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 esplicativo concernente

l'ordinanza sulla cartella informatizzata del paziente (OCIP) e

l'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI)

Versione del 22 marzo 2017

Indice

1 Parte generale

1.1 Situazione iniziale

Il Parlamento ha adottato la legge federale sulla cartella informatizzata del paziente (LCIP; RS 816.1, FF 2015 3951) il 19 giugno 2015. Nella sua qualità di legge quadro, la LCIP intende disciplinare le condizioni per il trattamento dei dati della cartella informatizzata del paziente. Ciò consente di soddisfare una premessa di centrale importanza per l'applicazione della «Strategia eHealth Svizzera» e costituisce un'importante misura per lo sviluppo del sistema sanitario svizzero.

Oggetto
La LCIP fissa le condizioni quadro per il trattamento di dati e documenti relativi alla cartella informatizzata del paziente, al fine di rafforzare la qualità delle cure mediche, migliorare i processi terapeutici, accrescere la sicurezza dei pazienti e l'efficienza del sistema sanitario, nonché promuovere l'alfabetizzazione sanitaria dei pazienti. Il disegno, sotto forma di legge quadro, sarà volto da un lato ad assicurare la sicurezza degli investimenti e dall'altro a garantire sufficiente flessibilità durante l'implementazione nelle regioni di erogazione dei servizi sanitari.

Con l'aiuto della cartella informatizzata del paziente, i professionisti della salute possono accedere a dati relativi alla cura dei loro pazienti, elaborati e rilevati a livello decentrato da altri professionisti della salute coinvolti nel processo terapeutico ed eventualmente memorizzarli nei sistemi d'informazione del loro studio medico o della loro clinica, al di fuori della cartella informatizzata del paziente. A tale scopo essi devono aderire a una comunità o comunità di riferimento certificata, ossia a un raggruppamento di professionisti della salute e delle loro strutture, e devono ottenere i necessari diritti d'accesso da parte dei pazienti. Inoltre, la cartella informatizzata consente anche ai pazienti di visionare i propri dati, di renderli accessibili e di gestirne i diritti d'accesso.

La gestione dei dati dei pazienti al di fuori della cartella informatizzata, come ad es. le norme per la documentazione e la responsabilità oppure il segreto professionale medico, non sono oggetto del disegno di legge. Lo stesso dicasi per le norme sullo scambio di dati tra i professionisti della salute e le assicurazioni sociali nonché per l'uso dei dati medici contenuti nella cartella informatizzata del paziente per la creazione di registri delle malattie e di qualità oppure a fini statistici e di ricerca.

Partecipazione alla cartella informatizzata del paziente
Per i pazienti, la cartella informatizzata è facoltativa. In virtù del principio dell'autodeterminazione in materia d'informazione, ognuno deve poter decidere se autorizzare la costituzione di una cartella informatizzata e in quale misura attribuire diritti d'accesso ai professionisti della salute.

Il principio della volontarietà si applica anche ai professionisti della salute e alle strutture in cui operano. Fanno eccezione unicamente i fornitori di prestazioni secondo gli articoli 39 e 49*a* capoverso 4 della legge federale del 18 marzo 1994[1] sull'assicurazione malattie: entro tre anni dall'entrata in vigore dell'OCIP – vale a dire entro il 14 aprile 2020 – gli ospedali devono aderire a una comunità o a una comunità di riferimento certificata, mentre le case per partorienti e le case di cura devono farlo entro cinque anni, vale a dire entro il 14 aprile 2022.

I professionisti della salute che operano a livello ambulatoriale sono liberi di decidere se offrire ai propri pazienti una cartella informatizzata. Se però aderiscono a una comunità o comunità di riferimento certificata, sono tenuti a rendere accessibili i dati pertinenti della cartella informatizzata.

Il trattamento di dati nel quadro della cartella informatizzata da parte di professionisti della salute è possibile solo con il consenso del paziente, che può attribuire i diritti d'accesso a singoli professionisti della salute o a gruppi di essi.

[1] RS **832.10**

Strumenti d'identificazione
L'identificazione e l'autenticazione univoche dei pazienti e dei professionisti della salute sono presupposti importanti per garantire un trattamento dei dati sicuro. Queste devono avvenire mediante uno strumento d'identificazione di un emittente certificato.

Numero d'identificazione del paziente
Per consentire la corretta aggregazione di tutti i dati e documenti medici concernenti un paziente nella cartella informatizzata, il nuovo numero d'identificazione del paziente è impiegato quale elemento di identificazione supplementare, a complemento dei dati di identificazione personali come cognome, nome, sesso o data di nascita. Il numero viene attribuito su richiesta dall'Ufficio centrale di compensazione dell'AVS (UCC).

Obbligo di certificazione
Per garantire un trattamento dei dati sicuro, tutti i partecipanti al sistema (comunità, comunità di riferimento, portali d'accesso esterni per la consultazione dei dati da parte dei pazienti, emittenti di strumenti d'identificazione) devono soddisfare condizioni di certificazione dettagliate. L'adempimento di queste condizioni tecniche e organizzative deve essere garantito da una procedura di certificazione.

Servizi di ricerca di dati
Alla Confederazione compete la gestione dei servizi centrali di ricerca di dati necessari per la comunicazione tra comunità e comunità di riferimento.

Aiuti finanziari
Inoltre, è previsto che per i tre anni successivi all'entrata in vigore della LCIP la Confederazione sostenga con aiuti finanziari la creazione e la certificazione di comunità e comunità di riferimento con un importo complessivo di 30 milioni di franchi. Questi sussidi sono vincolati al cofinanziamento da parte dei Cantoni o di terzi per lo stesso ammontare. I costi che i professionisti della salute e le loro strutture devono sostenere per gli adeguamenti dei propri sistemi informatici a uso specialistico o clinico non vengono coperti dagli aiuti finanziari della Confederazione.

1.2 Diritto dell'UE

Al momento della redazione del presente rapporto (marzo 2016) non esistevano impegni internazionali vincolanti nel settore «eHealth». Le direttive e le raccomandazioni internazionali (ad es. dell'UE) hanno tuttavia fornito punti di riferimento per l'elaborazione della LCIP; tra queste segnatamente la Raccomandazione della Commissione europea sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, nonché le seguenti direttive vincolanti in materia:

- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[2].
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[3].
- Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori[4].
- Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente

[2] GU L 281 del 23.11.1995, p. 31; modificata dal Regolamento (CE) n. 1882/2003, GU L 284 del 31.10.2003, p. 1.
[3] GU L 201 del 31.7.2002, p. 37; modificata da ultimo dalla Direttiva 2009/136/CE, GU L 337 del 18.12.2009, p. 11.
[4] GU L 337 del 18.12.2009, p. 11.

l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera[5].

- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE[6].

Per maggiori informazioni sul rapporto con il diritto dell'UE si rimanda al messaggio concernente la LCIP (FF 2013 4602 segg.).

1.3 Panoramica delle disposizioni esecutive concernenti la cartella informatizzata del paziente

Le disposizioni esecutive concernenti la cartella informatizzata del paziente sono costituite dall'ordinanza sulla cartella informatizzata del paziente (OCIP), dall'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI) e dall'ordinanza sugli aiuti finanziari per la cartella informatizzata del paziente (OFCIP). I dettagli sono illustrati nella tabella seguente.

<table>
<tr><td rowspan="2">Livello del Consiglio federale</td><td rowspan="2">Ordinanza sulla cartella informatizzata del paziente (OCIP)
– Capitolo 1: Gradi di riservatezza e diritti d'accesso
– Capitolo 2: Numero d'identificazione del paziente
– Capitolo 3: Comunità e comunità di riferimento
– Capitolo 4: Strumenti d'identificazione
– Capitolo 5: Accreditamento
– Capitolo 6: Certificazione
– Capitolo 7: Servizi di ricerca di dati
– Capitolo 8: Entrata in vigore</td><td>Ordinanza sugli aiuti finanziari per la cartella informatizzata del paziente (OFCIP)
– Sezione 1: Disposizioni generali
– Sezione 2: Criteri e calcolo
– Sezione 3: Procedura
– Sezione 4: Entrata in vigore</td></tr>
<tr><td>– Allegato: Costi computabili</td></tr>
<tr><td>Livello dipartimentale</td><td>Ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI)
– Allegato 1: Numero d'identificazione del paziente
– Allegato 2: Condizioni tecniche e organizzative di certificazione per le comunità e le comunità di riferimento
– Allegato 3: Metadati
– Allegato 4: Formati di scambio
– Allegato 5: Profili d'integrazione
– Allegato 6: Valutazione e ricerca
– Allegato 7: Requisiti minimi in materia di qualifica del personale degli organismi di certificazione
– Allegato 8: Condizioni tecniche e organizzative di certificazione degli emittenti di strumenti d'identificazione</td><td></td></tr>
</table>

1.3.1 Ordinanza sulla cartella informatizzata del paziente (OCIP)

L'OCIP disciplina i gradi di riservatezza e i diritti d'accesso (capitolo 1), le prescrizioni relative

[5] GU L 88 del 4.4.2011, p. 45.
[6] GU L 257 del 28.8.2014, p. 73.

all'attribuzione e alla gestione del numero d'identificazione del paziente da parte dell'UCC (capitolo 2), le prescrizioni inerenti alla costituzione e alla gestione di comunità e comunità di riferimento (condizioni di certificazione; capitolo 3), le prescrizioni riguardanti gli strumenti d'identificazione e i loro emittenti (capitolo 4), l'accreditamento (capitolo 5), la certificazione (capitolo 6) nonché i servizi di ricerca di dati (capitolo 7).

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

All'*allegato* 1 l'ordinanza dipartimentale disciplina i requisiti relativi al numero d'identificazione del paziente. Tra questi vi sono le prescrizioni per la strutturazione del numero d'identificazione del paziente e per il calcolo della cifra di controllo secondo l'articolo 5 capoverso 2 OCIP.

L'*allegato 2* disciplina le condizioni di certificazione per le comunità e le comunità di riferimento mediante le cosiddette condizioni tecniche e organizzative di certificazione (CTO; cfr. capitolo 3 «Comunità e comunità di riferimento» OCIP).

L'*allegato 3* (cfr. art. 10 cpv. 3 lett. a OCIP) contiene l'elenco dei metadati da utilizzare nella cartella informatizzata del paziente per garantire l'interoperabilità e la sicurezza dello scambio di dati.

L'*allegato 4* (cfr. art. 10 cpv. 3 lett. b OCIP) riporta i formati di scambio da utilizzare ad esempio per il libretto di vaccinazione elettronico o per il rapporto informatizzato di dimissione. Ad oggi i formati di scambio non sono ancora disponibili: sono in fase di elaborazione nell'ambito di processi che coinvolgono i portatori d'interessi e saranno ripresi nelle disposizioni esecutive con le future revisioni.

L'*allegato 5* (cfr. art. 10 cpv. 3 lett. c OCIP) precisa i profili d'integrazione da utilizzare per lo scambio di dati tra comunità nonché gli adeguamenti nazionali di questi profili. Contiene inoltre due profili d'integrazione nazionali, da utilizzare a complemento dei profili IHE.

L'*allegato 6* (cfr. art. 22 cpv. 2 OCIP) stabilisce i dati da fornire per la valutazione e i termini rilevanti per la loro fornitura; i dati in questione saranno ripresi nelle disposizioni esecutive in occasione di una revisione futura.

I requisiti minimi in materia di qualifica del personale addetto alle certificazioni sono stabiliti nell'*allegato 7*.

L'*allegato 8* (cfr. art. 31. cpv. 2 OCIP) fissa le condizioni tecniche e organizzative di certificazione degli emittenti di strumenti d'identificazione.

1.3.3 Ordinanza sugli aiuti finanziari per la cartella informatizzata del paziente (OFCIP)

L'OFCIP disciplina la concessione degli aiuti finanziari secondo gli articoli 20–23 LCIP. Secondo l'articolo 27 capoverso 3 LCIP, la presentazione di domande di aiuto finanziario per la costituzione e la certificazione di comunità e comunità di riferimento è limitata ai tre anni successivi all'entrata in vigore della legge. L'articolo 26 LCIP prescrive che gli articoli 20–23 LCIP e quindi l'OFCIP restino applicabili alle domande di aiuti finanziari presentate durante la loro durata di validità. I commenti concernenti l'OFCIP sono oggetto di un documento separato.

1.4 Ripercussioni

In sede di consultazione parlamentare, la LCIP è stata adeguata soltanto in alcuni punti (in particolare per quanto concerne la possibilità di cofinanziamento della costituzione di comunità o comunità di riferimento da parte di terzi per ottenere aiuti finanziari della Confederazione, l'uniformazione della procedura per la concessione degli aiuti finanziari, la riduzione del termine transitorio per l'adesione degli ospedali a comunità e comunità di riferimento certificate e la possibilità di utilizzare la tessera

d'assicurato). Pertanto è possibile rinviare sostanzialmente alle spiegazioni relative alle ripercussioni sui diversi attori di cui al messaggio concernente la LCIP (cfr. FF 2013 4631 segg.). Di seguito sono brevemente ripresi i punti principali contenuti nel messaggio e sono illustrate in particolare le ripercussioni che hanno effetto sulle disposizioni esecutive.

1.4.1 Ripercussioni per la Confederazione

Per la Confederazione l'attuazione della LCIP può generare oneri di personale e finanziari supplementari per i seguenti motivi indicati di seguito.

L'articolo 12 capoverso 2 LCIP autorizza l'Ufficio federale della sanità publlica (UFSP) ad adeguare all'evoluzione della tecnica le condizioni di certificazione per comunità e comunità di riferimento nonché per gli emittenti di strumenti d'identificazione (cfr. art. 10 cpv. 5, art. 30 cpv. 3 e art. 31 cpv. 3 OCIP).

Inoltre, nell'ambito della certificazione secondo la LCIP, l'UFSP è titolare dello schema di certificazione («schema owner») ed è pertanto l'organismo di riferimento per le domande del Servizio di accreditamento svizzero (SAS). Deve inoltre garantire uno scambio d'informazioni mirato tra le entità da certificare (comunità e comunità di riferimento nonché emittenti di strumenti d'identificazione) per quanto concerne la certificazione.

Per garantire una certificazione uniforme a livello nazionale nel quadro delle prescrizioni sull'interoperabilità, l'UFSP, insieme all'organo di coordinamento Confederazione-Cantoni «eHealth Suisse», mette a disposizione degli organismi di certificazione un sistema di test di certificazione che verifica il rispetto di norme, standard e profili d'integrazione nell'ambito della certificazione, occupandosi della sua gestione e del suo sviluppo (art. 28 cpv. 4 OCIP).

L'UFSP crea e gestisce servizi elementari di ricerca di dati per il funzionamento della cartella informatizzata del paziente (art. 14 cpv. 1 e art. 19 cpv. 1 LCIP).

Per incentivare la costituzione e la certificazione di comunità e comunità di riferimento, la Confederazione concede aiuti finanziari per un periodo di tre anni a partire dall'entrata in vigore (art. 20-23 LCIP). L'UFSP esamina le domande di aiuto finanziario, raccoglie i pareri dei Cantoni interessati e conclude contratti di prestazioni con le comunità o le comunità di riferimento beneficiarie degli aiuti finanziari. Il rispetto di questi contratti di prestazioni è verificato costantemente, per individuare possibili violazioni e adottare le misure del caso.

Il *Dipartimento federale dell'interno (DFI)* valuta la legge secondo i principi di idoneità, efficacia ed economicità (art. 18 LCIP e art. 22 OCIP).

Il trattamento di dati da parte di persone private rientra nel campo d'applicazione della legge federale sulla protezione dei dati (LPD; RS 235.1). In quanto organizzazioni di diritto privato, le comunità e le comunità di riferimento sottostanno alla LPD e quindi alla sorveglianza dell'*Incaricato federale della protezione dei dati e della trasparenza (IFPDT)*, se la sorveglianza non è disciplinata altrimenti nella legislazione speciale. Lo stesso vale per tutti gli altri attori fintantoché si tratta di privati.

Il *SAS* riconosce gli organismi per l'audit e la certificazione di sistemi di gestione, che hanno intenzione di effettuare certificazioni secondo la LCIP. In sede di accreditamento si verifica se l'organizzazione e la procedura di controllo predefinite sono adatte a verificare le condizioni di certificazione per comunità e comunità di riferimento nonché per gli emittenti di strumenti d'identificazione. Questa verifica comprende aspetti sia tecnici sia organizzativi.

L'*UCC* è competente per l'attribuzione e la gestione del numero d'identificazione del paziente secondo l'articolo 6 capoverso 1 OCIP e assicura che la banca dati d'identificazione venga adeguata secondo le esigenze della LCIP e dell'OCIP.

L'organo di coordinamento Confederazione-Cantoni «eHealth Suisse» si accerta che norme, standard e profili d'integrazione siano sviluppati nell'ambito di processi partecipativi. Il risultato di questi lavori confluisce direttamente all'UFSP, che è l'ufficio responsabile per la revisione della legge e delle disposizioni esecutive.

«eHealth Suisse» assume inoltre i compiti negli ambiti dell'informazione (art. 15 LCIP) e del coordinamento (art. 16 LCIP).

1.4.2 Ripercussioni su Cantoni e Comuni

Per i Cantoni l'attuazione del presente disegno può generare oneri di personale e finanziari supplementari per i seguenti motivi:

- esame ed eventuale adeguamento delle basi legali cantonali per l'introduzione della cartella informatizzata del paziente;
- eventuale partecipazione ai costi di costituzione, certificazione e gestione operativa delle comunità e comunità di riferimento;
- elaborazione di pareri su domande di aiuto finanziario della Confederazione per comunità o comunità di riferimento sul proprio territorio cantonale.

Poiché sono i Cantoni che devono garantire – e quindi organizzare – l'assistenza sanitaria, spetta a loro, nell'ambito della loro responsabilità finanziaria e della loro sfera di competenza, creare i presupposti per incentivare gli istituti stazionari (ospedali figuranti nell'elenco e convenzionati, cliniche di riabilitazione, case di cura e case per partorienti; art. 39 cpv. 1 lett. f e art. 49*a* cpv. 4 primo periodo LAMal), ma anche i liberi professionisti della salute (in particolare i medici), a riunirsi in comunità o comunità di riferimento e a farsi certificare.

2 Parte speciale

2.1 Ingresso

In virtù del fatto che la LCIP contiene numerose norme attributive di competenze, l'ingresso dell'OCIP rimanda alla LCIP nel suo complesso.

