia possibile tale accesso. La stessa osservazione è fatta anche da *K3* e *VZK*. Il Cantone *ZH*, *ZAD*, *K3* e *VZK* vogliono pertanto sopprimere il numero 6.1.4.6. *VGIch* ribadisce la posizione espressa sull'articolo 14 capoverso 2 OCIP anche sul numero 6.1.5. *STSAG* desidera aggiungere un numero 6.1.5.6 con il seguente testo: «das Risiko durch Einstellung der Zugriffsrechte die Behandlungssicherheit zu gefährden und eine allfällige Verantwortung hierfür zu tragen».

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

7. Consenso (art. 15 OCIP)

K3, *VZK* nonché i Cantoni *ZH e ZG* ribadiscono in questo contesto il loro parere sul numero 6. *SCH* chiede che per raggiungere l'obiettivo di una maggiore digitalizzazione possibile si debba accettare inequivocabilmente la firma elettronica, che secondo l'articolo 14 capoverso 2bis CO è equiparata a quella autografa. Si devono inoltre autorizzare anche altri mezzi ausiliari intesi a identificare in modo univoco le persone. La precisazione dovrebbe avvenire a livello di ordinanza (e non solo nel rapporto esplicativo). Il numero 7.1.1 deve quindi essere completato con la seguente frase: «[…] eingeholt wird. Der eigenhändigen Unterschrift gleichgesetzt sind die qualifizierte elektronische Signatur sowie andere Hilfsmittel zur eindeutigen Bestimmung der Identität der Patientin oder des Patienten».

8. Gestione (art. 16 OCIP)

Il Cantone *ZH*, *K3*, *VZK* e *ZAD* ritengono troppo dettagliato il numero 8 e chiedono una semplificazione. Gran parte di queste disposizioni risultano già dalla LCIP e dall'OCIP e possono essere stralciate. Ciò vale in particolare per i numeri 8.6 e 8.7.

8.1 Ingresso e uscita di pazienti (cpv. 1 lett. a)

Posta segnala che la frase al numero 8.1.1.1 sembra essere incompleta e dovrebbe essere corretta nel modo seguente: «[…] zur Sicherstellung der Vorgaben nach […]».

8.2 Identificazione dei pazienti (cpv. 1 lett. b)

Secondo *K3* e *VZK,* è eccessivo chiedere che il paziente debba soddisfare gli stessi elevati requisiti di SID dei professionisti della salute per accedere alla propria cartella informatizzata. Ciò comporterebbe che tutti i pazienti debbano procurarsi (e rinnovare) un SID a pagamento per poter gestire la loro cartella informatizzata. L'accesso dovrebbe essere gratuito per i pazienti ed eseguibile con strumenti analoghi all'online banking. Ciò vale sia per il numero 8.2.2 che per il numero 8.3.1 e, in funzione della situazione, anche per il numero 8.8.2. In riferimento al numero 8.2.2.1.1, *Posta* osserva che bisogna essere in possesso del NAVS13 per poter ottenere il NIP presso l'UCC. Secondo lei, chi rilascia un SID non è autorizzato a rilevare il NAVS13 e a trasmetterlo ad altri. Tutta la regolamentazione in materia di impiego del SID è poco pertinente. OFAC ribadisce la posizione espressa al numero 6.1.3.2 e *KSSG* l'osservazione fatta sul numero 6.1.3.2 anche a proposito del numero 8.2.2.2. *KSSG* chiede inoltre o lo stralcio del numero o l'aggiunta della possibilità tecnica di consultazione. *Integic* desidera un chiarimento su come garantire l'applicazione della disposizione al numero 8.2.2.2.

8.3 Identificazione e autenticazione (cpv. 1 lett. c)

VAKA, *K3* e *VZK* ritengono indispensabile menzionare al numero 8.3.3 la possibilità di effettuare l'autenticazione mediante mTan. *HIN* si dichiara nuovamente favorevole a un'autenticazione forte a 2 fattori e chiede quindi di mantenere il numero 8.3.3.1. *Posta* afferma che il numero 8.3.3.1 è incomprensibile: prima è richiesto un SID di un emittente certificato e poi si possono utilizzare procedure d'autenticazione a piacimento. Ci vuole uno standard che valga per tutti.

8.4 Cambiamento di comunità di riferimento (lett. e)

Privatim vorrebbe stabilire al numero 8.4.2 che anche le «vecchie» comunità di riferimento sono tenute a distruggere tutte le informazioni sulla cartella informatizzata del paziente – ad eccezione della documentazione che la legge prevede di conservare (p. es. art. 20, cpv. 2, lett. a OCIP). In concreto propone quanto segue: «alle im Zusammenhang mit dem elektronischen Patientendossier stehenden Daten unwiderruflich vernichtet werden. Ausgenommen sind Unterlagen, die von Gesetzes wegen aufzubewahren sind». *Medgate* rileva un errore nel testo del numero 8.4.2.2 e propone la seguente correzione: «die

Ermächtigung von Gesundheitsfachpersonen gemäss […]». In riferimento al numero 8.4.2.3, *BFH* non capisce perché in caso di cambiamento della comunità di riferimento, il rappresentante del paziente perda automaticamente i suoi diritti di rappresentanza. Questo dovrebbe essere esplicitamente comunicato al paziente. I Cantoni *GE*, *VS*, *VD*, *JU* e *FR* scrivono che la soppressione della cartella informatizzata del paziente in caso di cambiamento della comunità di riferimento dovrebbe essere possibile ma non obbligatoria. 6 Cantoni[143] dichiarano che un medico che lascia il paziente, conserva l'accesso alla sua cartella medica anche se non ne ha più bisogno. Secondo i suddetti Cantoni, non vi è motivo di credere che un paziente che cambia comunità voglia anche cambiare rappresentante. I numeri 8.4.2.2 e 8.4.2.3 devono essere stralciati. *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* si rallegrano che, come auspicato nell'indagine conoscitiva sulla LCIP, sia stata inserita una disposizione sul cambiamento di comunità di riferimento, dubitano però che il cambiamento di comunità di riferimento funzioni con le stesse regole stabilite in caso di scioglimento di una comunità di riferimento. Cosa succede se la comunità di riferimento non è in grado di traslocare? Suggeriscono di inserire l'obbligo di creare un meccanismo di salvaguardia e chiedono un nuovo numero 8.4.2.4 con il seguente testo: «der Wechsel der Stammgemeinschaft auch dann möglich ist, wenn die Stammgemeinschaft den Wechsel nicht durchführen kann».

8.5 Garanzia che la configurazione dei diritti di accesso venga elaborata secondo la volontà del paziente (cpv. 2: diritti di accesso (art. 2 OCIP cpv. 1) e opzioni del paziente (art. 3 OCIP)

KSSG considera il numero 8.5.1 incomprensibile e impossibile da interpretare. I numeri 8.5 e 8.5.1 devono essere formulati in modo da rendere i requisiti comprensibili e chiari.

8.6 Autorizzazione (cpv. 2): diritti di accesso (art. 2 OCIP cpv. 1-4)

VAKA non vede l'utilità di questo numero, che riprende semplicemente le informazioni dell'OCIP, e chiede di stralciarlo. In riferimento al numero 8.6.2.3, *BFH* rimanda al suo commento sulla problematica relativa all'articolo 8 lettera e OCIP.

8.7 Opzioni del paziente (art. 3 OCIP)

VAKA ribadisce qui il parere espresso sul numero 8.6. Riguardo al numero 8.7.2.1, il Cantone *AR* rimanda alle osservazioni e alle proposte di modifica fatte sull'articolo 3 lettera a OCIP. *KSSG* osserva che in ospedale sono soprattutto i medici assistenti a cambiare relativamente spesso di reparto e quindi di gruppo. Il numero 8.7.2.6 vieterebbe l'accesso a informazioni rilevanti proprio ai medici assistenti, che sono quelli che più hanno bisogno dei dati della cartella informatizzata del paziente. Il numero deve essere stralciato. Basterebbe informare il paziente dei nuovi ingressi e delle mutazioni. *Posta* segnala al numero 8.7.2.8, che dovrebbe essere un'impostazione standard e che bisognerebbe chiarire dove arriva la catena di autorizzazioni. 6 Cantoni[144] considerano il numero 8.7.2.9 poco chiaro e desiderano degli esempi concreti.

8.8 Rappresentante (art. 16 cpv. 3)

CMC, *BüAeV*, *GAeSO* e *KAeG SG* osservano che l'articolo 16 capoverso 3 OCIP non esiste e che bisogna quindi eliminare il rinvio nel titolo o eventualmente sostituirlo con l'articolo 3 lettera g OCIP. 6 Cantoni[145] chiedono di eliminare nella versione francese la ripetizione della parola «du patient» nei numeri 8.8.2 e 8.8.3.4. Riguardo al numero 8.8.3.4 aggiungono che il rappresentante può avere diversi strumenti di autenticazione (mTan, SwissID, ecc.) e che in pratica potrebbe risultare molto difficile, nell'ambito di un audit di certificazione, garantire l'applicazione di tale requisito. Chiedono inoltre di fornire esempi concreti sulla garanzia «manière univoque et correcte» e propongono la seguente formulazione del numero 8.8.3.4: «le compte utilisateur servant au représentant du patient est relié de manière […]».

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

9. Portale di accesso per i pazienti (art. 17 OCIP)

9.1 Conformità con le disposizioni di legge

9.1.1: *VAKA* dichiara che deve trattarsi di un errore e chiede lo stralcio del numero. *Posta* chiede cosa s'intenda per «einschlägig rechtlichen Anforderungen» e desidera una precisazione del numero 9.1.1. Sulla stessa falsariga, *privatim* scrive che non è chiaro a quali disposizioni legali si faccia riferimento. La redazione dovrebbe essere più precisa e si dovrebbero menzionare alcune delle disposizioni. Secondo i Cantoni *ZG e ZH*, *K3*, *VZK* e *ZAD* è ovvio che le relative disposizioni di legge debbano essere rispettate. Sarebbe sbagliato trasformare un obbligo scontato in una condizione di certificazione. Un servizio di certificazione non è in grado di verificare che tutte le disposizioni siano state rispettate. Il numero 9.1.1 deve pertanto essere stralciato.

9.1.3: 6 Cantoni[146] ritengono il numero 9.1.3.1 poco chiaro. Se un paziente mette a disposizione i dati, dà anche il suo consenso. La questione dovrebbe essere chiarita. *Medgate* segnale nello stesso numero il seguente errore di ortografia: «[…] nur dann im elektronischen Patientendossier erfasst […]».*Posta* afferma che i numeri 9.1.3.1 e 9.1.3.2 sono in contraddizione. Esistono documenti che vengono registrati al di fuori della cartella informatizzata del paziente e che per il trasferimento nella cartella necessitano del consenso del paziente. D'altro canto è vietato memorizzare dei documenti a titolo provvisorio al di fuori della cartella. Si richiede una precisazione. *SBC* è del parere che la limitazione prevista al numero 9.1.3.2 non abbia senso e chiede lo stralcio del numero. A tale richiesta si associa anche *SSIM* perché considera eccessivo esigere che la registrazione dei dati forniti dal paziente avvenga sempre e solo direttamente nella cartella informatizzata del paziente. Secondo *BINT* non è opportuno fare del numero 9.1.3.2 una regola generale e ne chiede la soppressione. Non è importante se un documento viene caricato direttamente nella cartella informatizzata del paziente e poi scaricato in un altro supporto di memoria, oppure il contrario. *Medgate* evidenzia anche qui un errore ortografico da correggere «bereitgestellten». *Privatim* si chiede come si debba procedere con i dati che devono confluire nella cartella informatizzata del paziente attraverso le applicazioni-salute e come si possa garantire che tali dati non siano provvisti di malware o problemi analoghi. OFAC osserva sul numero 9.1.3.3 che questo contraddice i numeri 3.5.1.3 e 9.5.1.3 che autorizzano il «bulk download». 6 Cantoni[147] non capiscono inoltre il senso della frase al numero 9.1.3.3. Bisognerebbe spiegare che cosa s'intende per «domaines fonctionnels». *SSIM* fa notare che il paziente può pilotare la trasmissione di dati attraverso le autorizzazioni. Potrebbe essere nell'interesse del paziente che i suoi dati vengano trasmessi implicitamente. Il numero 9.1.3.3 deve pertanto essere stralciato. Nell'interesse della terapia e della sicurezza del paziente, *FMH* chiede una verifica critica delle esigenze stabilite al numero 9.1.3.3.

9.2 Presentazione

12 partecipanti[148] ribadiscono i commenti fatti al numero 3.2.1.3 anche per il numero 9.2.1.3. *BFH* considera poco palese la differenza fra il numero 9.2.1.1 e il 9.2.1.2. *Medgate* rileva due errori di battuta. Al numero 9.2.1.1 si dovrebbe scrivere «Gesundheitsfachperson» invece di «Gesundheitsfachpersonen» e al numero 9.2.1.5 «Zugriffsrechte» invece di «Zugriffsrechten».