2.2 Commenti ai singoli articoli

Capitolo 1: Gradi di riservatezza e diritti d'accesso

Art. 1 Gradi di riservatezza

Secondo il *capoverso 1*, il paziente può attribuire ai dati medici della sua cartella informatizzata tre gradi di riservatezza (*lett. a–c*). L'attribuzione di un determinato grado ai dati è a discrezione del paziente, secondo la seguente suddivisione:

a) «normalmente accessibile»: documenti e dati relativi alla cura come rapporti, referti o trattamenti effettuati nonché informazioni su allergie e intolleranze o patologie particolari, garanzie di assunzione dei costi, direttive del paziente, dichiarazione di volontà di donare organi, dati di contatto delle persone da informare in caso di emergenza;
b) «limitatamente accessibile»: dati medici sensibili dal punto di vista del paziente, che dovrebbero essere accessibili solo a professionisti della salute con diritto d'accesso «esteso»;
c) «segreto»: dati medici che possono essere visionati solo dal paziente.

Le denominazioni dei gradi di riservatezza non sono da intendere come definizioni dei dati ai quali viene attribuito il grado. Gli esempi sopra riportati servono solamente a fini di chiarezza. A ogni tipo di documento può essere attribuito ognuno dei gradi di riservatezza. Determinante per la scelta è il fatto che l'entità del diritto d'accesso varia a seconda del grado di riservatezza (cfr. commenti all'art. 2).

In mancanza di attribuzione da parte del paziente, ai nuovi dati registrati è attribuito il grado di riservatezza «normalmente accessibile» (*cpv. 2*). Il paziente può modificare questa impostazione standard (cfr. commenti all'art. 4 lett. a). Anche i professionisti della salute possono, in deroga all'impostazione standard, attribuire ai nuovi dati da loro registrati il grado di riservatezza «limitatamente accessibile». Tuttavia, il professionista della salute può utilizzare questa possibilità solo se il paziente non si è avvalso dell'opzione di cui all'articolo 4 lettera a. In questo caso l'esplicita disposizione del paziente ha la precedenza.

I gradi di riservatezza sono applicati solo per i documenti e dati medici registrati nella cartella informatizzata del paziente e memorizzati negli archivi o nei registri di documenti. Ciò non riguarda i dati demografici del paziente, che si trovano segnatamente nell'indice dei pazienti della comunità o della comunità di riferimento. I dati demografici sono a disposizione di tutti i partecipanti al sistema della cartella informatizzata del paziente. Ciò è imperativo per consentire di cercare e trovare la cartella informatizzata del paziente. Anche gli accessi di emergenza possono essere effettuati solo se i dati demografici per la ricerca della cartella informatizzata del paziente sono utilizzabili. La ricerca mostra solo i dati demografici. L'accesso avviene in una seconda fase (mediante un diritto d'accesso attribuito o un accesso di emergenza autorizzato). Al momento di acconsentire all'apertura della cartella informatizzata del paziente, il paziente deve essere informato in merito a queste possibilità di trattamento dei dati, in modo che il suo consenso comprenda i relativi trattamenti dei dati. I processi di ricerca e di trattamento dei dati sono ricostruibili in ogni momento attraverso i verbali (log file).

Art. 2 Diritti d'accesso

L'articolo 2 disciplina le possibilità di attribuzione dei diritti d'accesso da parte del paziente. Le comunità

di riferimento devono garantire l'attuazione. Le disposizioni relative all'accesso di emergenza devono essere assicurate sia dalle comunità di riferimento, sia dalle comunità.

Secondo il *capoverso 1*, il paziente può accordare a professionisti della salute o a gruppi di professionisti della salute vari diritti d'accesso. È possibile avvalersi sia della possibilità di accordare il diritto d'accesso al grado di riservatezza «normalmente accessibile», che consente l'accesso ai soli dati normalmente accessibili, sia dell'opzione di accordare il diritto d'accesso a entrambi i gradi di riservatezza («normalmente accessibile» e «limitatamente accessibile»), corrispondente a un accesso più ampio. Solo il paziente può accedere al grado di riservatezza «segreto».

In situazioni di emergenza medica, anche i professionisti della salute ai quali non è stato accordato in precedenza un diritto d'accesso possono accedere alla cartella informatizzata del paziente (*cpv. 2*). In questo caso ottengono di norma l'accesso al grado di riservatezza «normalmente accessibile». Questa possibilità può essere sfruttata solo in caso di una situazione di emergenza medica, la cui esistenza è decisa esclusivamente sulla base di criteri medici. Come misura di emergenza contro un utilizzo abusivo dell'accesso di emergenza, per esempio mediante attacchi automatici a un terminale, l'accesso di emergenza deve essere confermato dal professionista della salute con un'interazione manuale e non riproducibile automaticamente (n. 2.2 lett. a allegato 2 OCIP-DFI). In questo contesto sono ipotizzabili ulteriori elementi di sicurezza, come ad esempio la ricezione di una password valida una sola volta o il reinserimento di un altro criterio di sicurezza. I professionisti della salute che figurano nell'elenco delle esclusioni non possono effettuare accessi di emergenza. Gli accessi di emergenza non sono possibili nemmeno se il paziente si è avvalso dell'opzione di negare l'accesso per le situazioni di emergenza medica (cfr. commenti all'art. 4 lett. e). In virtù del carattere eccezionale dell'accesso di emergenza, la legge prevede che il paziente sia informato in merito ad esso (art. 9 cpv. 5 secondo periodo LCIP). La comunità o comunità di riferimento nella quale avviene l'accesso di emergenza è responsabile per l'adempimento di questo obbligo d'informazione entro un termine adeguato (n. 2.2 lett. b allegato 2 OCIP-DFI). Tale obbligo può essere delegato alla struttura sanitaria nella quale è avvenuto l'accesso di emergenza o essere espletato in modo automatizzato a livello tecnico. Le modalità di attuazione dell'obbligo d'informazione (il paziente può essere informato dell'accesso di emergenza p. es. per lettera, e-mail o SMS) sono a discrezione delle comunità. Se comunica attraverso un canale non sicuro, l'organismo che fornisce l'informazione deve assicurarsi che l'informazione non contenga dati medici (n. 2.2 lett. c allegato 2 OCIP-DFI).

Per motivi di praticità, i diritti d'accesso possono anche essere attribuiti in modo generico a gruppi di professionisti della salute (p. es. un tumor board o un reparto di un ospedale). Questo comporta che il paziente possa cercare il gruppo in questione attraverso il servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute (art. 41 OCIP) e prendere conoscenza della sua composizione. Il *capoverso 3* prevede che, in seno ai gruppi di professionisti della salute, i diritti d'accesso dipendano dall'appartenenza al gruppo: il professionista della salute che aderisce a un gruppo ottiene il diritto d'accesso accordato a tale gruppo. Questa disposizione garantisce che il professionista della salute ottenga l'accesso alle informazioni necessarie per il trattamento. Quando il professionista della salute lascia un gruppo, il diritto d'accesso legato a tale gruppo gli viene revocato automaticamente.

Art. 3 Durata dei diritti d'accesso

L'*articolo 3* disciplina la durata dei diritti d'accesso accordati.

Secondo il *capoverso 1*, i diritti d'accesso accordati ai professionisti della salute valgono fino alla loro revoca da parte del paziente. La legislazione non prevede una scadenza specifica. Tuttavia, esiste l'opzione di limitare nel tempo i diritti d'accesso (cfr. commenti all'art. 4 lett. d).

Secondo il *capoverso 2* il paziente deve stabilire una scadenza per i diritti d'accesso accordati ai gruppi di professionisti della salute. Questa prescrizione è applicata per motivi di proporzionalità. È giustificata da una parte dal fatto che un trattamento in una struttura sanitaria stazionaria non si protrae di norma

per un periodo prolungato. Dall'altra, dal momento che nel caso di diritti d'accesso di gruppo il numero dei professionisti della salute autorizzati è sempre superiore a quello delle persone effettivamente coinvolte nel trattamento, lo svantaggio insito nella natura del diritto d'accesso di gruppo viene compensato dal fatto che il paziente deve decidere consapevolmente in merito alla durata di tali diritti. Come sostegno alla decisione, la comunità di riferimento può ad esempio offrire al paziente una serie di possibili scadenze.

Art. 4 Opzioni del paziente

Per quanto concerne l'applicazione dei gradi di riservatezza e l'attribuzione dei diritti d'accesso, il paziente ha a disposizione varie opzioni, elencate all'*articolo 4*. Le comunità di riferimento devono garantire l'attuazione. Le disposizioni relative all'accesso di emergenza devono essere assicurate sia dalle comunità di riferimento, sia dalle comunità.

Secondo la *lettera a*, il paziente può stabilire il grado di riservatezza da attribuire ai nuovi dati medici registrati. Può adeguare l'impostazione in modo che ai nuovi dati registrati sia attribuito il grado di riservatezza «limitatamente accessibile». Con questa opzione il paziente può attribuire fin dall'inizio un grado di riservatezza con possibilità d'accesso più restrittive ai dati che ritiene chiaramente sensibili. È il caso ad esempio di una diagnosi che può comportare una stigmatizzazione della persona. Naturalmente il paziente può ritornare in ogni momento all'impostazione standard «normalmente accessibile».

Secondo la *lettera b*, il paziente ha la possibilità di negare a singoli professionisti della salute l'accesso alla sua cartella informatizzata (cfr. art. 9 cpv. 3 LCIP). I professionisti della salute in questione sono inseriti in un cosiddetto «elenco delle esclusioni». Anche singoli professionisti della salute di un gruppo definito possono essere nell'elenco delle esclusioni. L'elenco delle esclusioni ha la precedenza. L'accesso a questi professionisti della salute è sempre negato, anche se sono membri di un gruppo al quale è attribuito un diritto d'accesso di gruppo. I professionisti della salute presenti in questo elenco non possono effettuare nemmeno accessi di emergenza.

Secondo la *lettera c*, il paziente può scegliere di essere informato sull'adesione di professionisti della salute ai gruppi ai quali ha accordato un diritto d'accesso (cfr. commenti all'art. 9 cpv. lett. f). In questo modo i pazienti possono verificare la composizione del gruppo se necessario ed eventualmente revocare a nuovi membri del gruppo il diritto d'accesso ottenuto automaticamente in virtù dell'ingresso nel gruppo.

Secondo la *lettera d*, il paziente ha la possibilità di fissare a sua discrezione una scadenza per i diritti d'accesso dei professionisti della salute. Così si garantisce che i professionisti della salute che probabilmente saranno coinvolti nel trattamento solo una volta o per breve tempo non possano accedere alla cartella informatizzata del paziente per un tempo sproporzionato. I diritti d'accesso provvisori decadono dopo la scadenza fissata senza ulteriori azioni da parte del paziente. In questo modo si riduce il rischio che i diritti d'accesso siano «dimenticati».

La *lettera e* conferisce al paziente la possibilità, per situazioni di emergenza medica, di estendere il diritto d'accesso al grado di riservatezza «limitatamente accessibile» o negare l'accesso.

Secondo la *lettera f*, il paziente ha la possibilità di nominare un rappresentante che può accedere a suo nome alla cartella informatizzata del paziente e anche attribuire i gradi di riservatezza e i diritti d'accesso. Non vi è un limite al numero di rappresentanti. I rappresentanti non necessitano né di un proprio numero d'identificazione del paziente né di una propria cartella informatizzata, ma possono accedere alla cartella informatizzata della persona rappresentata solo con il proprio strumento d'identificazione. Questa disposizione consente ad esempio a un familiare o ad altre persone di fiducia di rappresentare un bambino o una persona anziana.

Secondo la *lettera g*, il paziente ha la possibilità di autorizzare i professionisti della salute della sua comunità di riferimento a trasferire i diritti d'accesso loro accordati ad altri professionisti della salute o anche a gruppi di professionisti della salute. Le due opzioni sono disponibili indipendentemente l'una dall'altra. Il professionista della salute può trasferire il diritto d'accesso al massimo nella misura che gli è stata accordata.

Capitolo 2: Numero d'identificazione del paziente

Art. 5 Formato

Il *capoverso 1* definisce il formato e la composizione del numero d'identificazione del paziente secondo l'articolo 4 LCIP. Il numero d'identificazione del paziente è composto da 18 cifre compresa una cifra di controllo e la sua struttura si rifà a quella del «global service relation number» (GSRN) di GS1 (cfr. immagine). Il numero di base comprende un codice Paese e un numero di partecipante, che fa riferimento all'UFSP. Secondo la struttura di numerazione di GS1, il numero d'identificazione è composto da dieci cifre. La prima cifra del numero d'identificazione è utilizzata per definire il caso d'applicazione «cartella informatizzata del paziente». La serie di numeri può quindi essere ampliata per altri casi d'applicazione.

Cifra	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}
Designazione	Codice Paese		Numero partecipante					CIP	Numero d'identificazione									Cifra di controllo
Valore	**7**	**6**	**1**	**3**	**3**	**7**	**6**	**1**	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	$\mathbf{I_7}$	$\mathbf{I_8}$	$\mathbf{I_9}$	**C**

Il numero d'identificazione del paziente è gestito dall'UCC ed è attribuito in modo univoco al paziente all'apertura di una cartella informatizzata. È un numero non parlante e, conformemente al *capoverso 1*, non deve permettere di risalire all'identità del paziente o al suo numero d'assicurato secondo l'articolo 50*c* LAVS (NAVS13).

Le prescrizioni per la strutturazione del numero d'identificazione del paziente e per il calcolo della cifra di controllo sono definite nell'allegato 1 OCIP-DFI.

Art. 6 Domanda di attribuzione

La comunità di riferimento del paziente è competente per l'apertura della cartella informatizzata (art. 15 segg.). Pertanto il *capoverso 1* stabilisce che la comunità di riferimento è competente per la richiesta del numero d'identificazione del paziente all'UCC secondo *l'articolo 17 capoverso 1 lettera d* (cfr. art. 4 cpv. 1 LCIP). Il paziente deve prima essere identificato secondo il n. 8.2.1 lettera a allegato 2 OCIP-DFI.

I *capoversi 2 e 3* riguardano la garanzia di qualità nell'ambito dell'attribuzione del numero d'identificazione del paziente. Di norma, per identificare in modo univoco il paziente nella banca dati d'identificazione dell'UCC e per attribuirgli un numero d'identificazione del paziente dovrebbero essere sufficienti i dati di cui al *capoverso 2*. Il *capoverso* 3 conferisce all'UCC la facoltà di richiedere dati aggiuntivi in caso di situazioni non chiare.

Se il paziente non è presente nella banca dati d'identificazione dell'UCC o non possiede un numero d'assicurato secondo l'articolo 50*c* LAVS, la comunità di riferimento può richiedere all'UCC un numero d'assicurato, che servirà esclusivamente all'attribuzione di un numero d'identificazione del paziente.

Art. 7 Consultazione e registrazione

La consultazione, che comprende anche l'attribuzione (art. 6) e l'annullamento (art. 8) del numero d'identificazione del paziente, può svolgersi mediante procedura elettronica di richiamo.

Art. 8 Annullamento

Se un paziente revoca il suo consenso, la cartella informatizzata del paziente è soppressa ai sensi *dell'articolo 21*. L'UCC deve essere informato di ogni soppressione e il numero d'identificazione del paziente, in quanto parte della cartella informatizzata del paziente, deve essere annullato nella banca dati d'identificazione dell'UCC (cpv. *1*). Pertanto, non sarà più disponibile per le consultazioni secondo *l'articolo 7*.

Secondo il *capoverso 2*, l'UCC informa le comunità e le comunità di riferimento dell'annullamento del numero d'identificazione del paziente nell'ambito di una procedura di broadcast attraverso la piattaforma per lo scambio di dati SEDEX («secure data exchange») dell'Ufficio federale di statistica (n. 2.9.29 allegato 2 OCIP-DFI).

Il *capoverso 3* stabilisce che un numero d'identificazione del paziente annullato non può essere riattribuito, per evitare la possibilità di un riferimento errato. Se, dopo aver revocato la precedente, il paziente apre una nuova cartella informatizzata del paziente, a quest'ultima è attribuito un nuovo numero d'identificazione del paziente.

Capitolo 3: Comunità e comunità di riferimento

Sezione 1: Comunità

Se non altrimenti specificato, le disposizioni di questa sezione (art. da 9 a 13) si riferiscono sempre alle comunità e alle comunità di riferimento. Le disposizioni della sezione 2 (art. da 14 a 21) e i relativi commenti valgono solamente per le comunità di riferimento.

Art. 9 Identificatore di oggetto e gestione

Secondo il *capoverso 1* le comunità devono richiedere un identificatore di oggetto (object identifier, OID) al servizio di ricerca di dati degli OID secondo l'articolo 39 lettera d, per sé stesse e per le strutture sanitarie ad esse affiliate (cfr. commenti all'art. 42).

Secondo il *capoverso 2, l*e comunità sono tenute a prevedere (vale a dire definire, documentare e comunicare) e rispettare o prescrivere misure adeguate (vale a dire direttive, processi, procedure, strutture organizzative e responsabilità) e ad esigerne il rispetto, al fine di gestire le strutture sanitarie (p. es. ospedali, farmacie, studi medici, organizzazioni per la cura e l'assistenza a domicilio, case di cura), professionisti della salute e gruppi di professionisti della salute secondo i requisiti descritti.

Le condizioni tecniche e organizzative di certificazione nell'allegato 2 OCIP-DFI concretizzano i requisiti richiesti per la gestione di strutture sanitarie, professionisti della salute e ausiliari nonché gruppi di professionisti della salute di cui ai n. 1.2-1.6.

Gestione di strutture sanitarie

La *lettera a* stabilisce che siano disciplinate in particolare le modalità di ingresso di nuovi membri e di uscita di strutture sanitarie, professionisti della salute e gruppi di professionisti della salute che lasciano la comunità.

Il processo di ingresso comprende tra l'altro la stipula di una convenzione, nella quale la struttura sanitaria s'impegna a rispettare le prescrizioni organizzative interne di una comunità e in particolare i compiti e gli obblighi nell'ambito della protezione e della sicurezza dei dati (n. 1.2.2 nonché 4.9 allegato

2 OCIP-DFI). Nel quadro di questa convenzione la comunità può inoltre delegare alcune condizioni di certificazione alle strutture sanitarie ad essa affiliate. Tra queste condizioni rientrano in particolare la gestione dei professionisti della salute e dei gruppi di professionisti della salute che lavorano nella struttura sanitaria in questione (cpv. 2 lett. a–d). L'ammissione, la mutazione o l'uscita di un professionista della salute presuppone inoltre che la sua struttura sanitaria abbia già aderito alla comunità.

Inoltre, in caso di uscita di una struttura sanitaria che non aderisce a un'altra comunità o comunità di riferimento, la comunità deve garantire che i dati medici registrati negli archivi di documenti per la cartella informatizzata del paziente della struttura sanitaria uscente rimangano accessibili (n. 1.2.3 lett. b allegato 2 OCIP-DFI).

Secondo la *lettera d*, le comunità devono garantire che i dati delle strutture sanitarie ad esse affiliate siano aggiornati o siano mantenuti aggiornati dalle strutture sanitarie nell'ambito del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'*articolo 41*. Dal momento che questo servizio di ricerca di dati rappresenta la base per l'attribuzione dei diritti d'accesso ai professionisti della salute o ai gruppi di professionisti della salute, è necessario che i dati siano aggiornati con frequenza. Le comunità possono delegare questo compito alle strutture sanitarie, ma restano responsabili per la correttezza e l'aggiornamento dei dati registrati e devono garantire che le modifiche siano apportate in tempi ragionevoli, vale a dire nella maggior parte dei casi probabilmente ogni giorno (n. 1.2.4 allegato 2 OCIP-DFI).

Dalle prescrizioni relative alla gestione di un registro dei mezzi informatici e delle raccolte di dati di cui all'articolo 12 capoverso 1 lettera b e dalle misure concrete di cui al n. 4.6 allegato 2 OCIP-DFI deriva inoltre che le comunità devono mantenere aggiornato tale registro nell'ambito della gestione delle strutture sanitarie (ingresso, mutazione, uscita).

Gestione dei professionisti della salute

Secondo la *lettera a,* le comunità devono definire, documentare, attuare e rispettare o esigere processi adeguati per gestire i professionisti della salute che dovranno accedere alla cartella informatizzata del paziente nell'ambito delle strutture sanitarie affiliate alla comunità. Oltre ai requisiti di cui alle *lettere b, d, e* ed *f*, i processi devono garantire il rispetto di ulteriori prescrizioni (n. 1.3, 1.4, 1.6 e 4.7 allegato 2 OCIP-DFI), tra cui in particolare l'informazione dei professionisti della salute in merito ai loro compiti, diritti e doveri nell'ambito del trattamento dei dati dati della cartella informatizzata del paziente (n. 4.7.1 allegato 2 OCIP-DFI) nonché la comunicazione a queste figure dei rischi e delle misure nei settori della protezione e della sicurezza dei dati. Le comunità devono inoltre attuare procedure per il consenso dei professionisti della salute alle direttive specifiche della comunità o a quelle delle strutture sanitarie basate su di esse (n. 1.2.2 lett. b allegato 2 OCIP-DFI).

Le comunità devono inoltre stabilire la procedura concreta in caso di uscita di un professionista della salute da una comunità (p. es. in seguito a un cambio d'impiego, alla cessazione dell'attività professionale o al decesso). In caso di uscita ma anche di cambio del settore di attività in seno alla comunità, si dovrà verificare in particolare se i presupposti per l'accesso alla cartella informatizzata del paziente continuano a sussistere (cfr. la definizione di professionista della salute secondo l'art. 2 lett. b LCIP). In caso contrario le possibilità d'accesso (login) alla cartella informatizzata del paziente andranno bloccate immediatamente (n. 1.3.5 lett. b allegato 2 OCIP-DFI). L'ammissione, la mutazione o l'uscita di un professionista della salute presuppone necessariamente che la sua struttura sanitaria abbia già aderito alla comunità. La comunità può trasferire i compiti relativi alla gestione dei professionisti della salute alle strutture sanitarie ad essa affiliate.

L'identificazione di un professionista della salute secondo la *lettera b* deve soddisfare i requisiti di cui all'*articolo 24*, se non può essere effettuata mediante uno strumento d'identificazione di un emittente certificato secondo l'*articolo 31*. Inoltre, la comunità deve garantire che si tratti di un professionista della salute secondo l'articolo 2 lettera b LCIP (n. 1.3.3 lett. c allegato 2 OCIP-DFI), vale a dire di uno

specialista del settore sanitario riconosciuto dal diritto federale o cantonale che presta cure ai pazienti. A tale scopo è possibile utilizzare uno strumento d'identificazione per il quale l'emittente abbia verificato la qualifica professionale nell'ambito dell'emissione secondo l'articolo 25 capoverso 3 oppure basarsi sull'iscrizione in un registro federale o cantonale (p. es. Registro delle professioni mediche [MedReg], Registro delle professioni psicologiche [PsyReg] o Registro nazionale delle professioni sanitarie [NAREG]). Per i professionisti della salute riconosciuti secondo il diritto federale o cantonale ma non iscritti in nessun registro professionale attuale, la procedura per la verifica dei diplomi può essere se del caso stabilita di concerto con le associazioni professionali cantonali o nazionali.

Secondo la *lettera c*, le comunità devono attribuire ai gruppi di professionisti della salute un OID basato sull'OID della comunità secondo il *capoverso 1* (cfr. commenti all'art. 42). L'attribuzione e l'assegnazione dell'OID a un gruppo avvengono da parte della comunità sotto la propria responsabilità. A tale scopo la comunità crea ulteriori OID interni a un livello inferiore a quello del nodo della struttura sanitaria e li attribuisce ai gruppi della struttura sanitaria in questione per la registrazione nel servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute secondo la *lettera d*.

Secondo la *lettera d* i dati dei professionisti della salute devono essere registrati, aggiornati o eventualmente eliminati nel servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute secondo l'*articolo 41*. Se il professionista della salute è iscritto in un registro professionale federale o cantonale (MedReg, NAREG ecc.), i dati in esso contenuti andranno ripresi per il servizio di ricerca di dati (n. 1.2.2 lett. d allegato 2 OCIP-DFI). I dati da riprendere (n. 1.9.5.1.2 supplemento 1 all'allegato 5 OCIP-DFI) comprendono cognome, nome e GLN del professionista della salute. Nel fare ciò si dovrà assicurare in particolare che il servizio di ricerca di dati riporti solo i professionisti della salute che corrispondono alla definizione di cui all'articolo 2 lettera b LCIP, che svolgono la propria attività per la struttura sanitaria in questione e che hanno la necessità di accedere alla cartella informatizzata del paziente. Per quanto concerne i dati registrati presso di essa, la comunità deve garantire che l'aggiornamento e la correttezza dei dati siano verificati regolarmente dalla comunità stessa o dalla struttura sanitaria responsabile dei dati (n. 1.2.4 allegato 2 OCIP-DFI). Anche questi compiti possono essere trasferiti alle strutture sanitarie ad essa affiliate. Tuttavia, la comunità resta responsabile per la correttezza e l'aggiornamento dei dati registrati.

Secondo la *lettera e,* l'accesso dei professionisti della salute alla cartella informatizzata del paziente deve avvenire esclusivamente utilizzando uno strumento d'identificazione rilasciato da un emittente certificato secondo l'*articolo 31* (n. 1.4.1 allegato 2 OCIP-DFI). In tale contesto è irrilevante se l'accesso avviene attraverso il portale d'accesso per i professionisti della salute (art. 11) o tramite altri sistemi (per esempio con un accesso integrato nel sistema primario). Ciò significa che tutti gli accessi utilizzati dai professionisti della salute o dagli ausiliari per consultare la cartella informatizzata del paziente devono supportare una procedura di autenticazione forte adeguata all'evoluzione della tecnica con almeno due fattori di autenticazione. Una tale procedura di autenticazione è obbligatoria solamente per l'elaborazione di dati della cartella informatizzata del paziente. Un'autenticazione avvenuta con queste modalità di altre comunità certificate va ritenuta affidabile nel quadro dell'elaborazione di dati della cartella informatizzata del paziente a livello intercomunitario.

Le comunità devono garantire che, sia per i professionisti della salute, sia per gli ausiliari, l'identificatore univoco di cui all'articolo 25 capoverso 1 sia collegato in modo affidabile con l'identità registrata della persona all'interno della comunità (n. 1.4.2 allegato 2 OCIP-DFI; fase di registrazione).

I professionisti della salute possono impiegare ausiliari per l'elaborazione di dati della cartella informatizzata del paziente. Per tutelare i diritti della personalità degli ausiliari, i loro dati non sono inseriti nel servizio di ricerca dei dati delle strutture sanitarie e dei professionisti della salute secondo l'*articolo 41*. Pertanto non possono essere gestiti come persone autonome nell'ambito dell'amministrazione dei diritti da parte del paziente. Tuttavia, il collegamento degli ausiliari al professionista della salute che ne è responsabile va gestito all'interno della comunità, affinché gli ausiliari possano utilizzare le autorizzazioni del professionista della salute responsabile e l'elaborazione dei dati che effettuano possa

essere verbalizzata. Per l'identificazione e l'accesso degli ausiliari sono determinanti le disposizioni di cui all'*articolo 9 capoverso 2 lettere b ed e* (n. 1.3 allegato 2 OCIP-DFI).

Gestione di gruppi di professionisti della salute
Secondo la *lettera d*, le comunità devono garantire la gestione di gruppi di professionisti della salute nel servizio di ricerca dei dati delle strutture sanitarie e dei professionisti della salute secondo l'*articolo 41*. Le comunità possono trasferire questo compito alle strutture sanitarie ad essa affiliate, ma restano responsabili per la correttezza e l'aggiornamento dei dati registrati.

I pazienti possono accordare i diritti d'accesso anche a gruppi di professionisti della salute (art. 2 cpv. 1). I professionisti della salute che aderiscono in un momento successivo al gruppo ottengono il diritto d'accesso legato a tale gruppo (art. 2 cpv. 3), ma solamente nel caso in cui il paziente non abbia negato in linea generale l'accesso a quello specifico professionista (art. 4 lett. b).

La *lettera f* stabilisce che i pazienti che lo richiedono debbano essere informati sull'ingresso di professionisti della salute in gruppi di professionisti della salute. Questa informazione può avvenire in modo automatico ed elettronico.

Le comunità dovrebbero definire la composizione dei gruppi e le loro dimensioni in modo che i pazienti possano gestire in modo adeguato i diritti d'accesso. In particolare, non vi dovrebbe essere un numero sproporzionato di professionisti della salute non concretamente coinvolti nel trattamento che ottiene l'accesso tramite il diritto attribuito a un gruppo. In linea di principio le comunità o le strutture sanitarie che vi aderiscono devono provvedere a chiarire come intendono organizzare le possibilità d'accesso alla cartella informatizzata del paziente, quali professionisti della salute necessitano poi di un accesso e come questi dovrebbero essere eventualmente inseriti in gruppi di professionisti della salute. L'organizzazione concreta dovrebbe rispettare il principio della proporzionalità ed essere adeguata allo svolgimento dei compiti. Dal momento che spesso negli ospedali il percorso terapeutico si snoda in più unità organizzative (p. es. pronto soccorso → laboratorio → radiologia → degenza di medicina interna), può essere utile organizzare i gruppi in modo da rappresentare in modo adeguato tutte le unità coinvolte. In alternativa è anche ipotizzabile definire gruppi che siano in primo luogo responsabili per l'acquisizione di dati medici nel sistema primario. Ad esempio, per i reparti più grandi o per le cliniche di un ospedale potrebbero essere definiti gruppi per i quali la composizione è in gran parte stabile e la disponibilità delle persone registrate è sempre garantita. Nell'ambito dell'accettazione del paziente, i membri di un tale gruppo possono poi trasferire i dati medici rilevanti per il trattamento nel sistema primario dell'ospedale, dove saranno accessibili ai professionisti della salute coinvolti nel trattamento del paziente all'interno della struttura sanitaria. In questo modo, l'inserimento nel servizio di ricerca dei dati delle strutture sanitarie e dei professionisti della salute di piani di servizio aggiornati giornalmente inerenti a reparti interni di un ospedale o una casa di cura non è né necessario, né opportuno ai fini della praticità o dell'utilità per il paziente. Per quanto concerne le organizzazioni di cura e assistenza a domicilio, le dimensioni dei gruppi possono variare a seconda del modello di assistenza scelto (principio di rotazione o sistema della persona di riferimento).

Art. 10 Conservazione e trasmissione di dati

Attuazione dell'amministrazione dei diritti
Secondo il *capoverso 1 lettera a*, le comunità devono attuare l'amministrazione dei diritti in modo tale che le prescrizioni secondo l'articolo 9 LCIP e le disposizioni per l'attribuzione ai gradi di riservatezza e per l'accesso di emergenza secondo gli *articoli 1 e 2 capoverso 2 OCIP* siano attuati ed effettuati in modo corretto (n. 2.1–2.3 allegato 2 OCIP-DFI). Per quanto concerne le comunità in particolare, deve essere ripresa l'attribuzione dei dati della cartella informatizzata del paziente a uno dei tre gradi di riservatezza (art. 1) effettuata dal paziente attraverso il portale d'accesso della sua comunità di riferimento (n. 2.3.1 allegato 2 OCIP-DFI).

Inoltre, le comunità devono garantire che gli accessi ai dati dei loro archivi e registri di documenti avvengano solo conformemente a una decisione d'accesso precedentemente ottenuta della comunità

di riferimento del paziente (n. 2.3 allegato 2 OCIP-DFI). Per un'ulteriore protezione dai cosiddetti attacchi «man-in-the-client», il n. 2.2 dell'allegato 2 OCIP-DFI esige inoltre che gli accessi di emergenza siano confermati con una modalità tale da evitare gli abusi, in particolare quelli causati da un software dannoso installato su un terminale. Tale modalità può essere rappresentata ad esempio da un'ulteriore interazione manuale non riproducibile automaticamente (p. es. tramite l'immissione di una password valida una sola volta o di un PIN generato da un token locale).

Dal momento che l'attuazione corretta dell'amministrazione dei diritti e l'esercizio affidabile dei diritti d'accesso sono cruciali per garantire la protezione dei dati, le funzioni e la corretta verifica della validità dell'amministrazione dei diritti devono poter essere verificate anche nell'ambito di scenari di test automatizzati all'interno della procedura di certificazione (2.3.2 allegato 2 OCIP-DFI).

Archivi dei dati

Per ragioni di protezione e di sicurezza dei dati, i dati medici della cartella informatizzata del paziente secondo la *lettera b* possono essere memorizzati solo separatamente da altre raccolte di dati della comunità o della comunità di riferimento, in modo che non possano essere utilizzati in modo abusivo per altri scopi. Non è consentito in particolare il trasferimento di dati medici da o verso gli archivi di documenti, a meno che questa operazione non sia effettuata da professionisti della salute. È però consentita la trasmissione diretta di dati medici ad altri professionisti della salute e strutture sanitarie tramite elementi dell'infrastruttura informatica della cartella informatizzata del paziente, a condizione che anche i destinatari siano membri di una comunità certificata.

Lo scopo di questa disposizione è che i dati medici della cartella informatizzata del paziente siano mantenuti separati da altri dati perlomeno da un punto di vista logico (n. 2.4 lett. b allegato 2 OCIP-DFI) e possano quindi essere salvati nei relativi archivi di dati come copie dei dati medici creati nei sistemi primari delle strutture sanitarie. Questa separazione è giustificata anche dal fatto che i dati della cartella informatizzata del paziente da una parte sottostanno a obblighi di conservazione ed eliminazione diversi da quelli necessari per i dati dei sistemi primari e dall'altra vengono distrutti integralmente dopo la soppressione della cartella informatizzata del paziente (cpv. 1 lett. e) o selettivamente su richiesta del paziente (cpv. 2 lett. c).

Inoltre, gli archivi di documenti senza una separazione efficace delle raccolte di dati rappresentano un rischio sproporzionato per la protezione e la sicurezza dei dati, in quanto tali sistemi non possono essere isolati in modo sufficientemente efficace da grandi gruppi di utenti e reti e vi sarebbe anche il rischio di una diffusione incontrollata di dati nella cartella informatizzata del paziente e viceversa.

L'isolamento da altre raccolte di dati deve garantire che, ad esempio, le persone che dispongono di diritti d'accesso privilegiati al sistema operativo o alla banca dati del sistema primario non possano accedere contemporaneamente ai dati medici della cartella informatizzata del paziente e ad altre raccolte di dati. Indipendentemente dal fatto che la separazione sia fisica (vale a dire hardware dedicato, centri di calcolo separati), logica (p. es. con banche dati separate, macchine virtuali, isolamento crittografico ecc.) o sia ottenuta con una combinazione di più misure, l'isolamento deve consentire una separazione sicura delle raccolte di dati a livello tecnico. Una permeabilità involontaria (fallimento dell'isolamento) dovuta a un guasto tecnico, a software dannosi o a un'azione umana non autorizzata va evitata il più possibile con strumenti tecnici adeguati ed eventualmente con l'integrazione di misure organizzative.

Un isolamento logico sufficiente può essere ottenuto ad esempio con un criptaggio a livello di applicazione, a condizione che le chiavi per le raccolte di dati siano protette da accessi non autorizzati. In questo modo sono possibili anche utilizzi ibridi di archivi di documenti sullo stesso hardware e lo stesso sistema operativo e con le stesse banche dati. Oltre alle procedure previste per i professionisti della salute (registrare, scaricare), può esistere solamente un ulteriore ruolo dotato dei privilegi di sistema che consentono un trasferimento affidabile dei dati dalla cartella informatizzata del paziente ad altre raccolte di dati (e viceversa). Per ridurre ulteriormente questo rischio residuo riguardante il

trasferimento dei dati non autorizzato, le chiavi a livello di applicazione o gli accessi corrispondenti devono essere messi in sicurezza e protetti in maniera idonea, ad esempio con ulteriori misure organizzative («segregation of duties», «principio del doppio controllo»).

Criptaggio

La *lettera c* stabilisce che per la memorizzazione e il trasferimento dei dati le comunità utilizzino metodi di criptaggio secondo l'attuale stato della tecnica, al fine di preservare i dati da una perdita di riservatezza, autenticità e integrità (n. 4.12 allegato 2 OCIP-DFI; cfr. commenti all'art. 12 cpv. 4).

Distruzione dei dati

La *lettera d* stabilisce che i dati registrati dai professionisti della salute nella cartella informatizzata siano distrutti dopo 20 anni. Lo scopo di questa disposizione è di garantire la disponibilità dei dati medici per un tempo sufficientemente lungo. I dati registrati dal paziente non sottostanno ad alcun termine di eliminazione. Secondo il *capoverso 2 lettera b* determinati dati possono essere esclusi dalla distruzione su richiesta del paziente. I pazienti possono così assicurarsi, in caso di dati con una rilevanza molto estesa nel tempo ai fini delle cure (p. es. in caso di patologie croniche o congenite), che questi restino disponibili nella cartella informatizzata anche oltre il termine prescritto.

In casi eccezionali giustificati da motivi tecnici, segnatamente per quanto concerne i sistemi di archiviazione di file con volumi di dati molto elevati, come spesso accade nella diagnostica per immagini ad esempio in radiologia, i dati e i documenti medici non devono essere resi disponibili in copia, ma possono essere consultati direttamente negli archivi integrati dei sistemi primari. In questi casi le prescrizioni inerenti all'eliminazione dei dati secondo il *capoverso 1 lettere d ed e* nonché secondo il *capoverso 2 lettera c* sono limitate alla relativa registrazione nel registro dei documenti.