9.3 Assenza di barriere

VAKA, *K3* e *VZK* fanno notare al numero 9.3.1.1 che l'assenza di barriere si riferisce ai disabili e non alle persone anziane e suggeriscono di sostituire il termine «behinderte Patientinnen und Patienten» con «Menschen mit Behinderung». Concretamente, propongono lo stralcio delle parole «behinderte

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

oder ältere». In riferimento al numero 9.3, 6 Cantoni[149] rimandano ai pareri espressi sul numero 3. *SBV* ribadisce la posizione espressa sul numero 3.3.1.2 anche riguardo al numero 9.3.1.2. *VGIch* dichiara che gli elementi fondamentali del requisito dovrebbero essere disciplinati nell'ordinanza e non nel testo d'esecuzione del DFI, perché qui non si rispetta il principio di legalità.

9.4 Formati di dati: messa a disposizione

6 Cantoni[150] rimandano per il numero 9.4 ai pareri espressi sul capitolo 4. Il Cantone *ZH*, *K3*, *VZK* e *ZAD* scrivono che le disposizioni del numero 9.4 sono già contenute nella LCIP e nell'OCIP oppure sono ovvie e devono quindi essere stralciate. *SCH* ripete il parere sul numero 3.4 anche in riferimento al numero 9.4 mentre *K3* e *VZK* ripetono il commento sul numero 3.4.1.2 anche per il numero 9.4.1.2. Riguardo ai formati di dati, *Posta* osserva che l'OCIP-DFI definisce come fonte l'allegato 4, mentre le CTO l'allegato 3 (Metadati) e che è quindi necessaria una precisazione. Non ha senso inoltre che la cartella informatizzata del paziente diventi un convertitore di dati. Oggi non è più difficile convertire i dati in un file PDF presso l'utente o nel sistema primario. *Posta* ritiene che non si debbano convertire i documenti e chiede di sopprimere tale richiesta.

9.5 Formati di dati: consultazione

Il Cantone *ZH, K3, VZK* e *ZAD* ribadiscono la posizione espressa sul numero 9.4. 6 Cantoni[151] rimandano, in riferimento al numero 9.5, ai pareri sul numero 5. *BFH* chiede perché il portale di accesso debba supportare il download in un sistema primario, visto che il professionista della salute ha un proprio accesso. Anche il numero 9.5.1.2 deve essere stralciato. *SCH* segnala a riguardo che il paziente non dispone di un sistema primario. Anche *Medgate* non capisce cosa s'intenda in questo punto per sistema primario e suppone che si tratti di un errore, che deve quindi essere corretto. *Posta* afferma che l'esigenza stabilita al numero 9.5.1.3 non è chiara. Non compete alla LCIP stabilire come debbano funzionare le interfacce fra le comunità; fra le comunità si applicano le prescrizioni del Cross-Community Access (XCA) (o Cross-Community Fetch XCF). Tale requisito avrebbe un senso solo se se standardizzasse anche il «bulk download». Si chiede pertanto di stralciarlo. *Posta* fa inoltre notare che i rate limit e i relativi «use case» debbano essere definiti in dettaglio per evitare discussioni annose. Anche qui richiede la soppressione di tale requisito.

9.6 Dati verbalizzati (lett. c)

Il Cantone *ZH*, *K3*, *VZK* e *ZAD* ribadiscono il parere espresso ai numeri 9.4 e 9.5. *BFH* chiede cosa s'intenda per «lesbarer Form» e propone una diversa redazione: «[…] allen Gemeinschaften und Stammgemeinschaften in einem für sie nachvollziehbarem, eindeutig und leicht verständlichem Inhalt einzusehen». *Privatim* critica che tale formulazione non indica in quale misura il paziente possa effettuare una panoramica di tutti i dati verbalizzati dalle comunità e comunità di riferimento. Si tratta di un elemento importante per un controllo efficace. Si chiede di verificare se la redazione possa essere precisata in questo senso.

10. Disponibilità dei dati registrati dai pazienti (art. 18 OCIP)

10.1 Archivi di documenti per i documenti dei pazienti

10.1.1 / 10.1.2: *HIN* presuppone che per «dezidiert», al numero 10.1.1, non s'intenda una separazione fisica. È infatti sufficiente una separazione logica. Si propone la seguente aggiunta: «[…] bereitstellen, die von den Dokumentenablagen für die Gesundheitsfachpersonen und Gesundheitseinrichtungen logisch getrennt sind». *CMC*, *BüAeV*, *GAeSO* e *KAeG SG* sottolineano che l'archivio di documenti per i dati registrati dal paziente deve assolutamente essere tenuto separato da quello dei professionisti della

[149] FR, NE, GE, VS, VD, JU
[150] FR, NE, GE, VS, VD, JU
[151] FR, NE, GE, VS, VD, JU

salute e delle strutture sanitarie, in modo che i relativi documenti possano essere chiaramente distinti già in base al luogo di archiviazione e garantire così la sicurezza di trattamento. Alla stessa stregua di *HIN* desiderano aggiungere al numero 10.1.1: «bereitstellen, die von den Dokumentenablagen für die Gesundheitsfachpersonen und Gesundheitseinrichtungen getrennt sind». *KSSG* ricorda che una separazione degli archivi per i documenti registrati dal paziente e quelli inseriti dai professionisti della salute raddoppia i costi di manutenzione, licenza ed esercizio di un repository. La separazione può avvenire anche a livello logico. Il numero 10.1.1 deve essere stralciato. 6 Cantoni[152] criticano l'imprecisione della traduzione al numero 10.1.1 e chiedono la seguente rettifica: «[…] des lieux de stockage dédiés […]» In riferimento al numero 10.1.2 desiderano invece la seguente modifica: «[…] à aucun effacement». OFAC chiede per il numero 10.1.2, perché i dati non sono soggetti alle stesse disposizioni del numero 2.1.1.1. Una conservazione abusiva crea rischi inutili e viola il principio di proporzionalità della LPD.
10.1.3 / 10.1.4: In riferimento al numero 10.1.3, *BFH* osserva che 2 GB sono tanti se si tratta di un testo, ma pochi quando si devono registrare dati vitali e pochissimi quando si devono caricare delle immagini. Lo spazio oggi di solito disponibile è piuttosto 10 GB e non 2 GB. Si dovrebbe pertanto parlare di consuetudini di mercato o almeno di 10 GB di spazio di memoria. *PharmaSuisse* ritiene insufficienti 2 GB e propone come minimo 5 GB, come abitualmente avviene nei servizi di cloud gratuiti. 17 partecipanti[153] considerano i 2 GB di memoria arbitrari e chiedono di stralciare tale disposizione e sostituirla con una regola generale e astratta nell'OCIP, secondo la quale la cartella informatizzata del paziente debba offrire lo spazio necessario per archiviare i documenti rilevanti dei pazienti. 6 Cantoni[154] osservano che 2 GB sono totalmente insufficienti per coprire le esigenze di alcuni pazienti e propongono di riformulare il numero 10.1.3 come segue: «Les communautés doivent garantir et s'organiser pour fournir un espace de stockage correspondant au besoin». Il numero 10.1.4 deve essere inoltre stralciato.

10.2 Archiviazione offline dei documenti e metadati

Posta e *VAKA* scrivono che le regole sulla reimportazione di documenti sembrano non avere un vero «use case», ma generano costi relativamente elevati, poiché questa tecnologia non è ancora disponibile, ma sicuramente sarà molto onerosa. Il numero 10.2 deve essere stralciato. OFAC chiede quale sia lo scopo di queste disposizioni e se siano gratuite. Osserva inoltre che sarebbe inutilmente rischioso se un paziente mal informato mettesse il suo archivio offline, su un cloud di mercato.

Posta ritiene che se si vuole promuovere l'interoperabilità, si deve anche specificare come devono essere i formati. Il numero 10.2.1 deve essere stralciato oppure precisato. *BFH* chiede se per dati riferiti ai pazienti s'intendano qui solo i dati amministrativi oppure anche quelli terapeutici. Si ricorda che non sono stati ancora definiti dei formati d'interoperabilità a riguardo, almeno se per «interoperabilità» non s'intenda un PDF. È quindi opportuno specificare di quale dati riferiti ai pazienti si parli. *Economiesuisse* e *SBC* suggeriscono di applicare il numero 10.2.1 a tutti i dati dei pazienti e non solo a quelli registrati dai pazienti, che sono invece già disciplinati al numero 10. Eventualmente si dovrebbe modificare il titolo del numero 10 nel modo seguente: «[…] oder Patienten und Gesundheitsfachpersonen erfassten […]». *HIN* dichiara che in analogia al numero 3.4.1.2 si può partire dal presupposto che l'esigenza di cui al numero 10.2.1 sia sufficientemente soddisfatta se i formati non accettati non possono neanche essere introdotti nel sistema.

SCH segnala che l'ordinanza non prescrive formati o transazioni e che quindi lascia un grande spazio di manovra per le implementazioni proprietarie, le quali potrebbero però rivelarsi estremamente onerose per l'importazione sistematica. IHE definisce già nel framework tecnico (ITI-32 Portable Media Creator e Importer) gli attori, le transazioni e i formati per l'importazione e l'esportazione di dati dai registry e repository nelle comunità conformi all'IHE. Le specifiche si riferiscono ai relativi «use case» nel campo di DICOM e nei punti essenziali rinviano allo standard DICOM. La specifica IHE descrive già anche il calcolo dei valori hash dei dati e documenti al fine di garantirne l'integrità e lo stato originale. *SCH* chiede di modificare i tre numeri sotto 10.2 per fonderli in due numeri: «Gemeinschaften müssen den Patienten

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

und Patientinnen die Möglichkeit zum Export und Import der Daten und Dokumente ihres elektronischen Patientendossiers im interoperablen elektronischen For-mat gemäss IHE iti-32 zur Verfügung stellen; 10.2.2 Stammgemeinschaften müssen mit den in IHE iti-32 definierten Verfahren sicherstellen, dass Daten, die erneut im elektronischen Patientendossier verfügbar gemacht werden sollen, unverändert geblieben sind.»

K3 e *VZK* considerano impossibile realizzare in pieno quanto richiesto ai numeri 10.2.2 e 10.2.3, poiché i pazienti possono scaricare, cancellare e ricaricare documenti modificati. I due numeri devono essere pertanto stralciati. Sempre riguardo a questi due numeri, anche 6 Cantoni[155] affermano che non è possibile stabilire se i dati sono stati modificati se non si dispone di un sistema che per ogni documento genera una tracciabilità integrale, cosa irrealizzabile. Chiedono pertanto lo stralcio dei numeri 10.2.2 e 10.2.3. *Integic* chiede maggiori dettagli per i numeri sotto al 10.2 perché potrebbero dar adito a malintesi. In particolare il 10.2.3 potrebbe rivelarsi problematico ad esempio per i risultati della diagnostica per immagini (DICOM). L'archiviazione offline deve riferirsi sempre a tutta la cartella. Quando un partecipante esce da una comunità, il paziente non deve preoccuparsene. La comunità di riferimento può eventualmente riprendere i dati archiviati. *KSSG* osserva che una tale verifica non è attuabile sui profili IHE esistenti. Se un documento viene nuovamente registrato, viene emessa anche una nuova Unique Document ID, che servirà alla registrazione. La duplicazione dei documenti (verifica del hash, ecc.) non è una funzionalità IHE e di conseguenza *KSSG* chiede lo stralcio del numero 10.2.3. OFAC vuole una spiegazione sul senso di «disposition une nouvelle fois».

11. Punto di contatto per i pazienti (art. 19 OCIP)

CMC, *BüAeV*, *GAeSO* e *KAeG SG* si rallegrano della creazione di un service-desk per i pazienti, ma criticano che non sia ancora stato deciso chi debba sostenere i costi per tale servizio. Il service-desk non deve generare costi supplementari per i professionisti della salute, poiché l'introduzione della cartella informatizzata del paziente sarà già di per sé onerosa per questa categoria professionale. In riferimento al numero 11.1.1, *VGIch* scrive che valgono le stesse esigenze di verbalizzazione dei punti di contatto dei professionisti della salute. Si constatano delle lacune e imprecisioni nell'ordinanza. È necessario garantire la continuità. Gli accessi devono essere verbalizzati da tutti. Il partecipante aggiunge che il segreto professionale medico è una disposizione penale che non può essere sostituita da un «analogen Vereinbarung» come stabilito al numero 11.1.2.2. Riguardo al numero 11.1.2.4, *VGIch* suggerisce inoltre la seguente modifica del testo: «[…] Einwilligung der jeweiligen Patienten erfolgen können […]». Sulla stessa falsariga, *Medgate* segnala un errore di contenuto e propone la seguente correzione: «[…] Einwilligung der jeweiligen Patientin oder des jeweiligen Patienten erfolgen können […]. *Privatim* non capisce perché un professionista della salute debba dare il proprio consenso a un accesso a distanza sui terminali del paziente. Per questi accessi dovrebbe bastare il consenso del paziente. *BFH* chiede perché un professionista della salute debba essere informato se si procede a un accesso a distanza per motivi di supporto tecnico e se non sarebbe opportuno informare almeno anche il paziente. Nei metadati bisognerebbe inoltre aggiungere anche il ruolo di supporter.