Ai sensi della *lettera e*, una soppressione della cartella informatizzata del paziente secondo l'*articolo 21 capoverso 1* deve avere come conseguenza il ripristino dello stato precedente alla costituzione della cartella informatizzata del paziente. A tale scopo, tutti i dati del paziente devono essere distrutti in tutti i sistemi consultabili della comunità (registri di documenti, archivi di documenti, indice dei pazienti ecc.) e il numero d'identificazione del paziente deve essere eliminato da tutti i sistemi (n. 2.6 lett. b allegato 2 OCIP-DFI). La responsabilità di informare le altre comunità in merito alla soppressione di una cartella informatizzata del paziente spetta alla comunità di riferimento del paziente interessato (art. 21 cpv. 3). Questa disposizione non riguarda i verbali e i dati contenuti nei sistemi primari non consultabili e nei back up.

In virtù del principio dell'autodeterminazione in materia d'informazione, il paziente può decidere in merito al contenuto della propria cartella informatizzata. Da ciò derivano per il paziente le possibilità menzionate al *capoverso 2* (n. 2.7 allegato 2 OCIP-DFI).

Possibilità di scelta del paziente

All'articolo 3 capoverso 2, la LCIP stabilisce la presunzione che il paziente che ha acconsentito alla costituzione della cartella informatizzata accetti che i professionisti della salute vi registrino dati in caso di cura. Secondo il *capoverso 2 lettera a* il paziente può contestare questa presunzione in singoli casi e disporre in ogni momento che i professionisti della salute non registrino determinati dati nella sua cartella informatizzata. Di norma il paziente si avvale di questa possibilità nel caso di un trattamento concreto e quindi in contatto con una struttura sanitaria. Garantire ed esigere la relativa attuazione nelle strutture sanitarie spetta tuttavia alle comunità.

Secondo il *capoverso 2 lettera b* il paziente può richiedere in ogni momento che determinati dati siano esclusi dalla distruzione di cui al *capoverso 1 lettera d*, affinché questi restino disponibili a tempo indeterminato.

Il *capoverso 2 lettera c* conferisce ai pazienti il diritto di disporre che determinati dati medici che li riguardano siano distrutti nella loro cartella informatizzata. Ciò può avvenire a livello tecnico tramite una corrispondente funzione nel portale d'accesso della comunità di riferimento del paziente. Le comunità devono attuare tale disposizione di eliminazione (transazione *Delete Document Set* [ITI-62] del «profilo d'integrazione IHE» *XDS Metadata Update*; n. 2.9.13 e 2.9.14 allegato 2 OCIP-DFI) eliminando le corrispondenti registrazioni dai registri di documenti nonché i dati medici dagli archivi di documenti della cartella informatizzata del paziente. Per i dati medici che possono essere consultati direttamente dagli archivi di documenti dei sistemi primari (p. es. archivi di documenti integrati per file di immagini in radiologia) è necessario eliminare solamente la registrazione nel registro dei documenti, affinché non siano violati gli obblighi di documentazione e conservazione vigenti per i professionisti della salute.

Prescrizioni tecniche per la trasmissione dei dati

Per garantire l'interoperabilità e una disponibilità nonché una consultazione dei dati sicure e conformi alla protezione dei dati, le comunità devono rispettare le prescrizioni per la gestione e la trasmissione dei dati della cartella informatizzata del paziente di cui al *capoverso 3 lettere a-d*. Queste prescrizioni concretizzano ad esempio i tipi di media consentiti (elencati in modo esaustivo al n. 2.8 allegato 3 OCIP-DFI), la ricerca di pazienti nell'indice dei pazienti, la comunicazione con il registro dei documenti, l'archivio di documenti e l'amministrazione dei diritti, la comunicazione con l'emittente dello strumento d'identificazione nonché la comunicazione con i servizi di ricerca di dati di cui agli articoli 40 e 41. Il rispetto di questi requisiti rilevanti per l'interoperabilità ma anche per la protezione e la sicurezza dei dati è verificato nell'ambito della procedura di certificazione dagli organismi di certificazione tramite un sistema di test di certificazione messo a disposizione dall'UFSP (art. 28 cpv. 4). Ciò dovrà garantire non solo che la comunicazione tra tutti i componenti funzioni secondo il principio dell'interoperabilità a livello tecnico e semantico, ma anche che in ogni comunità siano disponibili le stesse interfacce standard per i sistemi primari da collegare. Per facilitare il collegamento conforme dei sistemi primari non ancora compatibili con IHE, i produttori hanno a disposizione un adattatore software («eHealth-Connector») la cui integrazione può semplificare il collegamento conforme dei loro prodotti alle interfacce all'interno della comunità. Se i prodotti sono già in grado di gestire nativamente le prescrizioni previste, l'«eHealth-Connector» non è necessario. Un collegamento standardizzato alle interfacce nelle comunità può essere visto come protezione degli investimenti per offerenti, utenti e comunità, in quanto una spesa effettuata una sola volta permette molteplici utilizzi.

Metadati

I metadati descrivono in modo strutturato i dati medici e i documenti messi a disposizione nella cartella informatizzata del paziente (p. es. formato tecnico del file, tipo di mittente, autore, data di creazione, grado di riservatezza attribuito). Secondo la *lettera a*, vanno utilizzati gli attributi dei metadati definiti all'allegato 3 OCIP-DFI nonché i loro valori o intervalli di valori consentiti. In tale contesto sono spesso impiegati elenchi di valori provenienti da codici semantici standardizzati (p. es. dalla terminologia «Snomed CT»), che garantiscono un'interoperabilità semantica dei metadati riferiti ai dati medici. Per assicurare un utilizzo uniforme a livello nazionale e supportato a livello tecnico dei metadati, la Confederazione gestisce il servizio di ricerca per i metadati consentiti secondo l'*articolo 39 lettera c*. Solo le caratteristiche (codice e designazione in inglese) riportate nell'allegato 3 OCIP-DFI hanno carattere normativo. Le traduzioni nelle lingue nazionali e in altre lingue nonché i termini colloquiali sono pubblicati da eHealth Suisse sotto forma di elenchi di sinonimi.

Tutti i tipi di dati medici classificabili tramite metadati possono essere messi a disposizione come dati non strutturati sotto forma di documenti (p. es. file contenenti immagini o PDF/A). Per la messa a disposizione di dati medici strutturati da parte di professionisti della salute, la *lettera c* stabilisce tuttavia che debbano essere utilizzati i formati di scambio per i contenuti medici previsti all'allegato 4 OCIP-DFI.

Profili d'integrazione

Secondo la *lettera c*, per la trasmissione delle informazioni all'interno delle comunità nonché tra comunità vanno utilizzate le transazioni dei profili d'integrazione di *Integrating the Healthcare Enterprise* (IHE) con i relativi adeguamenti nazionali («*national extensions*») riportati all'allegato 5 OCIP-DFI

nonché, per casi di applicazione specifici, le transazioni dei profili d'integrazione nazionali del DFI. I profili d'integrazione sono linee guida tecniche per l'attuazione secondo il principio dell'interoperabilità tecnica di specifici casi di applicazione, solitamente mediante utilizzo di norme e standard riconosciuti a livello generale.

I «profili d'integrazione IHE» riportati al n. 1 dell'allegato 5 OCIP-DFI sono riconosciuti a livello internazionale e quindi concepiti per un impiego universale. Affinché i requisiti concreti della LCIP e delle presenti disposizioni esecutive siano rispettati, sono di norma necessari ulteriori elementi di concretizzazione e definizione specifica (detti «adeguamenti nazionali»). Questi stabiliscono ad esempio che per determinate consultazioni possa essere utilizzato come identificatore solamente il numero d'identificazione del paziente e non il NAVS13. Al n. 2 dell'allegato 5 OCIP-DFI sono definiti anche profili propri del DFI, i cosiddetti «profili d'integrazione nazionali», che tengono conto delle particolarità dell'«Architettura eHealth Svizzera» alla base della cartella informatizzata del paziente, come ad esempio la conservazione decentrata dei dati e la gestione dei pazienti. Pertanto, il profilo d'integrazione nazionale CH:ADR (authorisation decision request) disciplina come le informazioni rilevanti ai fini dell'autorizzazione sono trasmesse alla comunità di riferimento che decide in merito all'accesso e come successivamente l'esito della verifica della validità del diritto d'accesso – la decisione d'accesso – è ritrasmesso alla comunità richiedente. Il profilo d'integrazione nazionale CH:PPQ (privacy policy query) invece consente di modificare la configurazione dell'amministrazione dei diritti da parte del paziente o dei professionisti della salute autorizzati a farlo. Di questo profilo d'integrazione nazionale fa parte anche il formato di scambio tecnico, da utilizzare per riprendere la configurazione dell'amministrazione dei diritti in caso di cambiamento della comunità di riferimento.

I requisiti validi per tutti i profili d'integrazione riguardano in particolare la garanzia dell'integrità e della riservatezza dei dati trasmessi. Per garantire l'integrità dei messaggi elettronici vanno pertanto utilizzati certificati elettronici affidabili, con i quali può essere verificata l'autenticità dei messaggi (n. 2.9.21 lett. b, 2.9.26, 2.9.28 lett. b e 2.9.29 allegato 2 OCIP-DFI). In questo contesto, per la marca temporale necessaria alla comunicazione e alla verbalizzazione dovrà essere utilizzata l'ora ufficiale in Svizzera, diffusa dall'Istituto federale di metrologia (METAS). Gli orologi di tutti i sistemi rilevanti per l'elaborazione dei dati devono pertanto essere sincronizzati con l'ora ufficiale in Svizzera (n. 2.9.30 allegato 2 OCIP-DFI).

Verbali

L'articolo 10 capoverso 1 lettera b LCIP prescrive che ogni trattamento di dati debba essere verbalizzato. Per il controllo della protezione dei dati, soprattutto da parte dei pazienti, è necessario che il trattamento dei dati della cartella informatizzata del paziente sia ricostruibile in modo adeguato attraverso una verbalizzazione significativa e a prova di revisione di tutti gli eventi rilevanti per la protezione dei dati.

Tra gli eventi da verbalizzare vi sono in particolare la messa a disposizione e la consultazione di dati medici, la modifica di metadati (p. es. grado di riservatezza), gli adeguamenti alla configurazione dell'amministrazione dei diritti nonché le decisioni di autenticazione e autorizzazione e i dati sulla base dei quali sono state prese tali decisioni. I verbali inerenti agli eventi devono contenere una serie di informazioni dettagliate (chi ha consultato o creato quali dati, quando e come). Il verbale deve inoltre distinguere tra accessi derivanti dall'utilizzo della cartella informatizzata del paziente e accessi tecnico-amministrativi nell'ambito della gestione del sistema (n. 4.13.3 allegato 2 OCIP-DFI). I requisiti dei verbali consultabili dai pazienti di cui alla *lettera d* sono concretizzati al n. 2.10 dell'allegato 2 OCIP-DFI.

I verbali devono essere protetti da modifiche con strumenti tecnici od organizzativi idonei, vanno conservati per dieci anni e poi distrutti (n. 2.10.7 e 2.10.8 allegato 2 OCIP-DFI).

Per concretizzare le disposizioni dell'*articolo 12 capoverso 4,* il n. 4.13.3 dell'allegato 2 OCIP-DFI formula ulteriori requisiti per i verbali, rilevanti ai fini della protezione e della sicurezza dei dati, per eventi nell'ambito della gestione del sistema, che non sono tuttavia previsti per la consultazione da parte dei

pazienti. Altre verbalizzazioni effettuate nell'ambito della gestione tecnica, non direttamente rilevanti per la protezione o la sicurezza dei dati (p. es. parametri di gestione o grandezze come frequenza delle ricerche, tempi di risposta o volumi di dati scambiati), non rientrano in questi requisiti, ma possono essere rilevanti per riconoscere gli incidenti relativi alla sicurezza secondo l'*articolo 12 capoverso 1 lettera a*.

Affinché il paziente possa consultare in ogni momento i verbali generati a livello decentrato, le comunità devono metterli a disposizione per la consultazione da parte dei pazienti attraverso il portale d'accesso (art. 18). Gli adeguamenti nazionali per la consultazione di verbali (per quanto concerne i profili d'integrazione IHE ATNA, XDS.b e XCA) al numero 2 dell'allegato 5 OCIP-DFI specificano le transazioni necessarie e il formato di scambio tecnico per la consultazione di verbali (n. 2.10.9 allegato 2 OCIP-DFI). Prendendo visione dei verbali nel portale d'accesso, il paziente può controllare costantemente chi ha avuto accesso alla sua cartella informatizzata e adire le vie legali in caso di un eventuale accesso non autorizzato (cfr. art. 24 LCIP).

Il *capoverso 4* prevede che il DFI possa rinunciare alla traduzione e alla pubblicazione ufficiale degli allegati dell'OCIP-DFI, e menzionarli soltanto con il titolo e un rimando all'ente presso cui possono essere ottenuti. Secondo l'*articolo 5 capoverso 1* della legge federale del 18 giugno 2004[7] sulle raccolte del diritto federale e sul Foglio federale (LPubb), la pubblicazione nella RU può essere evitata per i testi che concernono solo una cerchia ristretta di persone, sono di natura tecnica e si rivolgono solo a specialisti o devono essere pubblicati in un formato che non si presta alla pubblicazione nella RU. Questi testi possono essere consultati sull'homepage dell'UFSP. Per quanto concerne l'OCIP-DFI si rinuncia alla pubblicazione dell'allegato 2 (Condizioni tecniche e organizzative di certificazione per le comunità e le comunità di riferimento), 3 (Metadati), 4 (Formati di scambio), 5 (Adeguamenti nazionali dei profili d'integrazione e profili d'integrazione nazionali) e 8 (Condizioni tecniche e organizzative di certificazione degli emittenti di strumenti d'identificazione). Soprattutto per quanto concerne gli allegati 5 e 8 si tratta di requisiti prettamente tecnici, che si rivolgono a una cerchia molto ristretta di persone, vale a dire agli specialisti responsabili dell'implementazione tecnica. Inoltre, in applicazione dell'*articolo 14 capoverso 2 lettera b* LPubb, per gli allegati 3, 4, 5 e 8 è possibile rinunciare a una traduzione nelle lingue ufficiali, in quanto questi allegati sono utilizzati dagli interessati esclusivamente nella lingua corrente e universale per questo ambito specialistico (l'inglese). Una traduzione comporterebbe il rischio di interpretazioni errate o di una perdita d'informazioni (art. 10 cpv. 4).

L'articolo 12 capoverso 2 LCIP prevede che il Consiglio federale possa autorizzare l'UFSP ad adeguare all'evoluzione della tecnica i requisiti di certificazione, ma appare tuttavia più opportuno che sia il DFI a stabilire concretamente quali prescrizioni l'UFSP debba effettivamente adeguare (cpv. 5).

Art. 11 Portale d'accesso per i professionisti della salute

Il portale d'accesso per i professionisti della salute deve rispondere ai requisiti di cui al n. 3 dell'allegato 2 OCIP-DFI. Ad esempio la rappresentazione dei dati medici della cartella informatizzata del paziente deve riportare in modo corretto e completo tutte le informazioni rilevanti (n. 3.1 allegato 2 OCIP-DFI). Ciò vale in particolare per la rappresentazione di dati strutturati, come ad esempio i formati di scambio di cui all'articolo *10 capoverso 3 lettera b*. Inoltre, il portale d'accesso deve permettere di riconoscere chiaramente se i dati medici sono stati messi a disposizione da un professionista della salute o dal paziente stesso, quali dati medici non sono più validi o quali ulteriori versioni sono eventualmente disponibili. I dati medici messi a disposizione dai professionisti della salute non possono essere eliminati dagli stessi per ragioni di tracciabilità. Possono tuttavia essere dotati dell'informazione di stato «annullato» («deprecated»). Ciò permette ad esempio di sostituire informazioni errate od obsolete con dati medici corretti o più aggiornati. I pazienti, ma anche gli altri professionisti della salute, dovrebbero sempre visualizzare nel portale d'accesso solo la versione più aggiornata e non annullata dei dati medici o di un documento. In caso di necessità dovrebbe tuttavia essere possibile ripercorrere la cronologia delle varie versioni.

[7] RS **170.512**

Al fine di promuovere l'accesso senza barriere per i professionisti della salute con disabilità o limitazioni dovute all'età o alla lingua, i portali d'accesso devono essere organizzati in modo da consentire l'utilizzo senza barriere a questi gruppi di persone, ad esempio prevedendo la possibilità di lettura con programmi di sintesi vocale o la navigazione anche senza mouse. Determinante a tale scopo è il livello di conformità AA delle condizioni di conformità secondo le linee guida per l'accessibilità dei contenuti web 2.0 («Web Content Accessibility Guidelines 2.0»). Dal momento che molti requisiti sono vantaggiosi anche per l'utilizzo generale, il rispetto di queste linee guida rappresenta un valore aggiunto anche per gli altri utenti (n. 3.2 allegato 2 OCIP-DFI).

Per ragioni di interoperabilità e sicurezza dei dati, i tipi di media e i formati di file consentiti per la cartella informatizzata del paziente sono riportati con un elenco esaustivo al n. 2.8 dell'allegato 3 OCIP-DFI (n. 3.3 allegato 2 OCIP-DFI). Il portale d'accesso deve offrire la possibilità di mettere a disposizione, consultare e rappresentare questi tipi di media. Altri requisiti riguardano da una parte la possibilità di scaricare i dati medici e i documenti singolarmente ma anche raggruppati come selezione (n. 3.3 lett. c allegato 2 OCIP-DFI). D'altra parte bisogna garantire che i formati di scambio con dati medici strutturati siano non solo rappresentabili e scaricabili in forma leggibile dall'essere umano (n. 3.3 lett. d allegato 2 OCIP-DFI), ma possano anche essere scaricati nel formato originale strutturato (n. 3.3 lett. e allegato 2 OCIP-DFI), per poterli eventualmente elaborare ulteriormente in modo strutturato.

Affinché i professionisti della salute possano adempiere al loro obbligo di documentazione, il portale d'accesso deve supportare il richiamo di dati medici da memorizzare nel sistema primario della struttura sanitaria («download»). Per motivi di sicurezza, per il richiamo e il download di dati medici devono essere definiti limiti massimi del numero di singoli file (rate limit), che in caso di superamento attivano misure di blocco o misure di sicurezza supplementari (n. 3.3 lett. f allegato 2 OCIP-DFI). Ad esempio, il superamento del limite massimo potrebbe richiedere la compilazione preliminare di un cosiddetto CAPTCHA (completely automated public turing test to tell computers and humans apart), al fine di evitare consultazioni di massa automatiche non autorizzate.

Art. 12 Protezione e sicurezza dei dati

Secondo il *capoverso 1*, le comunità devono dotarsi di un sistema di gestione della protezione e della sicurezza dei dati adeguato ai rischi analogo alla norma ISO/IEC 27001:2013. Un tale sistema persegue un esame globale e coordinato dei rischi inerenti alla protezione e alla sicurezza dei dati della comunità, al fine di pianificare, introdurre, verificare e migliorare un ampio pacchetto di misure di sicurezza adeguate (direttive, processi, procedure, strutture organizzative nonché funzioni hardware e software ecc.) nel quadro di un sistema di gestione unitario. Devono essere tenute in considerazione in particolare la complessità e le dimensioni della comunità nonché soprattutto l'entità dei dati particolarmente degni di protezione all'interno della comunità (in particolare dati medici) della cartella informatizzata del paziente (n. 4.2.3 allegato 2 OCIP-DFI).

Le comunità sono responsabili di garantire il rispetto dei requisiti di questo articolo anche quando fanno eseguire prestazioni da terzi (organizzazioni di gestione) (n. 4.1 allegato 2 OCIP-DFI).

<u>Sistema di gestione della protezione e della sicurezza dei dati</u>
Il sistema di gestione della protezione e della sicurezza dei dati di cui si deve dotare una comunità deve definire e attuare misure adeguate volte a soddisfare le disposizioni qui menzionate. A tale scopo deve stabilire le responsabilità generali e specifiche per la gestione della protezione e della sicurezza dei dati, attribuirle alle persone responsabili e proteggere tutte le registrazioni rilevanti da smarrimento, distruzione e falsificazione.

Oltre ai requisiti summenzionati e di cui alle *lettere a–c*, il sistema di gestione della protezione e della sicurezza dei dati deve comprendere tra l'altro un catalogo dei rischi e un piano di trattamento dei rischi (n. 4.2.3 allegato 2 OCIP-DFI).

Secondo la *lettera a* deve essere allestito un sistema di monitoraggio e gestione degli incidenti relativi alla sicurezza (n. 4.3 allegato 2 OCIP-DFI). Dal momento che una situazione di totale sicurezza non è raggiungibile a priori, è particolarmente importante riconoscere tempestivamente almeno a posteriori eventuali incidenti relativi alla sicurezza, al fine di poter reagire con misure e processi definiti e con responsabilità chiare. Ciò può essere garantito costituendo un cosiddetto «security information and event management system» (SIEM), che permette ad esempio di identificare anomalie nel sistema e nei modelli di elaborazione, in modo da poterle affrontare in modo adeguato dal punto di vista tecnico e organizzativo. Il SIEM viene allestito in modo specifico per la comunità e dovrà pertanto tenere conto in particolare dell'esposizione e dell'evoluzione dei rischi specifiche per la comunità ed essere sempre adeguato ad esse. Riconosce e affronta almeno gli attacchi provenienti da Internet, la concentrazione anomala di accessi di lettura o scrittura agli archivi dei documenti, ai registri dei documenti o all'indice dei pazienti, che indicano utilizzi abusivi o attacchi automatizzati. Inoltre devono essere riconosciute e trattate le mutazioni inusuali e critiche dei diritti d'accesso nell'ambito della loro amministrazione o nel sistema di gestione delle identità e degli accessi (IAM). Ulteriori prescrizioni nell'allegato 2 OCIP-DFI riguardano ad esempio le modalità per riconoscere e affrontare le lacune di sicurezza nonché la protezione dai software dannosi (n. 4.4 e 4.5 allegato 2 OCIP-DFI).

Per affrontare incidenti relativi alla sicurezza noti, l'allegato 2 OCIP-DFI contiene, al n. 4.3.3, anche le prescrizioni relative alla comunicazione e al trattamento di eventi concernenti la protezione e la sicurezza dei dati. Ad esempio devono essere designati punti di contatto per la comunicazione di eventi concernenti la protezione e la sicurezza dei dati sia all'interno della comunità stessa, sia presso terzi incaricati ed essere definiti processi di emergenza idonei, a certe condizioni, a isolare i sistemi dal sistema generale («strategia di contenimento»). Ciò è necessario per limitare la potenziale entità dei danni o per non mettere a rischio anche altre parti vulnerabili del sistema. In adempimento al *capoverso 3* le comunità sono tenute a definire procedure formali per segnalare (notificare) all'UFSP gli eventi concernenti la protezione e la sicurezza dei dati particolarmente critici nonché a esigerne e controllarne il rispetto (n. 4.3.3 lett. a allegato 2 OCIP-DFI e commenti al cpv. 3).

Per quanto concerne l'approccio con le lacune di sicurezza, l'allegato 2 OCIP-DFI concretizza inoltre al n. 4.4 la responsabilità delle comunità di allestire una gestione (preventiva) delle stesse. Ciò significa in particolare che le informazioni sulle lacune di sicurezza esistenti o appena rilevate negli strumenti informatici impiegati (p. es. gli errori in componenti critici di software) sono trattate tempestivamente affinché – dopo la valutazione – possano essere avviate le contromisure adeguate (p. es. «patch» dei sistemi colpiti) (n. 4.13.2 lett. d allegato 2 OCIP-DFI).

Secondo la *lettera b* deve essere previsto in particolare un registro di tutti i mezzi informatici e delle raccolte di dati degni di protezioni utilizzati nella comunità per la cartella informatizzata del paziente («inventario dell'infrastruttura informatica») (n. 4.6 allegato 2 OCIP-DFI). Secondo il n. 4.6.2. lettera j dell'allegato 2 OCIP-DFI, tale inventario deve includere anche tutti i sistemi primari collegati, al fine di avere una panoramica su tutti i sistemi primari che scambiano dati con la cartella informatizzata del paziente. Questo inventario è parte integrante dell'«Inventario delle risorse rilevanti per la valutazione e il trattamento dei rischi» da stilare nell'ambito del sistema di gestione della protezione e della sicurezza dei dati. Gli elementi da inserire nell'inventario sono ulteriormente concretizzati al n. 4.2.3 lettera c allegato 2 OCIP-DFI e comprendono, oltre agli oggetti primari da proteggere, vale a dire i dati degni di protezione della cartella informatizzata del paziente, anche i processi per la loro elaborazione, in quanto immediatamente rilevanti per la protezione dei dati stessi (n. 4.2.3. lett. c cpv. i). Inoltre, nel quadro del sistema di gestione della protezione e della sicurezza dei dati devono essere protetti anche i cosiddetti oggetti secondari da proteggere. Tra questi vi sono soprattutto sistemi, infrastrutture e applicazioni ma anche dispositivi, strutture organizzative (organizzazioni interne interno incaricate della realizzazione del sistema, responsabilità ecc.), persone e processi da cui dipende la protezione degli oggetti primari da proteggere (n. 4.2.3. lett. c cpv. ii). Ad esempio è importante sapere quali sistemi gestiscono dati degni di protezione, da chi e come questi sono sorvegliati e cosa succede con le informazioni o quali processi di reazione e quali responsabilità esistono in caso di riconoscimento di un trattamento non autorizzato dei dati.

Dal momento che le organizzazioni e le loro risorse (strumenti informatici, raccolte di dati ma anche processi, strutture organizzative ecc.) e quindi anche la situazione di rischio sono esposte a una costante evoluzione, tutte le modifiche apportate alle suddette risorse rilevanti per la sicurezza devono essere valutate e documentate, affinché il sistema di gestione della protezione e della sicurezza dei dati possa operare con elementi aggiornati e corretti (n. 4.2.4 allegato 2 OCIP-DFI). Anche il catalogo dei rischi e il piano di trattamento dei rischi devono essere aggiornati al pari dell'«Inventario delle risorse rilevanti per la valutazione e il trattamento dei rischi» (n. 4.2.5 allegato 2 OCIP-DFI). Dal momento che, nell'ottica della protezione e della sicurezza dei dati, la gestione dei rischi rappresenta un tema strategico per un'organizzazione, il piano di trattamento dei rischi deve essere aggiornato regolarmente e approvato dalla direzione. Le linee guida rilevanti per garantire la protezione e la sicurezza dei dati devono inoltre essere rese note all'intera organizzazione.

Secondo la *lettera c*, le comunità devono definire tramite il sistema di gestione della protezione e della sicurezza dei dati prescrizioni specifiche in materia per le strutture sanitarie affiliate, nonché indirettamente anche per i loro professionisti della salute e per eventuali altri collaboratori, come ad esempio collaboratori attivi nell'ambito dell'informatica ospedaliera o terzi (n. 4.7-4.10 allegato 2 OCIP-DFI). Tra queste rientra ad esempio la prescrizione secondo cui le comunità devono obbligare le strutture sanitarie ad esse affiliate a informare i loro professionisti della salute che accedono alla cartella informatizzata del paziente sui loro compiti, diritti e doveri nell'ambito del trattamento dei dati della cartella informatizzata nonché in merito ai rischi e alle misure inerenti alla protezione e alla sicurezza dei dati (n. 4.7.1 lett. b allegato 2 OCIP-DFI, cfr. anche n. 1.2.2 lett. b e 1.3.3 lett. a allegato 2 OCIP-DFI). Le strutture sanitarie devono inoltre essere obbligate dalle comunità a garantire una configurazione sicura (p. es. tramite programmi di protezione dai software dannosi e misure di protezione a livello di rete) dei terminali utilizzati dai professionisti della salute per accedere alla cartella informatizzata del paziente (n. 4.7.1 e 4.7.2 allegato 2 OCIP-DFI). Le strutture sanitarie devono a loro volta obbligare i propri professionisti della salute a rispettare le misure richieste. Secondo il n. 4.7.3 dell'allegato 2 OCIP-DFI, le comunità devono garantire con misure idonee a livello organizzativo ed eventualmente tecnico, che i terminali con una configurazione non più considerata sicura non possano trattare i dati della cartella informatizzata del paziente. Bisognerà ad esempio evitare che terminali con sistemi operativi obsoleti e quindi non sicuri perché non più supportati dal produttore abbiano accesso ai dati della cartella informatizzata del paziente.

La comunità non può garantire la protezione e la sicurezza dei dati senza la collaborazione delle strutture sanitarie ad essa affiliate e di eventuali fornitori e prestatori di servizi. Pertanto secondo la *lettera c* devono rispettare i requisiti in materia di protezione e sicurezza dei dati, oltre ai professionisti della salute e ai collaboratori della comunità (p. es. personale del servizio di assistenza per i professionisti della salute), anche eventuali terzi coinvolti (p. es. organizzazioni di gestione o fornitori). Per quanto concerne il personale tecnico o amministrativo dei terzi menzionati, l'allegato 2 OCIP-DFI definisce in particolare i requisiti concernenti la gestione delle persone e dei loro accessi e diritti di utenti (n. 4.9 allegato 2 OCIP-DFI). Particolari prescrizioni sono applicate per persone con diritti di sistema («amministratori di sistema») estesi («privilegiati») per accessi a raccolte di dati e sistemi particolarmente degni di protezione (n. 4.9.1 allegato 2 OCIP-DFI). Queste cosiddette «persone chiave» possono rappresentare un rischio maggiore, se possono aggirare le misure di sicurezza esistenti. Per questo vanno segnalate al responsabile della protezione e della sicurezza dei dati e gestite da quest'ultimo. Queste persone sono selezionate secondo requisiti particolari e devono sottostare a requisiti di sicurezza delle comunità chiaramente definiti.

Inoltre, secondo i n. 4.9 e 4.10 dell'allegato 2 OCIP-DFI, ulteriori disposizioni sono applicate per la gestione dei fornitori, al fine di mantenere un livello di sicurezza sempre elevato per tutti gli attori coinvolti (comunità, strutture, fornitori e subfornitori) indipendentemente dalla struttura organizzativa. Ad esempio, le comunità sono tenute a estendere l'obbligo di rispetto dei requisiti in materia di protezione e sicurezza dei dati all'intera catena di fornitura, nel caso in cui i fornitori incarichino a loro volta un subfornitore (n. 4.9.4 lett. a ed e allegato 2 OCIP-DFI).

Responsabile della protezione e della sicurezza dei dati

Il *capoverso 2* prescrive che le comunità designino una persona indipendente a livello tecnico e organizzativo, responsabile della protezione e della sicurezza dei dati. Questa figura deve disporre delle competenze specialistiche, delle autorizzazioni e delle risorse necessarie ad assolvere tale compito. È responsabile dello sviluppo, dell'attuazione e della sorveglianza delle misure volte a garantire la protezione e la sicurezza dei dati, nonché dell'applicazione di misure correttive nell'ambito dello sviluppo costante della protezione e della sicurezza dei dati dell'organizzazione (n. 4.11 allegato 2 OCIP-DFI). Le comunità possono anche delegare a terzi l'esercizio operativo di questa funzione, ma restano responsabili per il rispetto dei requisiti.

Segnalazione di incidenti rilevanti per la sicurezza

L'obbligo di cui al *capoverso 3* di segnalare all'UFSP gli incidenti ritenuti rilevanti per la sicurezza, quindi particolarmente gravi, ha lo scopo di fornire le informazioni necessarie in merito a lacune individuate o sfruttate nell'organizzazione, al fine di avviare, se del caso e dopo le dovute analisi e valutazioni, misure per evitare ulteriori incidenti. In primo piano vi è l'acquisizione di conoscenze ed esperienze, non solo per le comunità stesse, ma anche per l'UFSP in qualità di autorità che disciplina la protezione e la sicurezza dei dati in questo ambito. Valutazioni regolari di questi eventi possono evidenziare eventuali tendenze nel panorama dei rischi, consentendo alle comunità di prevedere per tempo le contromisure del caso. In presenza di un pericolo grave per la protezione o la sicurezza dei dati della cartella informatizzata del paziente, l'UFSP può disporre ulteriori misure in applicazione della clausola di salvaguardia di cui all'*articolo 37*. Le comunità e le loro organizzazioni di gestione possono inoltre avvalersi anche delle prestazioni volontarie di consulenza e informazione della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) della Confederazione, che mette a disposizione della clientela preziose informazioni su pericoli attuali e misure idonee e incentiva lo scambio d'informazioni tra i gestori di infrastrutture critiche o a rischio.

Ulteriori requisiti

In applicazione del *capoverso 4*, ai n. 4.12-4.18 allegato 2 OCIP-DFI, il DFI stabilisce ulteriori requisiti concernenti la protezione e la sicurezza dei dati. Questi comprendono tra l'altro prescrizioni relative ai seguenti ambiti:

- criptaggio nella comunicazione e nella memorizzazione dei dati nonché gestione delle chiavi crittografiche (n. 4.12 allegato 2 OCIP-DFI);
- sicurezza d'esercizio, ripristino del sistema e verbalizzazione del funzionamento del sistema (n. 4.13 allegato 2 OCIP-DFI – i verbali tecnico-amministrativi nell'ambito del funzionamento del sistema secondo il n. 4.13.3 allegato 2 OCIP-DFI servono innanzitutto alla verifica del rispetto delle prescrizioni in materia di sicurezza e protezione dei dati in riferimento al singolo caso. Per tale ragione devono essere accessibili solo alle persone o agli organi che sorvegliano l'attuazione delle prescrizioni (n. 4.13.3 lett. g allegato 2 OCIP-DFI) e devono essere protetti da modifiche non autorizzate o passate inosservate (n. 4.13.3 lett. h allegato 2 OCIP-DFI);
- acquisto, sviluppo sicuro e manutenzione di sistemi (n. 4.14 allegato 2 OCIP-DFI);
- gestione di reti e servizi di rete nonché delle sessioni di rete (n. 4.15-4.16 allegato 2 OCIP-DFI);
- memorizzazione temporanea (n. 4.17 allegato 2 OCIP-DFI);
- disponibilità (n. 4.18 allegato 2 OCIP-DFI).

Al fine di garantire la massima sicurezza possibile per i dati della cartella informatizzata del paziente anche dal punto di visto giuridico, secondo il *capoverso 5* i supporti di memoria dei dati devono trovarsi in Svizzera e sottostare al diritto svizzero. La gestione può pertanto essere effettuata solo da persone giuridiche soggette al diritto svizzero (n. 4.19 allegato 2 OCIP-DFI). In questo modo i dati non sono sottoposti a una legislazione divergente da quella svizzera. Eventuali incongruenze con norme giuridiche estere possono così essere evitate a priori.

Art. 13 Servizio di assistenza per i professionisti della salute

Le comunità devono garantire che tutti i professionisti della salute abbiano a disposizione un contatto per il supporto tecnico e funzionale nell'utilizzo della cartella informatizzata del paziente («service

desk»). Per i collaboratori del «service desk» valgono prescrizioni e requisiti specifici (n. 5.1.2 allegato 2 OCIP-DFI). Questi devono essere informati in merito ai loro compiti, diritti e doveri, nonché ai rischi e alle misure concernenti la protezione dei dati e la sicurezza delle informazioni e sottostare a un obbligo analogo a quello del segreto professionale medico. Un accesso remoto ai terminali dei professionisti della salute può avvenire solo se l'utente stesso ne è a conoscenza e vi acconsente e deve essere documentato.

Sezione 2: Comunità di riferimento

I seguenti commenti riguardano le disposizioni della sezione 2 (art. da 14 a 21 OCIP), applicabili esclusivamente alle comunità di riferimento.

Art. 14 Requisiti supplementari per le comunità di riferimento

Le comunità di riferimento, vale a dire le comunità presso le quali i pazienti creano una cartella informatizzata del paziente e possono gestire i diritti d'accesso, devono rispettare, oltre alle prescrizioni di cui alla sezione 1 (art. da 9 a 13), anche quelle di cui alla sezione 2 (art. da 14 a 21).

Art. 15 Informazione del paziente

Il consenso del paziente deve essere accompagnato da un'informazione adeguata e obiettiva, di cui è responsabile la comunità di riferimento del paziente. Il paziente deve essere informato in modo completo e comprensibile in merito allo scopo della cartella informatizzata del paziente, alla procedura di costituzione e al funzionamento della stessa. Deve essere in grado di valutare quali ripercussioni comportano la concessione del consenso, le diverse impostazioni di amministrazione dei diritti d'accesso nonché una revoca. Se le informazioni sono assenti o insufficienti, la portata e la validità del consenso concesso sono limitate di conseguenza.

Le informazioni devono comprendere perlomeno i punti indicati al *capoverso 1* (n. 6.1 allegato 2 OCIP-DFI).

Secondo la *lettera a*, il paziente deve essere informato in merito allo scopo della cartella informatizzata (n. 6.1.1 allegato 2 OCIP-DFI). In questa definizione rientrano le informazioni sugli scopi della cartella informatizzata menzionati all'articolo 1 LCIP (qualità del trattamento, sicurezza del paziente, efficienza e alfabetizzazione sanitaria). Per una valutazione obiettiva delle opportunità e dei rischi della cartella informatizzata del paziente, può essere utile informare anche in merito agli scopi ai quali la cartella informatizzata non è destinata (nessun accesso da parte di assicuratori, datori di lavoro o autorità sanitarie).

Secondo la *lettera b*, devono essere spiegate le linee generali del trattamento dei dati nel contesto della cartella informatizzata del paziente (n. 6.1.2–6.1.5 allegato 2 OCIP-DFI). Si tratta in particolare di informare in merito alle possibilità di trattamento dei dati a disposizione del paziente o del suo rappresentante da una parte e dei professionisti della salute autorizzati all'accesso e dei loro ausiliari dall'altra. In queste spiegazioni di base rientrano anche le informazioni inerenti all'accesso d'emergenza e alle conseguenze di un'eventuale esclusione di tale accesso.