12. Soppressione della cartella informatizzata del paziente (art. 20 OCIP)

Riguardo al numero 12.1.1, *OFAC* scrive che la cartella informatizzata del paziente deve essere soppressa solo in caso di revoca del consenso o di decesso. In caso di mancato utilizzo si devono distruggere solo i documenti, non la cartella informatizzata del paziente, né il NIP e neanche i dati registrati dal paziente che non sono soggetti a nessuna scadenza di conservazione secondo il numero 10.1.2.

12.2 Condizioni per la soppressione della cartella informatizzata del paziente (cpv. 1)

K3 e *VZK* dichiarano che la disposizione di cui al numero 12.2 è già contenuta nell'OCIP e può quindi essere tralasciata. Anche il Cantone *ZH* e *ZAD* la considerano superflua e ne chiedono lo stralcio. 6

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

Cantoni[156] ripetono il parere espresso sull'articolo 20 OCIP e chiedono lo stralcio del numero 12.2.1.2. In riferimento al numero 12.2.1.3, *SBC* vorrebbe sapere se il processo viene attivato anche quando il paziente dona i suoi dati alla ricerca o li trasferisce ai suoi eredi. Nello stesso contesto, *economiesuisse* afferma che i dati di pazienti deceduti dovrebbero poter essere esportati in modo da essere messi a disposizione della ricerca. A tal scopo è però necessario il consenso del paziente nelle sue direttive anticipate o quello dei suoi familiari. *SSIM* osserva che la soppressione immediata dopo il decesso non è ammissibile perché i dati dovrebbero essere accessibii eventualmente per motivi medico-legali. Si propone di consentire la soppressione solo dopo un periodo di attesa di p. es. 360 giorni.

12.3 Soppressione della cartella informatizzata del paziente (cpv. 2)

K3, *VZK*, il Cantone *ZH* e *ZAD* ribadiscono il parere espresso sul numero 12.2 anche per il numero 12.3. *K3* e *VZK* osservano inoltre che la soppressione della cartella informatizzata del paziente non può essere affidata solo alla responsabilità della comunità di riferimento, ma deve essere disciplinata nello spazio di fiducia della cartella informatizzata del paziente. 6 Cantoni[157] affermano che in caso di soppressione della cartella informatizzata del paziente secondo l'articolo 20 OCIP, i dati non devono essere distrutti immediatamente, ma mascherati e resi inaccessibili. La cancellazione avverrebbe dopo 10 anni. Si dovrebbe quindi adeguare il numero 12.3 e aggiungerne uno sotto il numero 12.3 con il titolo «Masquage du dossier électronique du patient». *USB* domanda di verificare se la soppressione non possa/debba avvenire solo dopo un termine di transizione. I termini cancellazione/distruzione/soppressione dovrebbero poi essere chiariti e spiegati in tutte le ordinanze. *VGIch* considera poco chiaro il senso e lo scopo dell'obbligo d'informazione a tutte le comunità, come stabilito al numero 12.3.1.4. Se l'informazione è necessaria, dovrebbe essere l'UCC a informare – eventualmente in modo automatico – le altre comunità. Inoltre la revoca è valida di norma immediatamente. Ci si chiede come interpretare il termine adeguato previsto dall'articolo 20 OCIP. Anche le CTO riprendono la questione dell'adeguatezza, sebbene debbano contenere i requisiti tecnici e organizzativi per la certificazione e non un'interpretazione dell'ordinanza. Sarebbe consigliabile indicare una scadenza (p. es. un mese) nell'OCIP. *SBC* chiede da parte di chi debba avvenire l'informazione di tutte le comunità e comunità di riferimento. *KSSG* vorrebbe sapere come debba essere realizzata tale soppressione in tutte le comunità aderenti e ritiene che si debba creare un'informazione tecnica e quindi automatizzata. Si propone l'elaborazione di un apposito profilo IHE.

12.4 Widerruf der Einwilligung zur Führung eines cartella informatizzata del paziente (cpv. 2 lett. a)

6 Cantoni[158] criticano che il processo di revoca da parte del paziente attraverso il portale pazienti non è descritto al numero 12.4.1 e chiedono di aggiungere tale processo in questo numero. *Posta* osserva in merito al numero 12.4.1.2, che la revoca può avvenire anche per via elettronica e s'informa su come procedere. Chiede di adeguare tale esigenza. Al numero 12.4.2.1.2 vorrebbe invece sapere se un paziente debba presentarsi di persona per sopprimere la sua cartella informatizzata del paziente nel caso in cui non possa più utilizzare il proprio SID. Anche in questo punto è necessaria una modifica. Una disdetta scritta dovrebbe essere sufficiente.

12.5 Chiusura in caso di non utilizzo (cpv. 2 lett. b)

6 Cantoni[159] rimandano ai commenti fatti sull'articolo 20 OCIP e desiderano lo stralcio del numero 12.5. *SBC* chiede chi debba monitorare il requisito di cui al numero 12.5.1. *VGIch* vorrebbe aggiungere al numero 12.5.1.1 quanto segue: «[…] Aufhebung darüber nachvollziehbar informiert wird».

[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

3.2.3 Art. 3 Metadaten (allegato 3)

Art. 3	Metadaten
Die Metadaten nach Artikel 9 Absatz 3 Buchstabe b OCIP sind in Anhang 3 festgelegt.	

Articolo 3: 6 Cantoni[160] vorrebbero sapere qual è il collegamento con l'elenco dei metadati stilato da eHealth Suisse in collaborazione con i Cantoni, per esempio con la lista di documenti classificati in base ai codici LOINC. Chiedono di riprendere tale lista già tradotta e impiegata da diversi anni nei Cantoni, perché già armonizzata con le prassi internazionali.

Allegato 3

1.1 Ruolo dell'autore: *BFH* fa notare che con il 40999 «Andere» si può coprire molto, ma che sarebbe utile riflettere sul ruolo degli amministratori, supporter o altre persone che, p. es. come fornitori di servizi, creeranno in futuro una cartella, forse anche al di fuori di un percorso terapeutico concreto, per permettere ai cittadini di caricare i loro dati lifestyle o documenti più vecchi. *ChiroSuisse* osserva che nel codice nazionale 40003 la designazione tedesca è sbagliata e deve essere corretta con «Chiropraktor» (e non «Chiropraktiker»). *ASI*, *SWOR* e *FSAS* criticano che il termine «Therapeutin / Therapeut» (codice nazionale 40011) venga impiegato come nome generico per diverse professioni. Sarebbe opportuno riportare i titoli professionali completi. *FMH* ritiena sbagliata la traduzione tedesca di «Social Worker» (codice nazionale 40010), che dovrebbe essere sostituita dalla designazione corretta di tale professione «Sozialarbeiter FH». Per «Complementary therapist» (codice nazionale 40006) s'intendono inoltre coloro che operano nella medicina alternativa non medica e si dovrebbe pertanto utilizzare il titolo professionale riconosciuto in Svizzera secondo l'OML MA e OML TC . Il Cantone *BS* chiede se «Case Managerin» / «Case Manager» sia contenuto nel «Social Worker» (codice nazionale 40010). Dai metadati dovrebbe emergere a quale struttura sanitaria appartiene il «Case Managerin / «Case Manager». Il Cantone *ZH* e *pharmaSuisse* sarebbero favorevoli a suddividere il ruolo di «Pharmacist» (codice nazionale 40001) come avvenuto al numero 1.2 Code 50045/50046 in «Retail pharmacist» e «Hospital pharmacist», visto che queste due figure professionali sono molto diverse.

1.2 Specializzazione medica dell'autore: *KSSG* segnala che bisognerebbe aggiungere la specializzazione in oncologia non riportata nell'elenco. La radio-oncologia non è analoga. *HÄ CH* e *ÄTG* criticano la suddivisione troppo differenziata, che dovrebbe invece essere semplificata. Solo per gli infermieri vi sono 6 possibilità di scelta. *SMCF* osserva che la lista delle specializzazioni mediche dovrebbe basarsi sull'allegato 1 dell'ordinanza sulle professioni mediche (OPMed) e dovrebbe inoltre contenere la designazione di «médecin praticien». *PharmaSuisse* evidenzia che il termine «Pharmacologist» (codice nazionale: 50040) significa farmacologo e che esistono farmacologi medici e farmaceutici. Se il codice deve essere utilizzato esclusivamente per i medici, consiglia di modificare il termine inglese p. es. in «Medical Pharmacologist». Chiede inoltre di adeguare le attuali designazioni dei codici nazionali 50045 e 50046 in «Retail Pharmacist FPH» («Apotheker FPH in Offizinpharmazie») e «Hospital Pharmacist FPH» («Apotheker FPH in Spitalpharmazie»). Consiglia anche di aggiungere i termini «Clinical Pharmacist FPH» («Apotheker FPH in klinischer Pharmazie») e «Pharmaceutical administrative assistant» («Pharma-Betriebsassistentin»). Il Cantone *BS* scrive che alcuni termini non sono consueti in inglese (p. es. «Allergist») e propone se del caso di modificarli. Poiché manca la specializzazione in medicina di laboratorio, sarebbe inoltre opportuno valutare se aggiungere «Specialist for laboratory medicine». Ci si chiede se non specificare ulteriormente le formazioni relative a «specialized nurse» (codice nazionale 50065), indicando la specializzazione del personale infermieristico come specializzazione a sé stante. *ASI*, *SWOR* e *FSAS* chiedono una formulazione neutra delle specializzazioni mediche e non una combinazione fra designazione professionale e specializzazione medica (p. es. ruolo: medico, specialità generale: ginecologia). I suddetti partecipanti vorrebbero inoltre che le designazioni professionali infermieristiche (codice nazionale da 50062 a 50068) vengano elencate sotto il ruolo.

1.3 Stato di disponibilità del documento: *BINT* e *Integic* lamentano la mancanza di indicazioni sul ciclo

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

di vita dei documenti e sulle correzioni nella cartella informatizzata del paziente. Il Cantone *ZH* desidera aggiungere le categorie supplementari «Patient Medication» per i documenti informatizzati della eMedicazione e «Vaccination Information» per i documenti della cartella di vaccinazione informatizzata. In merito allo stato di disponibilità del documento, il Cantone *BS* osserva che il termine «deprecated» è totalmente inusuale e incomprensibile. Il contrario di «approved» è «denied». Si dovrebbe valutare la possibilità di impiegare un termine più comprensibile. *VGIch* scrive che per ogni documento si dovrebbe garantire un versionamento e parlare di documenti «gültig» e «annulliert» In base ai metadati un documento può inoltre avere uno stato di disponibilità «genehmigt» e «abgelehnt». *VGIch* propone di chiarire la terminologia ed eventualmente semplificarla per una migliore comprensione.

1.4 Categoria di documento: *KSSG* dichiara che, a differenza di quanto finora pubblicato, s'impiegano di nuovo i codici nazionali. La categoria di documento dovrebbe corrispondere a una norma internazionale (ISO 13606). *LUKS* considera poco chiare le diverse distinzioni (p. es. 70006 e 70010) e chiede un manuale per l'utente al di fuori del diritto di esecuzione. *BINT* e *Integic* rilevano la necessità di un'attribuzione delle diverse combinazioni/intersezioni fra categorie/tipi di documenti e chiedono di completare o riformulare il punto. Riguardo alle categorie di documenti, *HÄ CH* e *ÄTG* scrivono che i documenti/formati di scambio attualmente in fase di sviluppo nell'ambito dell'eMedicazione, eVaccinazione ed eRTO dovrebbero essere ripresi nella lista e adeguati continuamente ai nuovi sviluppi. *PharmaSuisse* raccomanda di aggiungere le categorie «Patient Medication» (Medikation des Patienten) per i documenti informatizzati dell'eMedicazione e «Vaccination Information» (Impfdaten) per i dati della cartella di vaccinazione informatizzata. *FMH* scrive che le categorie 70001 e 70002 potrebbero essere raggruppate in una sola categoria 70007/2 «Verlaufseintrag». Poiché la distinzione fra 70009 e 70013 è poco palese, propone di fondere anche queste due categorie in una sola intitolata «Meldungen/Warnungen» *BFH* vorrebbe sapere se la prescrizione medica (60005) rientra nella categoria 70012. Sarebbero necessarie delle spiegazioni, eventualmente anche un elenco aggiornato dei documenti CDA standardizzati contenuti nel biotopo della cartella informatizzata del paziente, con un riferimento a quale categoria e tipo di documenti essi appartengono (numero 1.12).

1.5 Grado di riservatezza: *SQS* osserva che il grado di riservatezza con il codice 30002 dovrebbe essere uguale in tedesco e in inglese, al contrario di quanto avviene attualmente. Il Cantone *BS* segnala al grado di riservatezza 30005 che «secret» significa segreto e suggerisce di utilizzare eventualmente il termine «protected data».