Secondo la *lettera c*, l'informazione deve comprendere anche l'avvertenza che la costituzione e l'utilizzo della cartella informatizzata del paziente sono facoltativi. Se il paziente ha dato il suo consenso alla costituzione di una cartella informatizzata, ai sensi dell'articolo 3 capoverso 2 LCIP è però lecito presumere che il paziente accetti in linea di principio la registrazione dei dati nella cartella informatizzata. Ciò significa che, se intende escludere determinate informazioni o trattamenti dalla cartella informatizzata, il paziente dovrà comunicarlo esplicitamente al professionista della salute che lo ha in cura (n. 6.1.2 lett. a allegato 2 OCIP-DFI). Le informazioni devono anche indicare che il paziente può revocare in ogni tempo il proprio consenso alla tenuta della cartella informatizzata senza indicarne i

motivi (art. 3 cpv. 3 LCIP; n. 6.1.3 allegato 2 OCIP-DFI). In questo contesto il paziente deve essere informato in merito alle conseguenze della revoca tra cui, ad esempio, il fatto che i dati medici di una cartella informatizzata revocata non saranno più disponibili in un'eventuale nuova cartella informatizzata aperta in seguito (n. 6.1.3 lett. g allegato 2 OCIP-DFI), dal momento che in caso di nuovo consenso viene attribuito un nuovo numero d'identificazione del paziente (cfr. commenti all'art. 8). Una cartella informatizzata del paziente aperta dopo una revoca è dunque una nuova cartella «vuota», che deve essere nuovamente riempita.

Secondo la *lettera d* le informazioni devono tra l'altro evidenziare come e a chi attribuire i diritti d'accesso a determinati dati medici (cfr. commenti agli art. 1–4). Il paziente deve essere informato in particolare in merito ai gradi di riservatezza (n. 6.1.4 allegato 2 OCIP-DFI), ai diritti d'accesso (n. 6.1.5 allegato 2 OCIP-DFI) e alle possibilità e opzioni di adeguamento, revoca e fissazione di una scadenza previste dall'articolo 4 nonché in merito alla possibilità di escludere completamente dall'accesso singoli professionisti della salute (cosiddetto elenco delle esclusioni; art. 4 lett. b).

Il *capoverso 2* prevede che il paziente sia informato sulle misure consigliate per la protezione e la sicurezza dei dati (n. 6.1.6 allegato 2 OCIP-DFI). Tra queste rientrano ad esempio indicazioni per un uso sicuro degli strumenti d'identificazione e delle informazioni di autenticazione segrete (p. es. password), le informazioni in merito ai rischi e le raccomandazioni di comportamento per difendersi da minacce e tentativi di frode rivolti ai pazienti come «social engineering», «phishing» e altri come pure consigli per l'utilizzo di terminali e browser Internet sicuri nonché per l'impiego di programmi di protezione contro software dannosi o attacchi alla rete.

Art. 16 Consenso

La legge prevede il consenso scritto. L'*articolo 16* precisa che il consenso deve essere firmato dal paziente. La prescrizione legale in merito alla forma deve essere rispettata anche se il consenso è impartito per via elettronica. Il diritto delle obbligazioni disciplina le condizioni secondo cui la firma elettronica è equiparata alla firma autografa, vale a dire quando è utilizzata una firma elettronica che adempie ai requisiti di cui all'articolo 14 capoverso 2bis CO[8] (firma elettronica qualificata ai sensi della legge sulla firma elettronica, FiEle[9]). Se questa condizione è soddisfatta, la forma scritta è ritenuta rispettata. La tracciabilità della concessione del consenso per via elettronica è garantita dalla verbalizzazione.

Art. 17 Gestione

Gestione dei pazienti

Secondo il *capoverso 1*, le comunità di riferimento devono definire, documentare, attuare e rispettare processi per l'apertura, la gestione e la soppressione della cartella informatizzata del paziente, nonché per l'identificazione e l'autenticazione dei pazienti (n. 8.1 allegato 2 OCIP-DFI).

La *lettera a* esige dalle comunità di riferimento disposizioni per i processi sovraordinati di apertura, gestione e soppressione della cartella informatizzata del paziente nonché per l'ingresso di un paziente nella comunità di riferimento e per l'uscita da essa. Determinanti per il processo d'ingresso sono le *lettere b–d*, le prescrizioni sull'informazione dei pazienti di cui all'*articolo 15*, nonché la disposizione inerente all'ottenimento del consenso all'*articolo 16*. Per il processo di soppressione di una cartella informatizzata del paziente sono determinanti le prescrizioni di cui all'*articolo 21*; i requisiti per il processo di cambiamento di comunità di riferimento sono concretizzati al n. 8.5 allegato 2 OCIP-DFI.

Qualora un paziente intenda costituire o revocare una cartella informatizzata oppure cambiare comunità di riferimento, è imperativo garantire che si tratti della persona corretta (n. 8.2 allegato 2 OCIP-DFI). A tal fine le comunità di riferimento devono identificare il paziente in modo sicuro (*lettera b)*. Concretamente, il n. 8.2.1 lettera a allegato 2 OCIP-DFI dispone che – se non è possibile effettuare

[8] RS **202**
[9] RS **943.03**

l'identificazione con uno strumento di un emittente certificato secondo l'*articolo 31* – devono essere soddisfatti i requisiti di cui all'articolo 24, vale a dire una verifica dell'identità mediante i documenti citati secondo la legge sui documenti d'identità o la legge sugli stranieri oppure mediante una domanda corredata di firma elettronica qualificata. Un'identificazione sicura e per quanto possibile univoca è non da ultimo anche la condizione per la corretta attribuzione del numero d'identificazione del paziente secondo la *lettera d*.

La *lettera c* stabilisce che le comunità di riferimento debbano garantire che – analogamente a quanto accade per i professionisti della salute (art. 9 lett. e) – l'accesso alla cartella informatizzata del paziente da parte dei pazienti e di eventuali rappresentanti sia possibile solo con uno strumento d'identificazione valido di un emittente certificato secondo l'*articolo 31* (n. 8.3 allegato 2 OCIP-DFI). Ciò significa che i portali d'accesso e i terminali utilizzati dai pazienti per consultare la cartella informatizzata del paziente devono supportare una procedura di autenticazione forte adeguata all'evoluzione della tecnica con almeno due fattori di autenticazione.

La *lettera d* stabilisce che, nell'ambito dell'apertura di una cartella informatizzata del paziente, le comunità di riferimento rispettino le prescrizioni degli articoli 6 e 7 per la richiesta del numero d'identificazione del paziente presso l'UCC (n. 8.2.1 lett. d allegato 2 OCIP-DFI). Secondo il n. 8.2.1 lettera b allegato 2 OCIP-DFI, la comunità di riferimento deve inoltre adoperarsi affinché, prima della costituzione di una cartella informatizzata, sia verificato che il paziente non ne possieda già una e quindi che per questa persona non esista un numero d'identificazione del paziente già attivo presso l'UCC. Ciò garantisce che in un dato momento esista al massimo una sola cartella informatizzata intestata a un paziente e che i suoi dati medici siano sempre attribuiti esclusivamente a questa cartella.

Ulteriori prescrizioni all'allegato 2 OCIP-DFI riguardano l'obbligo di riprendere i dati demografici dell'UCC e del numero d'identificazione del paziente nell'indice dei pazienti (n. 8.2.1 lett. e allegato 2 OCIP-DFI) nonché l'attribuzione corretta dell'identificatore univoco secondo l'articolo 25 capoverso 1 OCIP alla cartella informatizzata del paziente giusto (n. 8.2.2 allegato 2 OCIP-DFI).

La *lettera e* garantisce che i pazienti possano cambiare la propria comunità di riferimento. Il n. 8.5.2 allegato 2 OCIP-DFI dispone pertanto che le comunità di riferimento debbano garantire di essere in grado di trasferire la configurazione individuale dell'amministrazione dei diritti (policy configuration) a una nuova comunità di riferimento e di riprendere a loro volta una tale configurazione da un'altra comunità di riferimento. Indipendentemente dalla realizzazione tecnica interna e dalla rappresentazione della configurazione dell'amministrazione dei diritti, le comunità di riferimento devono essere in grado di esportarla in un formato che rispetti i principi dell'interoperabilità (basato sullo standard XACML) e di riprendere una tale esportazione nella propria amministrazione dei diritti. Determinante per lo scambio della configurazione è il formato specificato del profilo d'integrazione nazionale CH:PPQ del DFI secondo il n. 2 dell'allegato 5 OCIP-DFI. Dal momento che l'amministrazione dei diritti può avvenire solo all'interno della propria comunità di riferimento, i professionisti della salute possono trasferire i diritti d'accesso secondo l'*articolo 4 lettera g* solo se sono registrati nella comunità di riferimento del paziente che li autorizza. Pertanto, in caso di cambiamento della comunità di riferimento, è possibile che sia necessario autorizzare professionisti della salute della nuova comunità di riferimento. Anche i rappresentanti dei pazienti devono essere nuovamente registrati nella nuova comunità di riferimento.

<u>Attuazione dell'amministrazione dei diritti</u>
Secondo il *capoverso 2*, le comunità di riferimento devono soddisfare le condizioni tecniche e organizzative per garantire anche l'attuazione delle disposizioni dell'articolo 2 capoversi 1 e 3, dell'articolo 3 e dell'articolo 4 (cfr. commenti agli articoli citati nonché n. 8.6 allegato 2 OCIP-DFI).

L'attuazione dell'articolo 4 lettera f (nomina di un rappresentante) comporta, oltre all'attuazione tecnica, anche altri compiti organizzativi, descritti concretamente al n. 8.4 dell'allegato 2 OCIP-DFI. I rappresentanti non necessitano né di un proprio numero d'identificazione del paziente né di una propria

cartella informatizzata del paziente, ma possono accedere alla cartella informatizzata della persona rappresentata solo con il proprio strumento d'identificazione di un emittente certificato secondo l'articolo 31. Anche i rappresentanti devono essere informati sui principi fondamentali del funzionamento della cartella informatizzata del paziente nonché sulle possibilità, i diritti e i doveri connessi all'utilizzo della cartella informatizzata (n. 8.4.2 lett. b allegato 2 OCIP-DFI). Per tutelare i diritti della personalità della persona rappresentata è necessario garantire che il rappresentante sia identificato correttamente e che il suo diritto a svolgere tale ruolo si fondi sulle prescrizioni del diritto civile. Analogamente ai pazienti, anche i loro rappresentanti devono essere identificati in modo sicuro. Se non può avvenire con uno strumento d'identificazione di un emittente certificato secondo l'articolo 31, anche in questo caso l'identificazione deve rispettare i requisiti di cui all'articolo 24 (n. 8.4.2 lettera a allegato 2 OCIP-DFI). Inoltre, è necessario garantire che l'accesso del rappresentante sussista solo per la durata della rappresentanza (n. 8.4.2 lett. d allegato 2 OCIP-DFI). Possibili casi di applicazione sono la rappresentanza di un bambino o di una persona anziana da parte di familiari o di altre persone di fiducia, se la persona interessata non è in possesso delle condizioni tecniche e mentali per gestire in autonomia la propria cartella informatizzata.

Art. 18 Portale d'accesso per i pazienti

Il portale d'accesso per i pazienti deve soddisfare i requisiti di cui ai n. 9.1–9.5 dell'allegato 2 OCIP-DFI. Oltre alle prescrizioni valide anche per il portale d'accesso per i professionisti della salute secondo l'articolo 11, va rispettata in particolare la prescrizione di cui alla lettera a, concernente l'attuazione delle diverse possibilità di attribuzione dei gradi di riservatezza e dei diritti d'accesso secondo l'articolo 1 capoverso 1 e l'articolo 2 capoverso 1 nonché delle opzioni dei pazienti secondo l'articolo 4 lettere a-e e lettera g. Vi rientra anche la rappresentazione della composizione dei gruppi di professionisti della salute (n. 9.1 lett. c allegato 2 OCIP-DFI).

La rappresentazione dei dati della cartella informatizzata del paziente sull'interfaccia utente del portale d'accesso interno per i pazienti deve essere corretta e completa e deve ad esempio evidenziare in modo chiaro se i dati medici sono stati forniti da un professionista della salute o dal paziente stesso (n. 9.2 allegato 2 OCIP-DFI).

Ulteriori prescrizioni riguardano una rappresentazione chiara per il paziente dei verbali generati dal trattamento dei suoi dati di tutte le comunità e comunità di riferimento secondo la *lettera b* (n. 9.3 allegato 2 OCIP-DFI). Attraverso il portale d'accesso per i pazienti, questi ultimi devono avere la possibilità di visionare in ogni momento i verbali (art. 10 cpv. 3 lettera d) generati da ogni trattamento della cartella informatizzata del paziente (n. 9.3 e n. 2.10 allegato 2 OCIP-DFI). Dal momento che i verbali secondo il n. 2.10 dell'allegato 2 OCIP-DFI sono generati anche a livello decentrato in altre comunità, questi devono essere richiamati dalle rispettive comunità con una procedura di richiamo ed essere messi a disposizione dei pazienti per la consultazione sul portale d'accesso in forma consolidata e leggibile. La rappresentazione dei verbali per la consultazione si rifà agli adeguamenti nazionali dei profili d'integrazione secondo l'articolo 5 lettera b OCIP-DFI.

Secondo la *lettera c*, il portale d'accesso per i pazienti deve in particolare dare la possibilità a questi ultimi di escludere determinati dati medici dalla distruzione secondo l'articolo 10 capoverso 2 lettera b o di distruggerne altri presenti nella cartella informatizzata secondo l'articolo 10 capoverso 2 lettera c (n. 9.4.1 allegato 2 OCIP-DFI). Per quanto concerne i dati registrati dal paziente stesso, il n. 9.4.3 allegato 2 OCIP-DFI dispone concretamente che le funzioni chiave della cartella informatizzata del paziente sul portale d'accesso devono essere chiaramente separate da eventuali altre funzionalità che non sono oggetto delle norme della LCIP e delle sue disposizioni esecutive. In particolare, bisogna garantire che i dati della cartella informatizzata del paziente non siano trasferiti in ambiti funzionali o supporti di memoria «al di fuori» di essa e quindi del campo d'applicazione della LCIP in modo automatico e senza esplicito consenso del paziente.

Per incentivare l'accesso senza barriere per i pazienti con disabilità o limitazioni dovute all'età o alla lingua, i portali d'accesso secondo la lettera d devono soddisfare gli stessi requisiti dei portali d'accesso per i professionisti della salute di cui all'articolo 11 (n. 3.2 allegato 2 OCIP-DFI).

Art. 19 Dati registrati dai pazienti

Il paziente ha la possibilità di registrare personalmente i propri dati medici nella cartella informatizzata del paziente attraverso il portale d'accesso della propria comunità di riferimento (art. 10 cpv. 2 lett. b n. 3 LCIP), senza alcuna scadenza per la cancellazione (n. 10.1.2 allegato 2 OCIP-DFI).

Per motivi inerenti tra l'altro alla sicurezza dei dati, i dati registrati dal paziente stesso non dovrebbero essere memorizzati in archivi di documenti di una struttura sanitaria affiliata. Per questa ragione, ai sensi del n. 10.1.1 allegato 2 OCIP-DFI, le comunità di riferimento devono mettere a disposizione archivi di documenti interni dedicati ai dati registrati dai pazienti stessi. Lo spazio a disposizione per la memorizzazione di dati forniti dal paziente deve essere sufficiente.

Il n. 10.2 dell'allegato 2 OCIP-DFI prevede inoltre la possibilità che i pazienti possano esportare dal sistema i dati medici della propria cartella informatizzata, inclusi i metadati descrittivi. I dati esportati possono essere ad esempio conservati fisicamente, vale a dire «offline», e se necessario devono essere rimessi a disposizione nella cartella informatizzata senza oneri sproporzionati. Questo procedimento corrisponde alla strategia in uso per l'archiviazione di documenti non più immediatamente rilevanti per la situazione terapeutica del momento ed è in questo senso anche una misura volta a incrementare la protezione e la sicurezza dei dati. Affinché la reimportazione non generi duplicati, la funzione di esportazione va collegata all'eliminazione dei dati esportati oppure, al momento della reimportazione, deve essere applicata una procedura idonea a riconoscere i duplicati. Per evitare una perdita d'integrità (p. es. attraverso la manipolazione dei dati «offline»), una procedura adeguata (che prevede p. es. l'impiego di funzioni crittografiche di hash, come SHA-3) al momento dell'esportazione deve consentire di eseguire una verifica dell'integrità al momento di mettere nuovamente a disposizione i dati. La procedura applicata all'esportazione dovrà poi verificare al momento di una nuova messa a disposizione dei dati, se la loro integrità è stata mantenuta (n. 10.2.3 allegato 2 OCIP-DFI).

Art. 20 Servizio di assistenza per i pazienti

Oltre al contatto messo a disposizione dei professionisti della salute secondo l'articolo 13, le comunità di riferimento devono assicurare anche a tutti i pazienti un contatto per il supporto tecnico e funzionale nell'utilizzo della cartella informatizzata del paziente («service desk»). Questa possibilità di contatto è volta soprattutto a garantire che i pazienti ricevano sostegno e supporto nell'utilizzo della cartella informatizzata del paziente. Le prescrizioni applicabili al personale e alla verbalizzazione coincidono con quelle in vigore per il Servizio di assistenza per i professionisti della salute (n. 5 allegato 2 OCIP-DFI). In caso di conflitti o ricorsi, è possibile rivolgersi agli organi federali o cantonali già esistenti (p. es. incaricato federale o cantonale della protezione dei dati) in qualità di istanze di ricorso o servizi di mediazione.

Art. 21 Soppressione della cartella informatizzata

Il *capoverso 1* prevede che la comunità di riferimento sopprima la cartella informatizzata se il paziente revoca il suo consenso. A tale scopo è necessario assicurarsi che il paziente che revoca il consenso sia stato identificato in modo sicuro (n. 12.2.2 lett. a allegato 2 OCIP-DFI). Per ragioni di tracciabilità, la comunità di riferimento deve conservare la dichiarazione di revoca per dieci anni.

In caso di decesso del paziente, la comunità di riferimento può sopprimere la cartella informatizzata al più presto due anni dopo il decesso del paziente (*cpv. 2*). Questa disposizione serve ad attuare il principio di proporzionalità. Le cartelle informatizzate di persone decedute non devono infatti essere conservate a tempo indeterminato. Una volta venuta a conoscenza del decesso del paziente, la comunità di riferimento deve poter sopprimere la cartella dopo un termine di protezione di due anni. La

comunità di riferimento non è tuttavia obbligata ad eseguire attivamente ricerche in merito all'esistenza in vita, alla data del decesso o ad altri aspetti. Allo stesso modo, non sussiste nemmeno un obbligo di comunicazione dei decessi alle comunità di riferimento e alle comunità da parte dell'UCC o dei registri degli abitanti cantonali e comunali. Tuttavia, i Cantoni sono liberi di sancire nel diritto cantonale un obbligo di comunicazione in tal senso – creando la base legale necessaria – anche avvalendosi del NAVS13.

Secondo il *capoverso 3*, quando una cartella informatizzata viene soppressa, la comunità di riferimento deve revocare entro un termine adeguato tutti i diritti d'accesso a tale cartella nonché informare l'UCC e tutte le comunità e comunità di riferimento in merito alla soppressione della cartella. Le modalità e i canali d'informazione sono lasciati alla discrezione della comunità di riferimento, che deve comunque garantire che l'informazione raggiunga il destinatario e che in tale contesto non siano diffuse anche informazioni mediche. Tutti i dati devono essere eliminati secondo l'articolo 10 capoverso 1 lettera e nella comunità di riferimento e in tutte le altre comunità (n. 12.4 lett. c e n. 2.6 lett. b allegato 2 OCIP-DFI).

Sezione 3: Valutazione e ricerca

Art. 22

L'obiettivo della valutazione è la sorveglianza dell'idoneità, dell'efficacia e dell'economicità delle misure della LCIP (art. 18 LCIP). La valutazione della LCIP avviene tra l'altro sulla base di un sistema di monitoraggio, che garantisce la disponibilità dei dati necessari alla valutazione. Al fine di garantire la disponibilità dei dati, il *capoverso 1* stabilisce che le comunità e le comunità di riferimento debbano mettere a disposizione dell'UFSP, in forma pseudonimizzata, i dati necessari alla valutazione. Il *capoverso 2* specifica inoltre che il DFI stabilisce la periodicità dei dati da fornire e i relativi termini.

Altre fonti importanti che forniscono dati per la valutazione sono tra l'altro i servizi di ricerca di dati secondo l'articolo 39, e in particolare il servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute (*cpv. 3*) nonché la documentazione prodotta nell'ambito di una certificazione secondo la LCIP dagli organismi certificati o dagli organismi di certificazione (*cpv. 4*).

Capitolo 4: Strumenti d'identificazione

Secondo l'articolo 7 LCIP, per accedere alla cartella informatizzata i pazienti e i professionisti della salute devono disporre di uno strumento d'identificazione rilasciato da un emittente certificato secondo l'articolo 31.

La certificazione dell'emittente degli strumenti d'identificazione nonché i requisiti tecnici minimi definiti per il livello di sicurezza assicurano l'affidabilità dello strumento d'identificazione per quanto concerne l'identità dei pazienti e dei professionisti della salute e garantiscono che la persona che rivendica una determinata identità sia effettivamente la persona alla quale tale identità è stata attribuita.

L'emissione e la gestione di uno strumento d'identificazione per l'intero ciclo vitale si rifanno al procedimento descritto nella norma ISO/IEC 29115:2013, suddiviso nelle fasi di registrazione, gestione e impiego dello strumento d'identificazione nell'esercizio operativo. Ai fini dell'affidabilità dell'autenticazione assume un'importanza centrale la gestione del ciclo vitale dello strumento d'identificazione. Questo ciclo vitale comprende processi parziali come la produzione del supporto dell'identità elettronica, la personalizzazione, l'inizializzazione e il collegamento dell'identità elettronica al titolare come pure l'emissione, l'attivazione, la revoca e il rinnovo.

Questi processi parziali possono svolgersi con sequenze diverse, a condizione che la sicurezza sia garantita in modo documentabile. Ad esempio la fase della registrazione dei dati relativi all'identità con successivo collegamento dell'identità elettronica può avvenire dopo l'emissione dello strumento d'identificazione. Il procedimento potrebbe ad esempio svolgersi come segue: un paziente o un professionista della salute riceve da un emittente certificato uno strumento d'identificazione, che dispone di un identificatore elettronico univoco e di un meccanismo di autenticazione sicuro per accedervi. Nella fase successiva la persona attiva lo strumento d'identificazione, provando che dispone dei fattori di autenticazione necessari (p. es. password segreta). Infine, un procedimento affidabile collega ulteriori caratteristiche identificative della persona con lo strumento d'identificazione. Questo collegamento può essere garantito con la presenza fisica della persona o con l'ausilio di un'identificazione video. I supporti per l'identità elettronica già emessi – come ad esempio la tessera d'assicurato secondo l'articolo 42*a* della legge federale del 18 marzo 1994[10] sull'assicurazione malattie – non devono essere emessi nuovamente per adempiere alle prescrizioni di cui agli articoli 23 – 27.

Art. 23 Requisiti

I requisiti per la registrazione e la gestione degli strumenti d'identificazione nonché i requisiti di protezione per l'autenticazione sono contenuti nella norma ISO/IEC 29115:2013 con riferimento ai diversi gradi di riservatezza. Maggiore è il grado, maggiore è l'affidabilità dell'identità della persona che si autentica con lo strumento d'identificazione ottenuto presso la parte facente affidamento su tale strumento.

Secondo la *lettera a*, il grado di riservatezza 3 («riservatezza elevata») vale in egual misura per gli strumenti d'identificazione dei pazienti e per quelli dei professionisti della salute. Se uno strumento d'identificazione elettronico soddisfa i requisiti di un grado più elevato, si parte dal presupposto che esso soddisfi anche quelli di un grado di riservatezza inferiore.

Il grado di riservatezza 3 non richiede la presenza della persona al momento della registrazione dello strumento d'identificazione. Tuttavia è necessario garantire che il documento d'identità necessario per la registrazione sia valido e si riferisca alla persona reale, vale a dire al richiedente. Al momento della registrazione devono pertanto essere adottati provvedimenti volti a ridurre il rischio che l'identità del richiedente non corrisponda all'identità rivendicata con riferimento ad esempio a documenti smarriti, rubati, sospesi, revocati o scaduti (art. 24 cpv. 1).

Secondo la *lettera b*, lo strumento d'identificazione deve essere concepito dal punto di vista tecnico e organizzativo in modo che possa essere utilizzato con un elevato grado di affidabilità unicamente dalla persona autorizzata. A titolo di esempio, non deve essere possibile trasferire le chiavi digitali protette dello strumento d'identificazione a un altro sistema o supporto, ad esempio intercettando password trasmesse in chiaro.

La procedura di autenticazione prescritta alla *lettera c* deve comprendere l'impiego di una combinazione di almeno due tecniche di autenticazione ed essere conforme all'attuale stato della tecnica. Particolarmente diffuse sono le procedure che combinano i fattori «informazione» (p. es. password segreta) e «possesso» (p. es. possesso di una smart card o di una SIM card come supporto sicuro per le chiavi digitali).

Secondo la *lettera d* lo strumento d'identificazione può avere una durata di validità massima di cinque anni.

Art. 24 Verifica dell'identità

L'emittente dello strumento d'identificazione verifica l'identità del richiedente mediante un documento d'identità valido ai sensi della legge sui documenti d'identità (RS 143.1) o della legge sugli stranieri (RS

[10] RS **832.10**

142.20). Per richiedere lo strumento d'identificazione per corrispondenza, la persona che ne fa richiesta deve esibire all'emittente una copia autenticata del documento d'identità (p. es. l'«Identificazione Gialla» de La Posta o un'identificazione video). Una conferma dell'identità e degli attributi identificativi mediante firma elettronica qualificata ai sensi della legge sulla firma elettronica (RS 943.03) equivale all'esibizione della copia autenticata del documento.

L'emittente può delegare a terzi la verifica dell'identità del richiedente, al fine di disporre di un'ampia rete di organismi di registrazione in tutta la Svizzera (cpv. 2). I requisiti richiesti all'organismo di registrazione (*registration authority*) sono definiti al n. 4.2 allegato 8 OCIP-DFI (obiettivi di sicurezza per il contesto).

Art. 25 Dati

Secondo il *capoverso 1*, l'emittente dello strumento d'identificazione assegna al richiedente un identificatore univoco (eID). Questo identificatore deve essere utilizzato per collegare l'identità della persona nella comunità o comunità di riferimento con quella dell'emittente.

L'emittente registra inoltre gli attributi identificativi dei pazienti (cpv. 2) e dei professionisti della salute (cpv. 3) al fine di provare e verificare la loro identità. L'identificatore di cui al *capoverso 1* nonché gli attributi secondo il *capoverso 2 lettere a–d* e il *capoverso 3* possono essere trasmessi ai portali d'accesso interni delle comunità e delle comunità di riferimento nella risposta di autenticazione ai fini della verifica e dell'attribuzione dell'identità.

Lo strumento d'identificazione può essere utilizzato anche come prova della qualifica personale dei professionisti della salute (art. 9 cpv. 2 lett. b e d). A questo scopo l'emittente registra e conferma il GLN del professionista della salute (art. 25 cpv. 3 lett. a). Secondo il *capoverso 3 lettera b*, è necessario innanzitutto provare che la persona richiedente è un professionista della salute secondo l'articolo 2 lettera b LCIP. A tale scopo l'emittente confronta scrupolosamente i dati personali con un registro federale o cantonale (MedReg, NAREG ecc.), in modo da garantire che il titolare dello strumento d'identificazione disponga della formazione riconosciuta a livello federale o cantonale e – in caso di attività indipendente – di un'autorizzazione cantonale all'esercizio della professione. Secondo il *capoverso 3*, l'emittente può delegare la conferma dell'attributo «professionista della salute» a terzi («registration authority» – organismo di registrazione). Il controllo della verifica dell'identità da parte dell'emittente o dell'organismo di registrazione è disciplinato al n. 4.2 dell'allegato 8 OCIP-DFI.

Secondo il *capoverso 5*, l'emittente è tenuto a informare il richiedente sulle misure di sicurezza da adottare nell'impiego degli strumenti d'identificazione. Ciò comprende l'utilizzo sicuro delle password e le informazioni inerenti al trattamento e alla trasmissione a terzi degli attributi identificativi.

Art. 26 Rinnovo

Una volta superata la durata di validità massima di cinque anni (art. 23 lett. d), lo strumento d'identificazione deve essere richiesto nuovamente. Il *capoverso 2* afferma che, in deroga alla norma ISO/IEC 29115:2013, per il rinnovo dello strumento d'identificazione deve essere effettuata una verifica dell'identità secondo il grado di riservatezza 3 (art. 23).

Art. 27 Blocco

Il titolare dello strumento d'identificazione deve avere in ogni tempo la possibilità di disporre il blocco temporaneo o definitivo dello strumento d'identificazione per l'accesso alla cartella informatizzata del paziente. Dal momento che lo strumento d'identificazione può essere utilizzato in linea di principio per l'autenticazione al di fuori della cartella informatizzata del paziente, l'emittente deve prevedere procedure tecniche al fine di evitare un'autenticazione valida nel portale d'accesso per i pazienti e in quello per i professionisti della salute. Inoltre, l'emittente deve prendere provvedimenti per evitare un blocco non autorizzato.

Capitolo 5: Accreditamento

Art. 28 Requisiti

Gli organismi che certificano le comunità, le comunità di riferimento, i portali d'accesso e gli emittenti di strumenti d'identificazione devono essere riconosciuti dal SAS per l'audit e la certificazione di sistemi di gestione. L'accreditamento è retto dall'ordinanza del 17 giugno 1996 sull'accreditamento e sulla designazione[11] (OAccD). L'articolo 7 capoverso 1 di tale ordinanza prevede che l'organismo di certificazione debba rispondere a criteri determinanti a livello internazionale. Per gli organismi di certificazione che svolgono verifiche nell'ambito della cartella informatizzata del paziente i requisiti sono definiti dalla norma ISO/IEC 17021:2015, che stabilisce i requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione (cfr. allegato 2 OAccD).

Comunità, comunità di riferimento ed emittenti di strumenti d'identificazione devono assolvere compiti diversi, che sono verificati nell'ambito della certificazione. Per tale ragione l'accreditamento degli organismi di certificazione deve rispettare requisiti differenti ed è distinto per ciascun organismo (*cpv. 2*).

Il *capoverso 3* concretizza il concetto di procedura di controllo. Questa comprende i criteri per verificare il rispetto delle condizioni di certificazione (*lett. a*) le modalità di svolgimento della procedura di certificazione (inclusi il rinnovo della certificazione e la verifica; *lett. b*).

Il *capoverso 4* prescrive che, per la verifica del trasferimento di dati tra le comunità e le comunità di riferimento (interoperabilità), gli organismi di certificazione debbano utilizzare il sistema di test di certificazione messo a disposizione dall'UFSP. Con l'ausilio di questo sistema di test di certificazione è possibile verificare se la comunità o comunità di riferimento da certificare è in grado, nella pratica, di comunicare correttamente con altre comunità e comunità di riferimento.

Secondo il *capoverso 5* il DFI stabilisce i requisiti minimi concernenti la qualifica del personale addetto alle certificazioni (cfr. allegato 7 OCIP-DFI). Va comunque tenuto presente che nell'ambito dell'informatica medica e della protezione dei dati non esistono formazioni standard e che gli esperti sono relativamente rari. L'esperienza pratica assume pertanto particolare importanza.

Art. 29 Procedura

Il coinvolgimento dell'UFSP ha lo scopo di garantire da una parte che l'organismo di accreditamento possa utilizzare le conoscenze specialistiche dell'Amministrazione federale e dall'altra che l'UFSP abbia la possibilità di discutere con il SAS i dettagli dell'accreditamento.

Capitolo 6: Certificazione

Sezione 1: Condizioni

Art. 30 Comunità e comunità di riferimento

Un organo di certificazione accreditato secondo l'articolo 28 stabilisce se una comunità o comunità di riferimento soddisfa le condizioni di certificazione. Oltre alle condizioni di certificazione valide per le comunità (art. 9–13), le comunità di riferimento devono soddisfare anche le prescrizioni di cui agli articoli 14–21 (cpv. 1).

Il *capoverso 2* delega al DFI la competenza legislativa per la definizione dei dettagli inerenti alle condizioni di certificazione, consentendo un disciplinamento che tiene conto del pertinente livello legislativo.

[11] RS **946.512**

Il *capoverso 3* consente al DFI di attribuire all'UFSP la competenza di adeguare le condizioni di certificazione allo stato della tecnica (cfr. commenti all'art. 10 cpv. 5). Ciò è importante soprattutto per le condizioni di certificazione nell'ambito della conservazione e trasmissione di dati (art. 10) e nell'ambito della protezione e sicurezza dei dati (art. 12).

Art. 31 Emittenti di strumenti d'identificazione

Il *capoverso 1* contiene un elenco esaustivo delle condizioni di certificazione per gli emittenti di strumenti d'identificazione.

La *lettera a* contiene un rimando agli articoli 23–27, che devono essere rispettati dagli emittenti di strumenti d'identificazione. Questi devono in particolare garantire che gli strumenti d'identificazione corrispondano al grado di riservatezza 3 della norma ISO/IEC 29115:2013 (art. 23), che l'identità della persona sia verificata (art. 24) e che gli attributi identificativi del titolare dello strumento d'identificazione siano attribuiti correttamente (art. 25).

L'emittente deve garantire con una procedura adeguata che tutti i collaboratori e i subcontraenti dispongano delle conoscenze specialistiche, dell'esperienza e delle qualifiche necessarie a svolgere i compiti loro affidati (*lett. b*).

Secondo la *lettera c*, i sistemi e prodotti informatici utilizzati devono essere affidabili. Il concetto di affidabilità esprime la scrupolosità con la quale sono stati sviluppati questi prodotti e la misura in cui un utente di essi può fidarsi della funzionalità di sicurezza offerta.

Secondo la *lettera d*, al momento dell'emissione dello strumento d'identificazione, l'emittente deve assicurarsi che oltre ai controlli tecnici vengano adottate anche misure organizzative a garanzia della protezione e della sicurezza dei dati. Vi rientrano tra l'altro la sorveglianza costante dei dispositivi necessari all'emissione dello strumento d'identificazione nonché la protezione da un accesso non autorizzato, ad esempio permettendo l'accesso alle aree in cui sono trattati dati personali o crittografici nonché altre informazioni sensibili solo ai collaboratori autorizzati. L'emittente di strumenti d'identificazione deve affidarsi a metodi di provata efficacia per garantire la protezione e la sicurezza dei dati.

Le condizioni tecniche e organizzative di certificazione applicabili agli strumenti d'identificazione e ai loro emittenti sono concretizzate all'allegato 8 OCIP-DFI sotto forma di profilo di protezione (cpv. 2). Tale profilo serve a formulare le esigenze di sicurezza applicabili a una classe di prodotti (anche nei settori di software e hardware) e in particolare alla classe di tutti gli strumenti d'identificazione autorizzati per la cartella informatizzata del paziente secondo questa ordinanza.

L'oggetto da valutare (target of evaluation, TOE) del profilo di protezione comprende lo strumento d'identificazione stesso, il provider dell'identità (identity provider) per l'identificazione e l'autenticazione nonché le interfacce tecniche necessarie e i canali di comunicazione sicuri per l'autenticazione nei portali d'accesso delle comunità o comunità di riferimento. Nell'ambito della procedura di certificazione, le prove dei requisiti di sicurezza sono rilevate e verificate dall'organismo di certificazione con un livello di valutazione definito (evaluation assurance level, EAL). La verifica comprende gli ambiti «development», «life-cycle support», «security target evaluation» o «vulnerability assessment». Il livello di valutazione definito al n. 5.4 dell'allegato 8 OCIP-DFI (EAL 2) indica che il TOE deve essere valutato a livello funzionale e strutturale.

Il *capoverso 2* delega al DFI la competenza legislativa per la definizione dei dettagli inerenti alle condizioni di certificazione, consentendo un disciplinamento che tiene conto del pertinente livello legislativo.

Il *capoverso 3* consente al DFI di attribuire all'UFSP la competenza di adeguare le condizioni di certificazione allo stato della tecnica (cfr. commenti all'art. 10 cpv. 5). Si pensi ad esempio

all'adeguamento di prescrizioni altamente tecniche delle condizioni di certificazione per gli emittenti di strumenti d'identificazione.

Sezione 2: Procedura di certificazione

Art. 32 Svolgimento

Lo svolgimento della procedura di certificazione disciplinato in questo articolo riprende la norma ISO/IEC 17021:2015 e definisce le fasi della procedura di certificazione in ordine cronologico.

L'esame dei documenti secondo il *capoverso 1* consente all'organismo di certificazione di valutare, sulla base dei documenti presentati, se la comunità, la comunità di riferimento o l'emittente degli strumenti d'identificazione sono sufficientemente preparati all'audit di certificazione. Ciò consente di evitare costi inutili e incrementa le possibilità di svolgere un audit di certificazione efficace.

Nel quadro dell'audit di certificazione secondo il *capoverso 2*, l'organismo di certificazione verifica anche in loco il rispetto delle condizioni di certificazione da parte della comunità, della comunità di riferimento o dell'emittente di strumenti d'identificazione.