1.6 Formato del documento: 7 partecipanti[161] si chiedono se l'elenco sia veramente completo. Sembra impossibile che la cartella informatizzata del paziente possa essere composta solo da questi 3 tipi di documenti. Chiedono pertanto che vengano supportati almeno i formati di scambio ufficiali. Per referti di laboratorio nel processo di trapianto di organi si avrebbe così p. es. urn:che:epd:2.16.756.5.30.1.1.1.1.3.4.1. I suddetti partecipanti propongono inoltre che l'elenco dei tipi di documenti possa essere curato anche dall'UFSP, senza bisogno di una nuova ordinanza. I formati di scambio per la prescrizione medica elettronica e il rapporto informatizzato di dimissione sono già in cantiere e dovrebbero essere ripresi subito nel testo dell'atto normativo. IG *eHealth* e *Posta* fanno notare che il termine francese «Format du document» si riferisce alla forma del documento e non al suo contenuto. Questo significato di formato è stato impiegato in particolare nell'allegato 6 §3 (Indikatoren) e nelle CTO al numero 2.2.1.3. Chiedono di utilizzare un termine appropriato (p. es. Austauschformat - formato di scambio) e d'impiegare in tutti i testi una terminologia ben definita e coerente. In merito al formato dei documenti, *HÄ CH* e *ÄTG* vorrebbero sapere se non vi dovrebbero rientrare anche i documenti di eMedicazione ed eRTO. *SSIM* e *LUKS* propongono di inserire anche altri tipi di documenti (p. es. i valori di laboratorio nel processo di trapianto di organi).

1.7 Tipo di struttura sanitaria: *Medgate* critica che l'attribuzione dei fornitori di servizi di telemedicina sia poco chiara e propone di creare un codice apposito per gli istituti di telemedicina. *PharmaSuisse* suggerisce di tradurre il codice 20009 «Pharmacy» con il termine tedesco «Öffentliche Apotheke». Secondo il Cantone *BS,* il termine «private» al codice 20004 «private home-based care» si riferisce alla forma di

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

finanziamento e non dovrebbe trovarsi quindi in questo punto. Si dovrebbe utilizzare il termine «home-based care». La parola inglese «nursing home» (codice 20008) significa casa di cura e dovrebbe essere sostituita con un corrispondente inglese più preciso per il termine tedesco «sozio-medizinische Institution». *SCH* propone di riprendere «Telemedizin» negli OID nazionali. *FMH* esprime i seguenti commenti: codice 20001, utilizzare: «Systematische Auflistung der diagnostischen Institute» oppure il concetto generico di «diagnostische Institute»; codice 20002: traduzione: «Notfallstation»; codice 20004: designazione: «Spitex»; codice 20010: precisare medico/non medico; codice 20012: traduzione sbagliata.

1.8 Lingua del documento: *HÄ CH* e *ÄTG* osservano che gli ambulatori medici ricevono spesso delle cartelle mediche provenienti dagli Stati di origine dei loro pazienti (p. es. Turchia) e che sarebbe quindi opportuno prevedere almeno una categoria «other». *HL7*, *IHE* e *BINT* rilevano che dovrebbero essere ammessi anche i codici «de», «fr», «it», «en» (senza –CH o –US). Propongono di evitare le estensioni nazionali o almeno autorizzare anche i codici senza estensione nazionale. *IG eHealth* e *Posta* considerano inopportuno dichiarare che l'elenco sia esaustivo e chiedono come gestire il caso di un paziente che vuole caricare un documento in un'altra lingua. L'elenco deve essere definito come esempio o requisito minimo. Il seguente elenco viene impiegato nel settore sanitario: riferimento a OID 1.0.639.1[162]. *Posta* aggiunge a riguardo che dovrebbero essere autorizzati i Codici per la rappresentazione dei nomi delle Lingue ISO.

1.9 MIME Typ del documento: 14 partecipanti[163] osservano che l'elenco deve essere corretto perché contiene doppioni e quindi dati ridondanti. *HL7*, *IHE*, *medshare* e *Integic* propongono di aggiungere all'«application/pdf» l'obbligo di utilizzare il PDF/A, come previsto anche nelle prescrizioni dell'archivio federale[164] e di ELGA[165]. Tutti i file PDF incorporati nei documenti ELGA-CDA dovrebbero inoltre corrispondere allo standard PDF/A-1a (secondo «ISO 19005-1:2005 Level A conformance»). Secondo IG *eHealth* e *Posta* l'elenco dei formati di documenti è molto restrittivo. Mancano inoltre dei formati molto diffusi (p. es. PNG) e anche la definizione dei formati è poco precisa. TIFF è supportato, ma non si definisce quale estensione debba essere supportata. I due partecipanti chiedono di formulare l'elenco dei formati come requisito minimo. Il Cantone *ZH* vorrebbe aggiungere altri formati. *BFH* chiede perché si sia preso in considerazione solo il CDA Level 1. Nella sua osservazione, *USB* illustra fra l'altro il formato STL e suggerisce d'inserirlo come tipo di documento nella tabella MIME.

1.10 Specializzazioni mediche dei dati registrati nel documento: *KSSG* ribadisce il parere espresso al numero 1.2 «Specializzazione medica dell'autore». *ChiroSuisse* segnala che il termine inglese al codice 10007 è sbagliato e chiede di sostituirlo con «Chiropractic». *PharmaSuisse* e il Cantone *ZH* propongono di inserire anche le specializzazioni «Pharmakotherapie (pharmacotherapy) e Patient Care (Betreuung chronisch kranker Patienten). *SSIM*, *LUKS* e *FMH* fanno notare che attraverso una combinazione delle specializzazioni mediche e del tipo di documento si otterrebbe un maggiore grado di libertà e una migliore raffigurazione dell'integrità referenziale e chiedono quindi di rielaborare in questo senso i numeri 1.10 e 1.12.

1.11 Sesso del paziente: *PharmaSuisse* ritiene che non sia necessario indicare il sesso per cercare e trovare un documento e che non bisogna quindi inserirlo nei metadati. Tale funzione di ricerca potrebbe inoltre essere utilizzata in modo abusivo. Propone pertanto lo stralcio del numero 1.11.

1.12 Tipo di documento: I Cantoni *GE*, *VS*, *VD*, *JU* e *FR* reiterano il parere espresso all'articolo 3 OCIP-DFI. *BFH*, *BINT* e *Integic* ripetono i commenti fatti al numero 1.4, mentre *SSIM*, *FMH* e *LUKS* quelli fatti al numero 1.10. *KSSG* dichiara che, a differenza di quanto finora pubblicato, s'impiegano di nuovo i codici nazionali. La categoria di documenti dovrebbe essere collegata ai codici LOINC internazionali.

[162] http://www.hl7.org/oid/index.cfm?Comp_OID=1.0.639.1

[163] BFH, HIN, HL7, IHE, medshare, Integic, K3, VZK, PharmaSuisse, ZH, SQS, LUKS, SSIM, FMH

[164] https://www.bar.admin.ch/bar/it/home/archiviazione/versamento-di-documenti/documenti-digitali.html

[165] 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

Riferendosi al suo parere sull'articolo 4 / allegato 4, *PharmaSuisse* suggerisce di aggiungere i seguenti tipi di documenti: eAbgabe-/Anwendungsdokument (Dispensation Record), Kommentar zur Medikation (eMedication comment) e Labordaten (Laboratory data). *Posta* scrive che, in base alle raccomandazioni di eHealth Suisse, ogni tipo di documento dovrebbe essere attribuito con precisione a una categoria di documenti. Purtroppo, però, l'attribuzione non è indicata (nessuna prescrizione / raccomandazione). Se ogni comunità o addirittura ogni professionista della salute dovesse fare una propria attribuzione, ne risulterebbero incoerenze negli scambi fra le comunità o all'interno delle comunità. *Posta* chiede quindi delle prescrizioni su come attribuire precisamente i tipi di documenti a una categoria di documenti. *STSAG* critica che al codice 60037 il termine «Progress Note» non corrisponde alla traduzione tedesca «Kurve» e propone «Verlaufsbericht Intensivstation». Il Cantone *BS* suggerisce di cambiare il termine inglese al codice 60006 in «Electronic prescription» e segnala che al codice 60027 la parola inglese è sbagliata: istologia si dice «histology» e non ogni istologia proviene da una biopsia. La citologia non è stata presa in considerazione e dovrebbe essere quindi inserita.

3.2.4 Art. 4 Austauschformate (Allegato 4)

Art. 4	Austauschformate
Die Austauschformate nach Artikel 9 Absatz 3 Buchstabe c OCIP sind in Anhang 4 festgelegt.	

Articolo 4: *BRH* scrive che i formati medici di scambio contengono proprio i dati che sono rilevanti per la cartella informatizzata del paziente e al centro del processo di scambio medico di dati. Di conseguenza, secondo il rapporto esplicativo, dovrebbero essere elaborati nell'ambito di processi che coinvolgono i diversi portatori d'interessi e non essere contenuti nel diritto d'esecuzione. Propone quindi di definire i formati di scambio (almeno i Minimal Data Set) direttamente nell'OCIP-DFI. *SSIM* osserva che i formati di scambio non sono ancora disponibili e secondo l'UFSP devono essere elaborati nel quadro di processi che coinvolgono i portatori d'interessi. Per ottenere un processo efficace ed efficiente con risultati duraturi, si suggerisce di coinvolgere precocemente i diversi portatori d'interessi. *PharmaSuisse* deplora che l'allegato 4 non esista ancora e sottolinea che i formati di scambio servono allo scambio d'informazioni fra i professionisti della salute. Più il professionista dispone di dati, meglio potrà ottimizzare la terapia, aumentando così la sicurezza per il paziente. Il suddetto partecipante si dice molto favorevole al fatto che solo il paziente possa definire, attraverso le autorizzazioni di accesso, quali documenti il professionista può vedere. In questo modo tutte le informazioni sono in linea di massima disponibili per tutti i professionisti curanti di ogni gruppo professionale. Si rallegra inoltre che l'allegato 4 venga elaborato nell'ambito di processi che coinvolgono i portatori d'interessi e venga ripreso nel diritto d'esecuzione mediante le future revisioni. L'allegato 4 deve essere ultimato al più presto e corrispondere alle consultazioni dell'IPAG. *HL7* e *IHE* scrivono che si sono stabiliti solo 4 formati e che gli oggetti informativi svolgono un ruolo fondamentale in questo contesto. Come *Bleuer* osservano che, nel caso della diagnostica per immagini, nei prossimi tempi rimarrà un unico Use Case: il paziente riceve le immagini, i referti ecc. su un CD/DVD corredato di viewer. Tali viewer sono in parte proprietari; anche se i dati sono disponibili in formato DICOM, non sono necessariamente compatibili con tutti i viewer. Si dovrebbe quindi avere la possibilità di conservare nella cartella informatizzata del paziente i CD/DVD con le immagini, i referti ecc. assieme ai relativi viewer, p. es. in un formato ZIP. Tale formato dovrebbe essere supportato perché ammesso nel DICOM (v. dettagli DICOM PS3.12). *VLSS* critica che sia stata lanciata l'indagine conoscitiva sull'OCIP e anche sull'OCIP-DFI, prima di avere concordato i formati di scambio. Anzi, questi ultimi non sono neanche oggetto della proposta. Approvando le suddette ordinanze si accetterebbe praticamente «a scatola chiusa» questo aspetto fondamentale dal punto di vista medico. *VLSS* conosce bene l'esempio di «caso interprofessionale» grazie alla consultazione svolta internamente da FMH, ma si stupisce della precisione dei formati di scambio previsti. Invece di limitarsi a quanto necessario e utile, tutti i professionisti della salute coinvolti nel trattamento devono inserire nella cartella informatizzata del paziente, oltre alla parte medica, lunghe storie cliniche per i campi Problemi, Anamnesi, Terapie e Decorso. Si tratta di una prescrizione poco plausibile e irrealistica, che impedisce di focalizzarsi sull'essenziale e rischia di creare degli enormi cimiteri di dati che l'UFS, contrariamente al suo mandato legale, non sarebbe in grado di valutare perché troppo pochi pazienti vorrebbero una cartella informatizzata.

3.2.5 Art. 5 Integrationsprofil (allegato 5)

Art. 5	Integrationsprofile
Anhang 5 legt in Anwendung von Artikel 9 Absatz 3 Buchstabe d und e OCIP fest:	
a.	die Integrationsprofile;
b.	die nationalen Anpassungen der Integrationsprofile;
c.	die nationalen Integrationsprofile.

Articolo 5: Il Cantone *NE* si associa in questo punto al commento del Cantone *FR* sull'articolo 1 OCIP-DFI. *H+* si rallegra che il DFI si avvalga di standard tecnici riconosciuti a livello internazionale e utilizzati da tempo anche in Svizzera. L'importante è che alle comunità e comunità di riferimento non venga impedito, a causa della loro forma giuridica, di partecipare alle piattaforme di scambio di dati esistenti nell'ambito dell'eGovernment.