Se, dopo avere esaminato la documentazione e aver effettuato l'audit di certificazione, giunge alla conclusione che la comunità, la comunità di riferimento o l'emittente di strumenti d'identificazione soddisfa i rispettivi requisiti, l'organismo di certificazione rilascia il certificato secondo il *capoverso 3*.

Il *capoverso 4* stabilisce che, prima della scadenza del certificato dev'essere svolto un rinnovo della certificazione. I requisiti necessari per il rinnovo della certificazione corrispondono a quelli di un audit di certificazione secondo il capoverso 2. Questa procedura mira a garantire una continuità dell'attività della comunità o della comunità di riferimento, come pure dell'emittente degli strumenti d'identificazione, evitando che il certificato scada e che di conseguenza l'organizzazione in questione debba essere esclusa dalla partecipazione alla cartella informatizzata del paziente.

Art. 33 Comunicazione e pubblicazione dei certificati

Per garantire lo scambio di dati intercomunitario, secondo il *capoverso 1* le comunità e comunità di riferimento certificate devono essere iscritte nel servizio di ricerca di dati delle comunità e comunità di riferimento secondo l'articolo 40. Ogni certificazione ottenuta deve pertanto essere comunicata all'UFSP, affinché questo possa effettuare la registrazione corrispondente (art. 40 cpv. 2). Devono essere inoltre comunicate all'UFSP tutte le sospensioni o revoche di una certificazione, affinché la comunità o la comunità di riferimento interessata possa essere bloccata nel servizio di ricerca di dati delle comunità e comunità di riferimento ed esclusa quindi dalla partecipazione alla cartella informatizzata del paziente.

Oltre a registrare i dati nel servizio di ricerca di dati delle comunità e comunità di riferimento, l'UFSP pubblica anche un registro dei certificati rilasciati (*cpv. 2*). Questo registro consente ai pazienti una visione d'insieme degli enti che offrono la cartella informatizzata del paziente secondo la LCIP e degli emittenti di strumenti d'identificazione certificati.

Art. 34 Verifica

Il *capoverso 1* prevede che l'organismo di certificazione verifichi ogni anno se le condizioni di certificazione sono ancora soddisfatte integralmente. Se dovesse accertare il contrario, l'organismo di certificazione informa l'UFSP, che può disporre un rinnovo straordinario della certificazione conformemente all'articolo 37 capoverso 1 lettera c. Nel caso in cui l'inosservanza delle condizioni di certificazione riguardi un settore isolato, è possibile che la verifica sia limitata a tale settore. L'organismo di certificazione ha inoltre la possibilità di comminare sanzioni se sono soddisfatti i requisiti di cui all'articolo 38 capoverso 1.

Se riscontra mutamenti sostanziali rispetto alle condizioni di certificazione, l'organismo di certificazione ne informa l'UFSP, affinché questo possa identificare per tempo eventuali punti deboli delle disposizioni esecutive e avviare se del caso le misure necessarie.

Art. 35 Durata di validità

Una volta rilasciato, il certificato ha una durata di tre anni. Sono fatte salve le disposizioni di cui agli articoli 36 e 37 capoverso 1 lettera c. Per poter continuare a scambiare dati nell'ambito della cartella informatizzata del paziente in qualità di comunità o di comunità di riferimento o a svolgere l'attività di emittente di strumenti d'identificazione per comunità e comunità di riferimento senza soluzione di continuità, il rinnovo della certificazione deve essere concluso prima della scadenza della durata di validità del certificato. Il rinnovo è retto dall'articolo 32.

Art. 36 Comunicazione di sostanziali adeguamenti tecnici od organizzativi

Gli adeguamenti sostanziali devono essere comunicati all'organismo di certificazione conformemente al *capoverso 1*. Sono adeguamenti tecnici od organizzativi sostanziali in particolare i processi nuovi o modificati (rilevanti per la certificazione) o gli adeguamenti della struttura informatica per lo scambio di dati intercomunitario presso le comunità o le comunità di riferimento, nonché i mutamenti della procedura di autenticazione presso gli emittenti di strumenti d'identificazione.

Secondo il *capoverso 2*, l'organismo di certificazione decide se tale adeguamento debba essere esaminato nell'ambito di una verifica secondo l'articolo 34, di un rinnovo della certificazione o di un rinnovo straordinario della certificazione secondo l'*articolo 37 capoverso 1 lettera c*. La verifica e il rinnovo della certificazione avvengono secondo la periodicità consueta, mentre il rinnovo straordinario della certificazione deve essere effettuato prima possibile. Se la situazione dovesse richiederlo, la comunità o la comunità di riferimento possono essere escluse dalla cartella informatizzata del paziente finché il rinnovo straordinario della certificazione non sia stato superato. Una tale esclusione può essere disposta dall'organismo di certificazione sulla base dell'articolo 38 (Sanzioni) o dall'UFSP – se questo è informato dall'organismo di certificazione in merito a mutamenti sostanziali rispetto alle condizioni di certificazione secondo l'articolo 34 – sulla base dell'articolo 37 (Clausola di salvaguardia).

Art. 37 Clausola di salvaguardia

L'applicazione della clausola di salvaguardia avviene indipendentemente da un eventuale comportamento scorretto di una comunità, di una comunità di riferimento o di un emittente di strumenti d'identificazione. Si pensi ad esempio ai casi in cui, sulla base di rischi gravi in ambito TIC (determinati p. es. da virus, trojan ecc.), sia necessaria un'interruzione immediata della comunicazione intercomunitaria o l'utilizzo di determinati strumenti d'identificazione possa rappresentare un pericolo per la cartella informatizzata del paziente. Nei casi in cui una comunità, una comunità di riferimento o un emittente di strumenti d'identificazione contravvengano alle condizioni di certificazione, si applica l'articolo 38.

La *lettera a* consente all'UFSP di negare provvisoriamente la possibilità di trattare i dati della cartella informatizzata alle comunità e alle comunità di riferimento che rappresentano un rischio per la protezione e la sicurezza dei dati, bloccandone la registrazione nel servizio di ricerca di dati delle comunità e comunità di riferimento. Una volta che la comunità o la comunità di riferimento ha eliminato in modo documentabile il fattore o i fattori di rischio, la registrazione nel servizio di ricerca di dati delle comunità e comunità di riferimento può essere riattivata.

La *lettera b* consente all'UFSP di vietare l'uso di determinati strumenti d'identificazione elettronica che rappresentano un problema per la sicurezza a livello collettivo. In altre parole, non si tratta di bloccare uno strumento d'identificazione di un singolo paziente o di un singolo professionista della salute, bensì di vietare una tecnologia che non soddisfa (temporaneamente) gli standard di sicurezza.Un rinnovo straordinario della certificazione secondo la *lettera c* può essere disposto dall'UFSP se vi è una

comunicazione da parte di comunità o comunità di riferimento in merito a un incidente sopravvenuto nel sistema di gestione della protezione e della sicurezza dei dati ritenuto rilevante per la sicurezza secondo l'articolo 12 capoverso 3, indicante che le condizioni di certificazione non sono più soddisfatte.

Può essere disposto anche se l'organismo di certificazione rileva nell'ambito di una verifica secondo l'articolo 34 che una comunità, una comunità di riferimento o un emittente di strumenti d'identificazione non soddisfa più le condizioni di certificazione o se vi è un sospetto fondato che tali condizioni non siano più soddisfatte. A seconda dell'entità degli elementi da verificare è possibile che la comunità o la comunità di riferimento non possa più partecipare allo scambio di dati nell'ambito della cartella informatizzata del paziente finché non ha superato il rinnovo straordinario della certificazione.Gli emittenti di strumenti d'identificazione potrebbero invece trovarsi a non poter effettuare procedure d'identificazione e di autenticazione di professionisti della salute o di pazienti finché non hanno superato il rinnovo straordinario della certificazione.

Secondo il *capoverso 2* l'UFSP ha la possibilità di esigere dall'organismo di certificazione e dall'organismo certificato i documenti necessari per la certificazione o il rinnovo della certificazione. Talvolta l'UFSP può riconoscere un rischio grave per la cartella informatizzata del paziente e avviare di conseguenza le misure del caso solo sulla base di questi documenti.

Sezione 3: Sanzioni

Art. 38

Se nell'ambito di una verifica regolare della certificazione (art. 34) sono constatate gravi lacune, secondo il *capoverso 1* l'organismo di certificazione può sospendere o revocare la validità di un certificato. Una lacuna grave sussiste in particolare se non sono più soddisfatte condizioni essenziali della certificazione (*lett. a*). Ad esempio, se presso una comunità o una comunità di riferimento si riscontra ripetutamente che l'integrazione degli strumenti d'identificazione non funziona correttamente, il funzionamento del sistema di gestione degli accessi o dell'amministrazione dei diritti è difettoso, la comunicazione intercomunitaria non è garantita o il portale d'accesso non consente l'accesso a una persona autorizzata o lo consente a una persona non autorizzata. Di conseguenza, la registrazione nel servizio di ricerca di dati delle comunità e comunità di riferimento (art. 40 cpv. 2) viene bloccata. La *lettera b* riguarda i casi in cui un certificato è utilizzato in modo ingannevole o abusivo. Ciò potrebbe verificarsi ad esempio se il paziente viene ingannato in merito al significato del certificato, ad esempio se una comunità di riferimento afferma di essere certificata anche per l'emissione di strumenti d'identificazione.

Il *capoverso 2* stabilisce espressamente che in caso di controversia, il giudizio e la procedura sono retti dalle disposizioni di diritto contrattuale in materia.

Secondo il *capoverso 3,* l'UFSP può disporre una verifica da parte dell'organismo di certificazione. L'UFSP dispone così della base legale per procedere nei confronti di comunità, comunità di riferimento o emittenti di strumenti d'identificazione già certificati in presenza di un sospetto fondato – nell'interesse della sicurezza del sistema della cartella informatizzata del paziente.

Capitolo 7: Servizi di ricerca di dati

Sezione 1: Aspetti generali

Secondo l'articolo 14 LCIP, l'UFSP gestisce i servizi di ricerca di dati che forniscono in modo uniforme a livello nazionale i dati di riferimento necessari alla comunicazione tra comunità, comunità di riferimento e portali d'accesso. Oggetto delle disposizioni di questo capitolo dell'OCIP sono i requisiti relativi al contenuto e all'uso dei servizi di ricerca di dati nonché le condizioni per la loro gestione.

Art. 39

I dati dei servizi di ricerca di dati secondo le *lettere a–d* sono necessari per una comunicazione a norma di legge tra comunità e comunità di riferimento.

Il servizio di ricerca di dati delle comunità e comunità di riferimento secondo la *lettera a* contiene in particolare i dati tecnici necessari alla comunicazione elettronica con i rispettivi punti d'accesso. Per garantire l'integrità dei messaggi elettronici dei punti d'accesso, il servizio contiene anche la chiave pubblica con la quale le comunità e comunità di riferimento possono verificare l'autenticità dei messaggi trasmessi da altri punti d'accesso (art. 40 cpv. 1 lett. c).

I dati sulle strutture sanitarie e sui professionisti della salute autorizzati a trattare i dati della cartella informatizzata del paziente sono riportati nel servizio di ricerca dati di cui alle *lettere a e b*. Questo comprende anche l'appartenenza di professionisti della salute a gruppi di professionisti della salute. Sulla base di questa informazione il paziente può accordare i diritti d'accesso ai professionisti della salute e ai gruppi di professionisti della salute secondo l'*articolo 2 capoverso 1*.

Il servizio di ricerca dei metadati di cui alla *lettera c* contiene i metadati da utilizzare secondo l'articolo 10 capoverso 3 lettera a per la descrizione strutturata dei dati registrati nella cartella informatizzata del paziente. I valori e gli intervalli di valori dei metadati sono stabiliti nell'allegato 3 OCIP-DFI.

Il servizio di ricerca di dati di cui alla *lettera d* contiene gli OID necessari per le comunità e comunità di riferimento.

L'UFSP è responsabile per la gestione dei servizi di ricerca di dati secondo l'articolo 14 capoverso 1 LCIP in modo tale che vi rientrino anche la costituzione, la gestione e lo sviluppo di questi servizi.

Nell'ambito della costituzione dei servizi di ricerca di dati l'UFSP definisce interfacce standard attraverso le quali le comunità e comunità di riferimento certificate possono ottenere o fornire dati.

Sezione 2: Contenuto

Art. 40 Servizio di ricerca di dati delle comunità e comunità di riferimento

Affinché l'UFSP possa gestire le comunità e comunità di riferimento certificate secondo l'articolo 33 capoverso 1, gli organismi di certificazione devono trasmettere all'UFSP le informazioni in merito alle comunità e comunità di riferimento certificate di cui al *capoverso 1*. In tale contesto, oltre alla designazione (*lett. a*) e all'OID (*lett. b*) sono necessari anche dati che consentano di autenticare in modo sicuro i punti d'accesso e i messaggi delle comunità e comunità di riferimento (*lett. c e d*). Con l'ausilio di questi dati è possibile verificare se il mittente di un messaggio è un partecipante legittimo all'interno dello spazio di fiducia della cartella informatizzata del paziente e se la comunicazione può essere ritenuta affidabile. Questa verifica deve avvenire in modo tanto regolare da consentire che, ad esempio, la comunicazione con un partecipante non più affidabile possa essere rapidamente impedita.

Un trattamento dei dati secondo il *capoverso 2* è consentito solo all'UFSP. Le comunità e comunità di riferimento vi hanno accesso in sola lettura.

Art. 41 Servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute

Secondo l'articolo 9 lettera d, le comunità e comunità di riferimento devono garantire che i dati contenuti nel servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute siano aggiornati. Il servizio di ricerca di dati dispone di un'interfaccia standard attraverso la quale è possibile aggiornare i dati del registro centrale delle strutture sanitarie e dei professionisti della salute e metterli a disposizione di altre comunità e comunità di riferimento. L'articolo 41 precisa quali dati devono essere forniti dalle comunità e comunità di riferimento.

Tra i dati inerenti alle strutture sanitarie e ai gruppi di professionisti della salute secondo il *capoverso 1 lettera a* vi sono in particolare la designazione e l'indirizzo (n. 1), l'*OID* (n. 2) e, per le strutture sanitarie, anche il numero d'identificazione secondo l'articolo 3 capoverso 2 lettera c dell'ordinanza del 30 giugno 1993[12] sul Registro delle imprese e degli stabilimenti (numero RIS) (n. 3). Le comunità e comunità di riferimento devono richiedere gli OID secondo il *numero 2* per le strutture sanitarie ad esse affiliate. Nell'ambito degli OID ad esse assegnati possono gestire altri OID a un livello inferiore per l'identificazione dei gruppi all'interno di una struttura sanitaria (art. 9 cpv. 1).

La registrazione del numero RIS secondo il *numero 3* è necessaria per l'aggregazione dei dati della struttura sanitaria con i dati delle statistiche ufficiali dell'UST per il rilevamento dei dati nell'ambito della valutazione della legge (art. 22 cpv. 3).

Tra i dati riguardanti i professionisti della salute secondo la *lettera b* vi sono in particolare le generalità (*n. 1*), l'OID, che contiene il GLN (*n. 2*) nonché la designazione e l'indirizzo delle strutture sanitarie o dei gruppi di professionisti della salute a cui sono affiliati (*n. 3*). L'OID di cui al *numero 2* è composto dall'OID per il global location number (2.51.1.7) in generale e dal GLN concreto che è stato attribuito al professionista della salute. Se il GLN di un professionista della salute è 7601000000000, l'OID sarà OID 2 2.51.1.7.7601000000000.

Gli altri dati di cui al *capoverso 2* per il servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute sono stabiliti al n. 1.10 del supplemento 1 all'allegato 5 OCIP-DFI.

Art. 42 Servizio di ricerca di dati degli OID

Gli OID sono catene di cifre costruite in modo gerarchico per la designazione univoca a livello mondiale di oggetti di ogni genere, come istituzioni, sistemi, documenti, messaggi, certificati, classificazioni ecc. Per una gestione uniforme di registrazione, attribuzione e applicazione degli OID nell'ambito della sanità pubblica è previsto il nodo OID «eHealth-CH; 2.16.756.5.30», la cui gestione è stata assunta dal 1° gennaio 2011 dalla fondazione RefData in qualità di organismo di registrazione di riferimento. Registrando gli OID specifici per la sanità nel nodo «eHealth-CH» è possibile evitare ulteriori sottoalberi per la sanità pubblica nel nodo OID nazionale. Secondo la strategia messa a punto da eHealth Suisse per l'utilizzo degli OID, le organizzazioni possono creare propri OID per sé stesse e, al di sotto del nodo della propria organizzazione, creare e utilizzare ulteriori OID sotto la loro responsabilità. Ai titolari degli OID si richiede di pubblicare anche i propri identificatori in modo conforme alla protezione dei dati, se gli OID fanno riferimento a propri domini di oggetti. Particolarmente degni di protezione sono gli oggetti il cui riferimento OID – in congiunzione con i dati che identificano la persona nell'oggetto – consente di trarre conclusioni sullo stato di salute della persona.

Dal 1° gennaio 2011 la gestione degli OID è stata assunta dalla fondazione RefData in qualità di organismo di registrazione di riferimento. Le comunità e comunità di riferimento possono richiedere e consultare presso tale fondazione gli OID per l'utilizzo secondo l'articolo 9 capoverso 1 (comunità e comunità di riferimento) e capoverso 2 lettera c (struttura sanitaria). Gli OID per i gruppi di professionisti della salute sono gestiti dalle comunità e comunità di riferimento stesse. L'OID di un professionista della salute si ricava dal suo GLN (cfr. commenti all'art. 41).

[12] **RS** 431.903

Art. 43 Emolumenti

Sulla base della stima che in Svizzera saranno costituite circa dieci comunità e comunità di riferimento, un emolumento annuo di 40 000 franchi appare adeguato. Tale importo consente un rifinanziamento dei costi per la costituzione e la gestione dei servizi di ricerca di dati per un periodo di dieci anni (*cpv. 1*). L'emolumento è forfettario, dal momento che i servizi di ricerca di dati sono utilizzati nella stessa misura da tutte le comunità e comunità di riferimento. Inoltre, il volume di dati elaborato da una comunità o comunità di riferimento è trascurabile per il calcolo dei costi, in quanto la parte preponderante di essi è rappresentata dalla costituzione dei servizi stessi.

Il *capoverso 2* stabilisce che per il resto si applicano le disposizioni dell'ordinanza generale dell'8 settembre 2004 sugli emolumenti (RS 172.041.1), che contiene in particolare prescrizioni riguardanti fatturazione, esigibilità e prescrizione.

Capitolo 8: Entrata in vigore

Art. 44

La LCIP e le relative disposizioni esecutive (OCIP, OCIP-DFI e OFCIP) entrano in vigore il 15 aprile 2017.