Allegato 5a

I Cantoni *GE*, *VS*, *VD*, *JU* und *FR* affermano di non avere le competenze per pronunciarsi su questo allegato, che deve essere validato da IHE Suisse. OFAC si affida a IHE Suisse per la standardizzazione e la documentazione dei profili d'integrazione. Anche *KSSG* ha fiducia nel parere di IHE Suisse e HL7. Il Cantone *SG* rimanda alla verifica da parte di IHE Suisse e HL7 e aggiunge che mancano dei profili d'integrazione che definiscono la cancellazione attraverso le comunità. Secondo *LUKS* è importante che il diritto d'esecuzione della LCIP sia al passo coi tempi in campo tecnico. È quindi opportuno tenere conto e autorizzare i futuri sviluppi dello standard FIHR di HL7. IHE Suisse e HL7 dovranno essere consultati per un'ulteriore valutazione e rielaborazione. IG *eHealth* e *Posta* dichiarano che questa disposizione non ha senso. I profili IHE definiti sono previsti in parte per l'impiego in un Affinity Domain e in parte per l'impiego «Cross Community». Il legislatore ha stabilito che la legge disciplina il settore fra le comunità e quindi non ha senso definire dei profili che sono destinati a essere utilizzati esclusivamente all'interno di Affinity Domain. Non è inoltre chiaro come si debba interpretare l'elenco dei profili. Ogni sistema che vuole partecipare alla comunità deve supportare tali profili? È quindi vietato integrare una soluzione che trasmette messaggi di HL7 mediante File Transfer? Queste disposizioni possono essere oggetto di audit e generano pertanto dei costi, che devono essere invece evitati. *IG eHealth* e *Posta* propongono di distinguere, nella formulazione dei profili, fra MUST (deve) e SHOULD (dovrebbe). *Integic* scrive a riguardo: «1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption»: RESTful- ATNA è un nuovo Supplement for Trial Implementation e dovrebbe pertanto essere ripreso (Add RESTful Query to ATNA - Published 2015-08-07)[166]. Accanto alla soluzione proposta tramite estensione nazionale, è disponibile anche una soluzione con IHE RESTful-ATNA. *SSIM* e *SBC* osservano che i fornitori di componenti informatici dovrebbero registrarli (omologazione). La registrazione dei sistemi informatici dovrebbe inoltre essere completamente separata dalla certificazione delle comunità. Tale modo di procedere permetterebbe di ridurre notevolmente i costi di certificazione delle singole comunità, poiché i componenti tecnici sarebbero già registrati; ci sarebbe una ripartizione chiara delle responsabilità fra fornitori di componenti informatici e comunità, si otterrebbe un mercato aperto per i componenti tecnici, si semplificherebbe il processo di acquisto da parte della comunità, si promuoverebbe un'infrastruttura «best of breed», che non sarebbe un ecosistema chiuso di un solo fornitore, e si conferirebbe così uno stimolo a tutto il settore. *SSIM* e *SBC* propongono di far sì che la certificazione di una comunità, la quale impiega componenti registrati, non debba ripetere la procedura di registrazione dell'infrastruttura tecnica, ma si limiti a certificare solo i processi organizzativi e le misure di protezione dei dati. *SSIM* sostiene inoltre le proposte di IHE Suisse. *HIN* considera molto utile la panoramica e la breve descrizione sotto forma di tabella. *Medshare* è a favore della soluzione attraverso i profili d'integrazione. *FMH* chiede invece ancora lo stralcio, perché si oppone a una regolamentazione a livello di ordinanza.

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

Allegato 5b

1.1 Definitions of terms

Posta e *IG eHealth* scrivono quanto segue riguardo al numero 1.1:

1.1.1: - La formulazione «may» è in contraddizione con l'obbligo di documentazione per i professionisti della salute. È preferibile la seguente redazione: «Healthcare professionals must save this data».
- Riguardo al brano di frase «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. Aspettative sbagliate possono creare grossi problem. Proposta: Clarify the formulation and make sure that the proper emphasis is made.
- Riguardo al brano di frase «view their data»: The emphasis could be improved. Proposta: 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. Proposta: change the terminology.
- Riguardo alla 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.

1.1.3: - 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 (NAVS13) with the electronic patient dossier-NIP. This statement is unclear. The community must provide the NAVS13 to the UCC (OCIP 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 NAVS13 for patient matching. Proposta: delete this statement or clarify the statement so that it complies with the laws. Tale chiarimento ha un effetto diretto sull'applicazione.
- Riguardo al brano di frase «the gateways may correlate»: Why is it not must? Some transactions like patient discovery mandate the use of the electronic patient dossier-NIP as the only identifier. Proposta: sostituire «may» con «must», altrimenti si potrebbero riscontrare dei problemi di compatibilità.

HIN dichiara in riferimento al brano di frase «Primary Systems may correlate their local patient identifier with the MPI-NIP» che probabilmente per «Primary Systems» s'intendono i sistemi primari delle strutture sanitarie. Se tale ipotesi è corretta: al 2.11.1 allegato 2 (CTO) c'è scritto fra l'altro che il NIP non viene collegato direttamente e in modo permanente con i documenti dei pazienti. Questa affermazione nelle CTO sembra essere in contraddizione con quanto affermato in questo punto e dovrebbe quindi essere chiarito. Anche il termine «HIS» non è spiegato. Potrebbe trattarsi del «Hospital Information System». Questo termine deve essere ripreso nel glossario.

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

BINT e *medshare* fanno notare che, oltre alla soluzione proposta dell'estensione nazionale, è disponibile anche la soluzione con IHE RESTful-ATNA. RESTful-ATNA è un nuovo Supplement for Trial Implementation, che dovrebbe essere ripreso. In questo ambito si indica anche un Wiki-Link[167]. Mentre *BINT* fa riferimento anche a un documento su RESTful-ATNA del 07.08.2015[168], *medshare* indica un documento in data 27.05.2016[169]. *Posta* scrive quanto segue: 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

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

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* segnala che l'Actor Document Consumer non agisce come query in direzione dell'Audit Record Repository, ma solo come scrittura nel senso di Record Audit Event (ITI-20) Transaction. Un Audit Record Repository non è un componente attore capace di supportare XDS-b. Il workflow nella forma descritta non è conforme a IHE. Si raccomanda una precisazione o uno stralcio poiché un ITI-18 e un successivo ITI-43 da Doc Consumer a ARR non corrisponderebbe ai profili IHE menzionati. *HL7* e *IHE* scrivono: 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. Chiedono lo stralcio. *Posta* e *IG eHealth* dichiarano quanto segue in riferimento al numero 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 aggiunge su questo punto: 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. *Integic* fa notare riguardo al numero 1.4.2.2 che è indicata solo l'Actor Secure Application. Soprattutto le comunità e i raggruppamenti di registry e repository devono essere indicati come Secure Node e si dovrebbe aggiungere qui l'attore. *HL7* e *IHE* desiderano la seguente riformulazione del brano di frase «These actors […] ATNA Audit Repositories» al numero 1.4.2.3: «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». Riguardo al numero 1.4.2.4.1, rilevano che non si debba prescrivere come effettuare la richiesta di audit interna alla comunità. Si potrebbe p. es. utilizzare anche IHE RESTful ATNA. Al numero 1.4.2.5 chiedono inoltre lo stralcio del primo, del terzo e del quarto trattino dei quattro riportati nel testo.

1.4.3: *Integic* rileva che ITI-57 può modificare solo il ConfidentialityCode, sollevando quindi perplessità sul versionamento. Si dovrebbe consentire la soppressione di un documento nella cartella informatizzata del paziente, visto che secondo la rappresentazione dei cicli di vita dei documenti (vedi ITI-41 RPLC) è contenuto nel Document Registry. IG *eHealth* e *Posta* chiedono quanto segue per il numero 1.4.3.2: instead of UUID this should read documentUniqueId. Riguardo al numero 1.4.3.1.2 aggiungono: «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: Riguardo all'AuditMessage/ActiveParticipant, *Integic* consiglia d'introdurre come 1.1 mandatory Element non solo l'UserID, ma anche un nome leggibile della persona attiva in modo da proporre una verbalizzazione comprensibile per il paziente. *HIN* rileva che il GLN al numero 1.4.4.1.1 deve essere definito come obbligatorio, mentre nell'ordinanza (articolo 24 OCIP) la trasmissione è facoltativa (può). Sembra essere una contraddizione. Vi sono dei casi nei quali il GLN non è ancora definito. Si propone di mettere ovunque un obbligo, un «MUST» per i GLN. Ne consegue che gli ambulatori devono disporre di un GLN prima di poter aderire a una comunità. *Posta* e *IG eHealth* scrivono riguardo al numero 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. Proposta: Remove MUST requirement to store audit event data in a pre-defined format. Sul numero 1.4.4.1.1 osservano: 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. Proposta: remove the Swiss national extension.

1.5 Requirements on PIXv3 for Patient Identity Feed

Posta e *IG eHealth* scrivono riguardo a OtherIDs: From the documents of EPDV storing the electronic patient dossier-NIP 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

Riguardo al numero 1.7.2.1.1, *Posta* e *IG eHealth* richiedono un chiarimento: 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

Posta e *IG eHealth* illustrano un caso nel loro parere e domandano come debba essere risolto. Chiedono inoltre quanto segue: An example for patient matching across communities should be provided. Sul numero 1.8.2 commentano: 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 ribadisce il parere espresso sul numero 1.4.4.1.1 anche per i numeri 1.9.5.1.1 e 1.9.5.1.2.

Allegato 5c

1 Introduction

KSSG chiede riguardo all'impiego di XDS-I, se il DICOM WADO Service rientri nella certificazione. Questo farebbe parte dei sistemi primari se nel XDS Repository si registra solo il KOF. Chiede inoltre se i portali per i pazienti debbano supportare un apposito DICOM Viewer, che sappia gestire WA-DO (Akteur Imaging Document Consumer), e se ciò è rilevante per la certificazione. Tutto il settore XDS-I per lo scambio di file con immagini non è stata considerato nelle CTO ed è quindi opportuno verificare l'OCIP e le CTO secondo il requisito di IHE XDS-I. *Posta* e *IG eHealth* scrivono in riferimento al brano di frase

«It has been specified for the Document Registries to act as Policy Enforcing Service Providers in terms of a XACML PEP» quanto segue: 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.
Essi ritengono inoltre che questo tipo di prescrizioni rende difficile l'attuazione di soluzioni proprie dei diversi fornitori. IG eHealth propone: Do not specify HOW something must be implemented. Specify the desired result instead.

2 Volume 1 – Integration Profiles

IG eHealth e *Posta* scrivono riguardo al numero 2.2 quanto segue:
- 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. Proposta: 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. Proposta: 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-NIP: This assumes that there will never be any cross-patient use cases. This appears to be not very future proof. Proposta: Do not require org text and org ID attributes for patients. Drop electronic patient dossier-NIP as resource attribute.
Per *Integic* la durata di validità di 10 minuti è troppo breve per la prassi e dovrebbe essere prolungata a 30 - 60 minuti. Riguardo al numero 2.3.2, *Posta* e *IG eHealth* segnalano: 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 e *Posta* osservano riguardo al numero 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. Questo ha ripercussioni dirette sull'implementazione e la performance. Proposta: Drop the attribute. Esprimo inoltre il seguente parere sul numero 3.1.5: 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. Anche questo ha ripercussioni dirette sull'implementazione e la performance. Proposta: Add trigger event «RetrieveDocumentSetRequest». *Integic* segnale riguardo al numero 3.1.6.1 che «ADR due to XDS Register Document Set-b» dovrebbe essere il numero 3.1.6.2. IG *eHealth* e *Posta* osservano sul numero 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* evidenzia riguardo al numero

3.3 che manca il formato di scambio tecnico sulla Policy, che viene scambiato con CH:PPQ, e che deve quindi essere specificato. Riguardo al numero 3.3.9, *Integic* propone di correggere «ACMLPolicyQuery Response» in «XACMLPolicyQuery Response».

3.2.6 Art. 6 Evaluation (allegato 6)

Art. 6 Evaluation
Gemeinschaften und Stammgemeinschaften müssen dem BAG für die Evaluation nach Artikel 21 Absatz 2 OCIP die Daten nach Anhang 6 zur Verfügung stellen.

Articolo 6: 6 partecipanti[170] desiderano completare questo articolo con la prescrizione che le comunità devono fornire i dati all'UFSP solo in forma anonimizzata. Dai dati contenuti nell'allegato 6 risulta che ciò è sufficiente per le valutazioni previste. Si suggerisce d'inserire un nuovo capoverso 2 con questo tenore: «Die Gemeinschaften und Stammgemeinschaften sind verpflichtet, die Daten vor der Weiterleitung an das BAG zu anonymisieren oder anonymisieren zu lassen». I Cantoni *GE*, *VS*, *VD* e *JU* chiedono di precisare i parametri richiesti: - il periodo preso in esame – in modo globale o per paziente – la frequenza – media – mediana – in cifre assolute, ecc. L'elaborazione di tali parametri genererà costi per le comunità i quali dovrebbero essere coperti dalla Confederazione. Il testo dovrebbe essere completato con l'indicazione dell'ordine di grandezza finanziario. *HL7*, *IHE* e *medshare* domandano di fissare la periodicità e i termini. *HIN* vorrebbe dei requisiti di reporting fattibili, in particolare il reporting dovrebbe avvenire su richiesta e non automaticamente. L'articolo 6 dovrebbe pertanto essere modificato come segue: «Gemeinschaften und Stammgemeinschaften müssen dem BAG auf Anfrage nach […]».*SSIM* sottolinea che i dati e i parametri sui dati di base, i diritti di accesso, i file, l'utilizzo e la protezione dei dati debbano essere limitati al minimo possibile e non sfruttati per controllare i fornitori di prestazioni. *Santésuisse* afferma che in vista della valutazione del raggiungimento dello scopo e dell'obiettivo della legge e dell'ordinanza secondo la LCIP (art.1 cpv. 3), nel rapporto esplicativo manca qualsiasi indicazione su come attuare concretamente tale valutazione. Le cifre contenute nell'allegato 6 non sono infatti a suo parere sufficienti a valutare la cartella informatizzata del paziente dal punto di vista del miglioramento della qualità del trattamento, dei processi terapeutici, della sicurezza del paziente, ecc.

Allegato 6

1. Dati di base: *OFAC* afferma che spetta agli ospedali e agli istituti di cui agli articoli 39 e 49a della legge federale sull'assicurazione malattie (LAMal) dichiarare la loro data di adesione, probabilmente all'UFSP. Questa informazione non ha nessuna pertinenza in un parametro di valutazione. *HIN* segnala che in alcuni casi la combinazione di età, sesso e domicilio non è abbastanza anonima e che l'anonimità del paziente deve essere invece garantita. Propone la seguente formulazione al secondo parametro: «[…] nach Alter, Geschlecht und Wohnort, wobei ein noch zu definierendes Clustering bei Gruppen kleiner als 7 anzuwenden ist». Richiede inoltre una spiegazione su cosa s'intenda per domicilio. *Posta* osserva che il parametro relativo a età, sesso e domicilio è già contenuto nei parametri del numero 1 e numero 2. Si deve correggere oppure cancellare il parametro in uno dei due punti.

2. Diritti di accesso: *HIN* e *Posta* ribadiscono il parere espresso sul numero 1. *SSIM* e *FMH* ritengono che i diritti di accesso siano irrilevanti e al contempo eccessivi per la valutazione. *SSIM* chiede una revisione. Secondo *STSAG,* il numero e il tipo di file per grado di riservatezza è irrilevante a livello di DFI e non corrisponde a un'adeguata valutazione dei parametri. La loro significatività è bassa e il margine di manovra risultante è incerto. Si dovrebbe evitare una raccolta inutile di dati. Lo stesso vale per il numero di professionisti della salute esclusi. Anche questo parametro dovrebbe essere eliminato. *LUKS* osserva che i diritti di accesso vengono decisi dai pazienti. Non è rilevante per la valutazione in quale misura i pazienti li limitano o li ampliano. Il paziente può vedere sul portale della cartella informatizzata se vi è stato un accesso di emergenza e chi l'ha effettuato. Il numero 2 deve essere modificato. *KSSG* fa notare che sembra relativamente difficile rilevare tali cifre visto che il punto 4.14.1.9 delle CTO vieta la memorizzazione dei dati relativi ai pazienti in ATNA e logfiles, ecc.

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

3. Files: Secondo *LUKS* il numero dei documenti registrati non dice nulla sull'utilità della cartella informatizzata del paziente. *SSIM* e *FMH* ritengono irrilevante ed eccessivo il numero di files per la valutazione. Anche *STSAG* è della stessa opinione e considera irrilevante il numero di files suddivisi per formati. *LUKS*, *SSIM*, *FMH* e *STSAG* chiedono lo stralcio di tale parametro. *Posta* segnala che il termine «Format» è già stato utilizzato per un altro scopo e dovrebbe essere sostituto da «MIMEType» secondo l'allegato 3, §1.6.

4. Impiego: *FMH*, *SSIM* e *LUKS* considerano questi dati irrilevanti per la valutazione e vedono nella loro rilevazione piuttosto un'intenzione di controllo. Ne suggeriscono pertanto lo stralcio. *KSSG* evidenzia che i parametri sull'impiego possono essere forniti solo parzialmente poiché alcuni attributi non fanno parte dei metadati. *HIN* scrive che qui s'introducono i termini «Dateiklasse» e «Datei-Art» e che «Dateiklasse» corrisponde probabilmente a «Dokumentenklasse» (cap. 1.4 nell'allegato 3) e «Datei-Art» a «MIME Typ des Dokuments» (cap. 1.9 nell'allegato 3). Se tale ipotesi è sbagliata, si richiede un chiarimento nel testo. *Posta* critica che nei parametri non si siano definiti i termini «Datei-Art» e «Dateiklasse» e chiede o di aggiungere una definizione o di impiegare i termini probabilmente corretti di «Dokumentenklasse» e «Dokumenten Typ» secondo l'allegato 3. Riguardo alla statistica sulla cancellazione dei dati, *Posta* afferma che il paziente non ha la possibilità di cancellare un documento, ma solo di modificare il grado di riservatezza. Gli indicatori devono pertanto essere stralciati. Riguardo all'ultimo parametro del numero 4, riferito al numero di accessi per paziente, *Posta* chiede quali dati debbano essere rappresentati (NIP, cognome, nome, …) o cosa venga anonimizzato. È necessaria una precisazione oppure lo stralcio. Secondo *STSAG,* non c'è bisogno di rilevare il numero dei professionisti della salute, poiché l'utilità è bassa e la significatività irrilevante nelle grandi strutture. È inoltre sufficiente la rilevazione da parte della comunità di riferimento. Anche le categorie e i tipi di dati sono poco significativi e quindi si dovrebbero sopprimere i parametri in questo contesto. Anche una lista degli accessi con riferimento temporale è troppo onerosa e poco significativa. Basta una rilevazione da parte della comunità di riferimento. Lo stesso vale per gli accessi dei pazienti (riferimento temporale e categorie e tipi di dati).

5. Protezione dei dati: Il Cantone *SG* chiede cosa viene considerato un reclamo e suggerisce di precisare il concetto.

3.2.7 Art. 7 Mindestanforderungen an das Personal (allegato 7)

Art. 7 Mindestanforderungen an das Personal
Die Mindestanforderungen an die Qualifikation des Personals nach Artikel 27 Absatz 4 OCIP, welches Zertifizierungen durchführt, sind in Anhang 7 festgelegt.

Articolo 7: *SSIM* fa notare che le condizioni di certificazione del personale sono molto severe. *SQS* ribadisce il parere espresso sull'articolo 27 capoverso 4 OCIP e chiede lo stralcio completo dell'articolo 7.

Allegato 7

Riguardo al numero 1.1.1, *SQS* osserva che le condizioni tecniche e organizzative che le comunità e comunità di riferimento devono soddisfare non presentano contenuti tali da richiedere conoscenze specifiche in materia d'informatica medica per poter garantire una verifica adeguata nell'ambito della certificazione. In base al rapporto esplicativo sulla LCIP, i requisiti in materia di competenze dei servizi di certificazione devono essere stabiliti secondo principi e procedure applicati a livello internazionale. Se si sceglie come standard la certificazione secondo l'ordinanza sulle certificazioni in materia di protezione dei dati (OCPD) le condizioni applicate al personale del servizio di certificazione sarebbero rette dall'OCPD, che disciplina nell'allegato i requisiti concernenti la qualifica del personale degli organismi di certificazione addetto alla certificazione. Anche nell'ISO/IEC 27006 (se si certifica in base all'ISO 27001) o nell'ISO 17021 si disciplinano le competenze del personale. Nel quadro del numero 1.1.5, *SQS* aggiunge che l'ISO/IEC 27006 diventa rilevante solo se si certifica in base all'ISO/IEC 27001. Anche in questo caso, i requisiti relativi alla qualifica del personale addetto alla certificazione risultano già dall'accreditamento. I numeri 1.1.1 e 1.1.5 devono essere stralciati. Riguardo ai numeri 1.1.1, 1.1.2,

1.1.3, 2.1.1, 2.1.2 e 2.1.3, *HIN* chiede 5 anni di esperienza professionale (al posto di 2) in assenza di una formazione specifica; 2 anni sono invece sufficienti in caso di formazione supplementare. *HIN* considera basso il numero concreto di anni di esperienza professionale richiesto nelle diverse discipline (informatica medica, protezione dei dati), ossia 2 anni di esperienza professionale o 1 anno di formazione. Per delle attività importanti come la certificazione in settori sensibili come i dati del paziente, si dovrebbero avere delle persone con maggiore esperienza. *HIN* si rallegra invece dell'obbligo di certificazione per gli ID-provider e le comunità. Secondo *SSIM*, *FMH* e *LUKS* i requisiti per i servizi di certificazione sono troppo elevati, così da pregiudicare la concorrenza e far lievitare i costi. Questi requisiti severi non consentirebbero di migliorare la sicurezza dei dati che, per esperienza, dipende più dal comportamento dell'utente che dalle misure di protezione tecnica. *Lovis* osserva che si debba garantire l'affidabilità e la responsabilità. Riguardo al numero 1.1.2, *OFAC* segnala un'incoerenza giuridica: le comunità amministrate dai Cantoni, saranno sottoposte, in qualità di organismi cantonali, al diritto sulla protezione dei dati del loro Cantone. Le disparità sono notevoli: nessun Cantone prevede nel suo diritto in materia di protezione dei dati l'applicazione di un sistema di gestione della protezione dei dati e ciò è in contraddizione con la LPD, l'OLPD e la dottrina dell'IFPDT sull'autoregolazione. Nessun Cantone prevede nel suo diritto in materia di protezione dei dati una procedura di certificazione. *OFAC* aggiunge di non essere direttamente interessata da questo allegato, ma desidera che i requisiti applicabili ai servizi di certificazione non divergano da quelli già in vigore e gestiti dal servizio di accreditamento svizzero (SAS).

3.2.8 Art. 8 Schutz der Identifikationsmittel (allegato 8)

Art. 8	Schutz der Identifikationsmittel
Die Vorgaben für den Schutz der Identifikationsmittel nach Artikel 30 Absatz 2 OCIP sind in Anhang 8 festgelegt.	

Articolo 8: *IG eHealth* scrive che è necessario dare la massima priorità alla semplicità e chiarezza per il paziente, perché un impiego difficoltoso rappresenta un ostacolo all'utilizzo della cartella informatizzata del paziente. Oltre ai necessari requisiti di sicurezza è quindi importante garantire la praticità con regole di base e preimpostazioni semplici. L'allegato 8 dovrebbe essere rielaborato. Per garantire il successo della cartella informatizzata del paziente è importante offrire SID sicuri e conviviali. L'esperienza dimostra che le smart card non sono ben accettate e che presentano grosse sfide in termini di compatibilità con l'infrastruttura informatica disponibile e in termini di processi di emissione. I sistemi come mTAN o le procedure che si avvalgono di meccanismi biometrici o comportamentali sono di fatto esclusi. È opportuno assicurare che i SID possano essere utilizzati negli ospedali, con un grado di protezione sufficiente e accettato a livello cantonale, anche per l'accesso alla cartella informatizzata del paziente. Sarebbe inammissibile dovere effettuare ulteriori investimenti in questo campo. Dove legalmente autorizzato, si dovrebbe inoltre evitare la duplice identificazione (SID) per gli accessi interni all'ospedale e un SID separato per l'accesso alla cartella informatizzata del paziente).

Allegato 8

1.2 TOE Overview

OFAC segnala che il termine «LDEP» è tradotto con «FLEHR», mentre «EPDV» non è stato tradotto in inglese e non vuole dire nulla in francese. O si rispetta una regola precisa e si traduce tutta la terminologia specifica della LCIP in inglese, o si traducono tutti i testi nelle lingue nazionali. Gli acronimi e le traduzioni della Confederazione, del DFI e dell'UFSP non sono inoltre omogenei in tutto il documento. Sia acronimi che traduzioni devono essere omogenei e se possibile tradotti nella lingua del documento. *Posta* osserva riguardo al numero 1.2.1, che la definizione del Target of Evaluation (TOE) non consente procedure biometriche né comportamentali per l'autenticazione. Senza questa modifica non si può utilizzare mTAN. Chiede di riprendere le definizioni dell'ISO 29115, capitolo 3.3, invece d'introdurre una definizione «Device». Riguardo al numero 1.2.2, rileva che il termine «identification means» è impiegato in modo sbagliato e che deve essere corretto. Gli «authentication means» sono degli strumenti per sbrigare il processo di autenticazione, mentre gli «idenfication means» servono a svolgere il processo

d'identificazione. Il termine «holder of the token» fa pensare che le procedure senza token siano di fatto vietate. Il termine «token» deve pertanto essere sostituito con «authentication factor» secondo l'ISO 29115. Dalla descrizione del TOE sembra risultare che vengano ammesse solo le procedure basate su IdP. Ci si chiede cosa avviene delle procedure che non necessitano di IdP. Il TOE deve essere formulato in modo tale da descrivere la procedura di autenticazione e quella attraverso IdP. Viene infine introdotto il termine «Context» che non è pertinente nell'ambito dell'autenticazione. L'autenticazione deve verificare che l'identità dichiarata sia corretta, mentre il contesto è una questione di autorizzazione. Non rientra nel campo di applicazione del presente documento sapere se l'Identity Provider necessita di tale contesto per scegliere la procedura di autenticazione più adeguata. Il riferimento al contesto deve quindi essere stralciato o considerato facoltativo. Riguardo al numero 1.2.2, *SCH* ritiene molto dettagliate le spiegazioni sul workflow per l'autenticazione, mentre viene descritto solo l'IdP-initiated Approach. Dovrebbero essere i produttori di applicazioni per la cartella informatizzata del paziente a decidere quale workflow preferiscono per l'autenticazione, IdP- o RP-initiated Approach. Anche i protocolli fra Relying Party e IdP nonché le procedure di autenticazione dovrebbero essere regolati dal mercato. Sarebbe inoltre più semplice per l'utente navigare prima sul portale della cartella informatizzata del paziente ed effettuare successivamente il login. Questo modo di procedere corrisponde meglio alle aspettative di molti utenti e aumenterebbe l'adesione del pubblico alla cartella informatizzata del paziente. *SCH* chiede di eliminare l'IdP-initiated Workflow per l'autenticazione. Si dovrebbero stabilire solo i presupposti e i risultati dell'autenticazione e non descrivere i passi per raggiungerla. *SCH* propone: 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

Posta segnala riguardo alla tabella 1 che le descrizioni sembrano autorizzare solo le procedure basate su smart card. Se non si modifica questo punto, non sarà più possibile avvalersi del mTAN o di altri mezzi senza smart card. Si richiede di riprendere le definizioni dell'ISO 29115, capitolo 3.3. *Posta* aggiunge riguardo al numero 1.5: - Public keys by definition are public and they need to protection. È chiara l'intenzione, ma la formulazione è sbagliata. Proposta: 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). È una questione puramente terminologica. Proposta: 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. Se non si modifica, risulteranno problemi con l'integrazione di nuovi profili FHIR IHE e dispositivi mobili. Proposta: 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. Proposta: 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. Proposta: change the formulation.

1.6 External Entities and Subjects

Posta dichiara riguardo alla tabella 2 al numero 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. *Posta* presenta nel suo parere la spiegazione di IdP contenuta in Wikipedia.

Posta segnala che i commenti fatti sono solo questioni terminologiche e chiede per tutti gli aspetti illustrati: Use properly defined terms that avoid confusion.

3 Security Problem Definition

Posta scrive riguardo alla tabella 3: CredentialHandling: The wording is geared towards smart card use. Se non si modifica non si potrà utilizzare mTAN. Chiede di riprendere le definizioni dell'ISO 29115, capitolo 3.3. *SCH* osserva riguardo al CredentialHandling che se l'utente può revocare autonomamente le sue credenziali, non è necessaria una comunicazione con il service desk dell'IdP. L'ultima frase alla tabella 3, sotto CredentialHandling, deve essere completata alla fine nel modo seguente: «[…] appropriate channels or that the claimant is able to revoke/reset his device/token through appropriate means". Riguardo al numero 3.2, *SCH* vuole la seguente aggiunta sulla 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 […]». Riguardo al P.TrustedCommunityEndpoint si dovrebbe aggiungere: «[…] as defined in section 6.3 or 6.4».

4 Security Objectives

Posta osserva riguardo all'O.Confidentiality nella tabella del numero 4.1: Please note that all references to public keys in the user data conflict with this requirement. Public keys are made for dissemination. Si tratta di una questione meramente terminologica. Proposta: modify the definition of user data. Segnala inoltre riguardo all'O.Authentication: The explanation in the second paragraph should be aligned with ISO 29115. Ciò è rilevante per l'accettazione di mTAN. Proposta: use the term «authentication factor». In merito al numero 4.2, *Posta* fa il seguente commento sull'OE.User Security Awareness: This paragraph contains references to smart card registration processes. Se non si modifica, non sarà più possibile utilizzare mTAN. Si chiede quindi di riprendere le definizioni dell'ISO 29115, capitolo 3.3. *HIN* segnala riguardo al numero 4.3.1 che la colonna «OE. SecureAreas and Equipment» non è collegata a nessuna riga e lo stesso vale per la riga «A.Physical». Il punto deve essere corretto o completato.

5 Security Requirements

Posta scrive riguardo al numero 5.2.12, FCS_COP.1(1) quanto segue: Elliptic Curve keys are way smaller than RSA/DH/EG keys with comparable security[171]. Requiring an elliptic curve keys to be 2k in size makes no sense. Se non si modifica, la sicurezza rimane ferma ai livelli attuali, mentre con i riferimenti si evolve automaticamente. *Posta* chiede di non definire degli algoritmi, ma di far riferimento alle raccomandazioni dell'ufficio tedesco Bundesamt für Sicherheit in der Informationstechnik (BSI) o del National Institute of Standards and Technology (NIST). Inoltre precisa: The referenced standard FIPS PUB 180-3 was superseded by FIPS PUB 180-4 in March 2012. Su questo punto rimanda agli standard attuali[172].

6 Appendix

OFAC scrive riguardo al SAML nel numero 6.4 che questa restrizione tecnologica non è accettabile. SAML non è né universale, né immortale. Il funzionamento degli IdP e dei token d'identificazione deve essere descritto in termini di requisiti di massima e non in modo troppo tecnico, troppo limitativo e troppo

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

effimero. *SCH* osserva che nel presente documento si menziona solo il protocollo SAML per l'autenticazione, mentre ne esistono altri ben collaudati come OpenID Connect basato su OAuth 2.0. L'interoperabilità dei SID deve limitarsi ai formati dei dati relativi all'identificazione dei pazienti. I protocolli fra Relying Party e IdP nonché le procedure di autenticazione dovrebbero essere regolati dal mercato. Si chiede di aggiungere a «SAML Specification» anche una «OpenID Connect/ OAuth 2.0 Specification». Le ordinanze/gli allegati dovrebbero inoltre impostati in modo da potere aggiungere altri protocolli. Nel parere è contenuta anche la seguente proposta: 6.5 OpenID Connect/OATH 2.0 Specification; Note: The specification will be drafted during or subsequently to appraisal.

4. Allegati

4.1 Elenco dei pareri pervenuti

L'elenco comprende tutti i partecipanti all'indagine conoscitiva relativa al diritto d'esecuzione della LCIP secondo la tabella 1.

Abbreviazione	Cantoni
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
Abbreviazione	**Partiti**
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
Abbreviazione	**Associazioni mantello svizzere dell'economia**

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)
Abbreviazione	**Altre organizzazioni**
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	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 (SGMI) 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
Abbreviazione	**Organizzazioni non interpellate e privati**
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 Kantonszahnärzte und Kantonszahnärztinnen 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 Altre abbreviazioni e termini

Abbreviazione	Titolo
NAVS13	Numero AVS a 13 cifre
ATP	Attributeprovider
BAG OFSP UFSP	Bundesamt für Gesundheit Office fédéral de la santé publique Ufficio federale della sanità pubblica
(D)DoS	Attacchi (Distributed) Denial-of-Service
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
EDI DFI DFI	Eidgenössisches Departement des Innern Département fédéral de l'intérieur Dipartimento federale dell'interno
GLN	Global Location Number
HPD	Health Provider Directory
SID	Strumento d'identificazione
IDP	Identification Provider
IHE	Integrating the Healthcare Enterprise
IPAG EPD	Gruppo di lavoro interprofessionale per la cartella informatizzata del paziente (GTIP-CIP)
ISMS	Information Security Management System (Sistema di gestione per la sicurezza delle informazioni)
SIC	Sistema d'informazione clinica
LOINC	Logical Observation Identifiers Names and Codes
MedReg	Registro delle professioni mediche universitarie
MPI	Master Patient Index
NIP	Numero d'identificazione del paziente
CSP	Controllo di sicurezza relativo alle persone
SaaS	Software as a Service
SIEM	Security Information and Event Management System sic
STL	Standard Transformation Language
STS	Secure Token Service
CTO	Condizioni tecniche e organizzative di certificazione
WAF	Web-Application-Firewall
IEE	Idoneità, efficacia ed economicità
XUA	Cross-Enterprise User Authentication
UCC	Ufficio centrale di compensazione

4.3 Organizzazioni con un parere identico a quello di Aargauische Spitäler, Kliniken und Pflegeinstitutionen (VAKA)

Il presente rapporto non riporta esplicitamente il parere delle seguenti organizzazioni quando coincide con quello di VAKA	
Abbreviazione	**Nome**
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

4.4 Progetto di ordinanza sulla cartella informatizzata del paziente (OCIP) in francese

Ordonnance sur le dossier électronique du patient (ODEP)

Version du 22 mars 2016 pour l'audition

Le Conseil fédéral suisse,
vu la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP)[1],
arrête:

Chapitre 1 Niveaux de confidentialité et droits d'accès

Art. 1 Niveaux de confidentialité

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

a. niveau de confidentialité «données utiles»;
b. niveau de confidentialité «données médicales»;
c. niveau de confidentialité «données sensibles»;
d. niveau de confidentialité «données secrètes».

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

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

Art. 2 Droits d'accès

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

a. «limité»: accès au niveau de confidentialité «données utiles»;
b. «normal»: accès aux niveaux de confidentialité «données utiles» et «données médicales»;
c. «étendu»: accès aux niveaux de confidentialité «données utiles», «données médicales» et «données sensibles».

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

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

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

1 RS 816.11

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

Art. 3 Options du patient

Le patient peut:

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

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

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

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

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

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

g. désigner un représentant;

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

Chapitre 2: Numéro d'identification du patient

Art. 4 Format du numéro d'identification du patient

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

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

2 RS 831.10

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

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

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

a. nom;
b. prénoms;
c. sexe;
d. date de naissance;
e. numéro d'assuré selon l'art. 50*c* LAVS[3].

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

Art. 6 Consultation du numéro d'identification du patient

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

Art. 7 Annulation

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

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

Chapitre 3 Communautés et communautés de référence

Section 1 Communautés

Art. 8 Gestion

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

a. régler les modalités d'entrée et de sortie;
b. identifier les professionnels de la santé;
c. assurer la mise à jour des données dans le service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40;

[3] RS 831.10

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

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

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

Art. 9 Tenue et transfert des données

[1] Les communautés doivent garantir:

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

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

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

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

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

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

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

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

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

b. les métadonnées à utiliser;

c. les formats d'échange à utiliser;

d. les profils d'intégration à utiliser;

e. les prescriptions relatives aux données historisées.

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

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

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

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

Art. 11 Protection et sécurité des données

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

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

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

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

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

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

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

Section 2 Communautés de référence

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

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

Art. 14 Information du patient

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

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

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

Art. 15 Consentement

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

Art. 16 Gestion

[1] Les communautés de référence doivent:

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

b. identifier les patients;

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

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

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

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

Art. 17 Portail d'accès pour les patients

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

Art. 18 Disponibilité des données enregistrées par les patients

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

Art. 19 Service d'assistance pour les patients

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

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

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

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

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

c. décès du patient.

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

a. en cas de suppression:

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

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

Section 3 Données à fournir pour l'évaluation

Art. 21

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

[2] Le DFI fixe les données à fournir.

Chapitre 4 Moyens d'identification

Art. 22 Exigences applicables au moyen d'identification

Le moyen d'identification doit:

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

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

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

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

Art. 23 Vérification d'identité

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

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

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

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

Art. 24 Données du moyen d'identification

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

a. nom;
b. prénoms;
c. sexe;
d. date de naissance;
e. numéro de la pièce d'identité fournie conformément à l'art. 23, al. 1.

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

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

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

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

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

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

Art. 26 Blocage du moyen d'identification

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

8 *Global Location Number*

Chapitre 5 Accréditation

Art. 27 Critères

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

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

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

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

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

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

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

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

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

Art. 28 Procédure d'accréditation

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

Chapitre 6 Certification

Section 1 Critères de certification

Art. 29 Communautés et communautés de référence

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

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

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

9 RS **946.512**

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

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

Art. 30 Editeurs de moyens d'identification

[1] Les éditeurs de moyens d'identification doivent:

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

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

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

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

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

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

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

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

Section 3 Procédure de certification

Art. 31 Déroulement

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

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

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

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

Art. 32 Déclaration à l'OFSP

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

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

Art. 33 Surveillance

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

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

Art. 34 Durée de validité

Le certificat est établi pour une durée de trois ans.

Art. 35 Déclaration d'adaptations techniques ou organisationnelles substantielles

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

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

Art. 36 Clause de sauvegarde

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

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

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

c. ordonner une recertification extraordinaire.

Section 4 Sanctions

Art. 37

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

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

b. un certificat est utilisé fallacieusement ou abusivement.

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

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

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

b. suspendre la validité ducertificat;

c. retirer le certificat.

Chapitre 7 Services de recherche de données

Section 1 Généralités

Art. 38

[1] Les services de recherche contiennent:

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

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

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

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

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

Section 2: Contenu

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

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

a. désignation;

b. identifiant univoque (GLN);

c. identificateur d'objet (OID);

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

e. adresse internet du point d'accès.

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

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

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

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

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

Section 3 Transfert de tâches à des tiers

Art. 41 Contrat de prestations

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

[2] Le contrat de prestations règle en particulier:

a. les objectifs à atteindre;

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

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

d. les conséquences de l'inexécution du contrat;

e. les modalités de compte rendu périodique.

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

Art. 42 Emoluments

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

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

Art. 43 Surveillance

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

[2] La surveillance comprend en particulier:

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

b. l'obtention de comptes rendus périodiques;

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

Chapitre 8 Dispositions finales

Art. 44 Abrogation et modification d'autres actes

Art. 45 Entrée en vigueur

La présente ordonnance entre en vigueur le ....

[12] RS 172.041.1

4.5 Progetto di ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI) in francese

Ordonnance du DFI sur le dossier électronique du patient
(ODEP-DFI) *Version du 22 mars 2016 pour l'audition*

Le Département fédéral de l'intérieur (DFI),
vu les art. 4, al. 2, 9, al. 3, 10, 11, al. 3, 17, 18, 21, al. 2, 27, al. 4, 29, al. 2, 30, al. 2 et 3 de l'ordonnance du ... sur le dossier électronique du patient[1] (ODEP),
arrête:

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. 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 définies à l'annexe 2.

Art. 3 Métadonnées

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

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. 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. 6 Evaluation

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

1 RS 816....

Art. 7 Exigences minimales applicables au personnel

Conformément à l'art. 27, al. 4, ODEP, les exigences minimales applicables à la qualification du personnel qui réalise les certifications sont définies à l'annexe 7.

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. 9 Entrée en vigueur

La présente ordonnance entre en vigueur le ...

Annexe 1
(art. 1)

Vérification de la clé de contrôle

1. Composition du numéro d'identification du patient

x_{n-10}	x_{n-9}	x_{n-8}	x_{n-7}	x_{n-6}	.	x_{n-5}	x_{n-4}	x_{n-3}	x_{n-2}	.	x_{n-1}	x_n
Numéro à 10 chiffres												**Clé de contrôle**
1	**2**	**3**	**4**	**5**		**6**	**7**	**8**	**9**		**0**	**5**

2. Logique de la clé de contrôle

2.1 La clé de contrôle est le dernier chiffre du numéro (x_n). Elle s'obtient par les opérations suivantes:

2.1.1 multiplier alternativement par 3 et par 1 chaque chiffre en procédant de droite à gauche, à partir de l'avant-dernier (xn-1). Additionner ensuite les produits obtenus:

total intermédiaire = $(3x_{n-1}) + (1x_{n-2}) + (3x_{n-3})$ …

2.2.2 déterminer ensuite la valeur (clé de contrôle xn) qui, ajoutée au total intermédiaire, donnera le prochain multiple de 10.

2.2 Remarque:

2.2.1 Si le total intermédiaire est déjà un multiple de 10, la clé de contrôle est 0.

3. Illustration du principe :

Numéro d'identification du patient	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	→ ? ←
Multiplicateur	1	3	1	3	1	3	1	3	1	3	
Résultat	1	6	3	12	5	18	7	24	9	0	← total intermédiaire: 85
Valeur à ajouter pour obtenir un multiple de 10	90 est le prochain multiple de 10 après le total intermédiaire 85. La différence, et donc la clé de contrôle, est 5 →										? = **5**

Annexe 2
(art. 2)

Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence[2]

2 Les critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence ne sont pas publiées au RO. Commande: Office fédéral de la santé publique, Schwarzenburgstrasse 157, 3003 Berne. Téléchargement: www.ehealth.admin.ch.

Annexe 3
(art. 3)

Métadonnées[3]

[3] Les métadonnées ne sont pas publiées au RO. Commande: Office fédéral de la santé publique, Schwarzenburgstrasse 157, 3003 Berne. Téléchargement: www.ehealth.admin.ch. Elles ne seront pas traduites dans les langues officielles.

Annexe 4
(art. 4)

Formats d'échange[4]

[4] Les formats d'échange ne sont pas publiés au RO. Commande: Office fédéral de la santé publique, Schwarzenburgstrasse 157, 3003 Berne. Téléchargement: www.ehealth.admin.ch.

Annexe 5
(art. 5)

Profils d'intégration[5]

1. Profils d'intégration IHE[6]

Profil d'intégration	Document technique	Transactions	Adaptations nationales
ATNA	IHE IT Infrastructure Technical Framework, Volume 2a (ITI TF-2a), Revision 12.0	Maintain Time [ITI-1] Authenticate Node [ITI-19] Record Audit Event [ITI-20]	Oui
HPD	IHE IT Infrastructure Technical Framework, Supplement, Healthcare Provider Directory (HPD), Revision 1.6–2015-08-31	Provider Information Query [ITI-58] Provider Information Feed [ITI-59]	Oui
PDQ V3	IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b), Revision 12.0	Patient Demographics Query HL7 V3 [ITI-47]	Oui
PIX V3	IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b), Revision 12.0	Patient Identity Feed HL7 V3 [ITI-44] PIXV3 Query [ITI-45] PIXV3 Update Notification [ITI-46]	Oui
XCA	IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b), Revision 12.0	Cross Gateway Query [ITI-38] Cross Gateway Retrieve [ITI-39]	

5 Ces profils d'intégration peuvent être consultés gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne, www.ehealth.admin.ch ou d'IHE Suisse, Oberstrasse 222, 9014 St-Gall, www.ihe-suisse.ch. Les adaptations nationales des profils d'intégration et les profils d'intégration nationaux ne sont pas publiés au RO. Commande: Office fédéral de la santé publique, Schwarzenburgstrasse 157, 3003 Berne. Téléchargement: www.ehealth.admin.ch. Cette annexe ne sera pas traduite dans les langues officielles.

6 Integrating the Healthcare Enterprise

XCA-I	IHE Radiology Technical Framework, Volume 3 (RAD-TF-3), Revision 14.0	Cross Gateway Retrieve Image Document Set [RAD-75]	
XCPD	IHE IT Infrastructure Technical Framework Supplement, Cross-Community Patient Discovery (XCPD) Health Data Locator and Revoke Option, Revision 2.7–2015-08-31	Cross Gateway Patient Discovery [ITI-55] Patient Location Query [ITI-56]	
XDS	IHE IT Infrastructure Technical Framework, Volume 2a (ITI TF-2a), Revision 12.0	Registry Stored Query [ITI-18] Provide and Register Document Set-b [ITI-41] Register Document Set-b [ITI-42] Retrieve Document Set [ITI-43]	
XDS-I	IHE Radiology Technical Framework, Volume 2 (RAD-TF-2), Revision 14.0	Retrieve Images [RAD-16]; Retrieve Presentation States [RAD-17] Retrieve Key Image Note [RAD-31] Retrieve Evidence Documents [RAD-45]	
XDS Metadata Update	IHE IT Infrastructure Technical Framework Supplement – XDS Metadata Update, Revision 1.6-2015-08-31	Update Document Set [ITI-57] Delete Document Set [ITI-62]	
XUA	IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b), Revision 12.0	Provide X-User Assertion [ITI-40]	Oui

2. Profils d'intégration nationaux

CH:ADR	Authorization Decision Request	AuthorizationDecision-Request	
CH:PPQ	Privacy Policy Query	PolicyQuery AddPolicyRequest DeletePolicyRequest UpdatePolicyRequest	

Annexe 6
(art. 6)

Indicateurs pour l'évaluation

1. Données de base

Indicateur	Relevé par[7]
Nombre et type d'institutions de santé et de leurs professionnels de la santé affiliés aux communautés et aux communautés de référence.	C, CR
Nombre de patients qui ont ouvert un dossier électronique du patient, classés selon l'âge, le sexe et le domicile.	CR
Date de l'affiliation d'hôpitaux et d'autres établissements visés aux art. 39, al. 1, let. f, et 49*a*, al. 4, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[8] (LAMal) à une communauté ou à une communauté de référence.	C, CR

2. Droits d'accès

Indicateur	Relevé par
Nombre de patients qui ont ouvert un dossier électronique du patient, classés selon l'âge, le sexe et le domicile.	CR
Options choisies par les patients pour les droits d'accès conformément à l'art. 3, let. a, e et f, ODEP.	CR
Nombre de patients qui ont limité, étendu ou exclu l'accès en cas d'urgence médicale conformément à l'art. 3, let. b, ODEP.	CR
Nombre de patients qui ont modifié le niveau de confidentialité pour les nouvelles données enregistrées dans leur dossier électronique du patient conformément à l'art. 3, let. c, ODEP.	CR
Nombre de patients qui ont désigné un représentant en vertu de l'art. 3, let. g, ODEP.	CR
Nombre de patients qui, en vertu de l'art. 3, let. h, ODEP, ont habilité des professionnels de la santé affiliés à leur communauté à accorder en leur nom des droits d'accès à d'autres professionnels de la santé.	CR

7 CR = à relever par les communautés de référence certifiées; C = à relever par les communautés certifiées
8 RS 832.10

Nombre et type de fichiers par niveau de confidentialité au sens de l'art. 1, al. 1, ODEP.	C, CR
Nombre de professionnels de la santé dont l'accès au dossier électronique du patient est refusé conformément à l'art. 3, al. 1, let. d, ODEP.	CR
Nombre d'accès par des professionnels de la santé en cas d'urgence médicale conformément à l'art. 2, al. 5, ODEP.	CR

3. Fichiers

Indicateur	Relevé par
Nombre de fichiers enregistrés, classés selon le format (PDF, texte, JPEG, DICOM, etc.).	C, CR

4. Utilisation

Indicateur	Relevé par
Nombre de professionnels de la santé qui ont saisi au moins un fichier dans le dossier électronique de leurs patients.	C, CR
Nombre de fichiers saisis par les professionnels de la santé selon la catégorie et le type de fichier.	C, CR
Nombre de fichiers supprimés par le professionnel de la santé.	C, CR
Nombre de fichiers supprimés par le patient.	CR
Nombre d'accès au dossier électronique du patient par les professionnels de la santé dans le temps, selon la catégorie et le type de fichier.	C, CR
Nombre d'accès par patient au dossier électronique du patient dans le temps, classés selon la catégorie et le type de fichier.	CR
Nombre de fichiers de données saisis par les patients, classés selon la catégorie et le type de fichier.	C, CR
Nombre de professionnels de la santé qui obtiennent des droits d'accès de la part de patients, par patient.	C, CR

5. Protection des données

Indicateur	Relevé par
Nombre de réclamations de patients concernant un accès non autorisé en cas d'urgence médicale.	C, CR

Annexe 7
(art. 7)

Exigences minimales applicables à la qualification du personnel des organismes de certification

1 Certification des communautés et des communautés de référence

1.1 L'organisme de certification doit prouver qu'une partie du personnel qui certifie les systèmes de gestion possède les qualifications suivantes:

1.1.1 connaissance de l'informatique médicale: une activité pratique d'au moins deux ans dans le domaine de l'informatique médicale doit être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée doit être fourni attestant des études d'une année au moins, avec comme matière principale l'informatique médicale doit être fourni;

1.1.2 connaissance du droit de la protection des données: une activité pratique d'au moins deux ans dans le domaine de la protection des données doit être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale le droit de la protection des données doit être fourni;

1.1.3 connaissances dans le domaine de la sécurité informatique: une activité pratique d'au moins deux ans dans le domaine de la sécurité informatique doit être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale la sécurité informatique doit être fourni;

1.1.4 formation d'auditeur selon la norme ISO/IEC 17021:2006[9];

1.1.5 formation d'auditeur selon la norme ISO/IEC 27006:2011[10].

1.2 L'organisme de certification doit prouver qu'il dispose de personnel qualifié pour chacun des domaines qu'il couvre. L'évaluation des systèmes de gestion de la protection des données peut être menée par une équipe interdisciplinaire.

2 Certification des éditeurs de moyens d'identification

2.1 L'organisme de certification doit prouver qu'une partie du personnel qui certifie les systèmes de gestion possède les qualifications suivantes:

2.1.1 connaissances dans le domaine de l'identification et de l'authentification: une activité pratique d'au moins deux ans dans le domaine de l'identification et de l'authentification doit être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale l'identification et l'authentification doit être fourni;

2.1.2 connaissance du droit de la protection des données: une activité pratique d'au moins deux ans dans le domaine de la protection des données doit

9 Cette norme peut être consultée auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne

10 Cette norme peut être consultée auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne

être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale le droit de la protection des données doit être fourni;

2.1.3 connaissances dans le domaine de la sécurité informatique: une activité pratique d'au moins deux ans dans le domaine de la sécurité informatique doit être attestée ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale la sécurité informatique doit être fourni;

2.1.4 formation d'auditeur selon la norme ISO/IEC 17021:200611;

2.1.5 formation d'auditeur selon la norme ISO/IEC 27006:201112.

2.2 L'organisme de certification doit prouver qu'il dispose de personnel qualifié pour chacun des domaines qu'il couvre. Les audits peuvent être menés par une équipe interdisciplinaire.

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

12 Cette norme peut être obtenue contre paiement auprès de l'Association suisse de normalisation (SNV, www.snv.ch) ou consultée gratuitement auprès de l'OFSP, Schwarzenburgstrasse 157, 3003 Berne

Annexe 8
(art. 8)

Prescriptions relatives à la protection des moyens d'identification[13]

13 Les prescriptions relatives à la protection des moyens d'identification ne sont pas publiées au RO. Commande: Office fédéral de la santé publique, Schwarzenburgstrasse 157, 3003 Berne. Téléchargement: www.ehealth.admin.ch. Elles ne seront pas traduites dans les langues officielles.