Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI

RS 816.111

Allegato 2 dell'ordinanza del DFI del 22 marzo 2017 sulla cartella informatizzata del paziente

Condizioni tecniche e organizzative di certificazione delle comunità e comunità di riferimento

Edizione 2: 24 giugno 2019

Entrate in vigore: 15 luglio 2019

A. Requisiti per le comunità

1 Identificatore di oggetto e gestione (art. 9 OCIP)

1.1 Identificatore di oggetto (art. 9 cpv. 1)

Le comunità devono richiedere al servizio di ricerca di dati per gli identificatori di oggetto (OID) un OID ai sensi dell'articolo 42 per sé stesse e per le strutture sanitarie ad esse affiliate.

1.2 Gestione delle strutture sanitarie (art. 9 cpv. 2 lett. a e d OCIP)

1.2.1 Le comunità stabiliscono i processi per l'ingresso, la gestione e l'uscita delle strutture sanitarie.

1.2.2 Il processo per l'ingresso delle strutture sanitarie deve garantire che:

a. venga richiesto un OID al servizio di ricerca di dati per gli OID secondo l'articolo 42 OCIP;
b. siano stipulati contratti con le strutture sanitarie sui loro compiti e obblighi, in particolare in materia di protezione e sicurezza dei dati secondo il numero 4.7;
c. sia avviato il processo di «ingresso di professionisti della salute» (cfr. n. 1.3.3) per tutti i professionisti della salute che aderiscono a una struttura sanitaria;
d. siano aggiornati i dati del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP;
e. sia aggiornato l'«inventario della struttura informatica» di cui al numero 4.6.

1.2.3 Il processo per l'uscita di strutture sanitarie deve garantire che:

a. sia avviato il processo di «uscita di professionisti della salute» (cfr. n. 1.3.5) per tutti i professionisti della salute della struttura sanitaria uscente;
b. qualora una struttura sanitaria uscente non dovesse aderire a nessun'altra comunità, i dati della struttura sanitaria uscente riguardanti la cartella informatizzata del paziente rimangano accessibili;
c. sia aggiornato l'«inventario dell'infrastruttura informatica» di cui al numero 4.6.

1.2.4 Per i dati da esse registrati nel servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP, le comunità devono:

a. designare una persona responsabile;
b. garantire una verifica regolare dell'aggiornamento e della correttezza dei dati.

1.3 Gestione dei professionisti della salute (art. 9 cpv. 2 lett. a-f OCIP)

1.3.1 Le comunità stabiliscono i processi per l'ingresso, la gestione e l'uscita dei professionisti della salute.

1.3.2 Esse assicurano l'aggiornamento dei dati nel servizio di ricerca dei dati delle strutture sanitarie e dei professionisti della salute secondo l'articolo 41 OCIP.

1.3.3 Il processo per l'ingresso di professionisti della salute deve garantire che:

a. il professionista della salute s'impegni a rispettare le direttive specifiche della comunità sull'impiego della cartella informatizzata del paziente (cfr. n. 4.7.1 lett. b);

b. il professionista della salute sia identificato mediante un apposito strumento d'identificazione rilasciato da un emittente certificato o in conformità ai requisiti dell'articolo 24 OCIP;

c. si tratti di un professionista della salute secondo l'articolo 2 lettera b LCIP;

d. siano aggiornati i dati del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP;

e. qualora il professionista della salute sia iscritto in un registro professionale federale o cantonale, i dati ivi contenuti devono essere ripresi.

1.3.4 Il processo per la gestione di professionisti della salute deve garantire che:

a. siano aggiornati i dati del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP;

b. i presupposti per l'accesso alla cartella informatizzata del paziente siano sottoposti periodicamente a una verifica.

1.3.5 Il processo per l'uscita di professionisti della salute deve garantire che:

a. siano aggiornati i dati del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP;

b. l'accesso alla cartella informatizzata del paziente sia disattivato per il professionista della salute uscente.

1.4 Identificazione e autenticazione (art. 9 cpv. 2 lett. e OCIP)

1.4.1 Per accedere alla cartella informatizzata del paziente, i professionisti della salute devono autenticarsi mediante uno strumento d'identificazione valido, rilasciato da un emittente certificato secondo l'articolo 31 OCIP.

1.4.2 Le comunità devono garantire che l'identificatore univoco di cui all'articolo 25 capoverso 1 OCIP sia collegato al professionista della salute giusto e al suo GLN.

1.4.3 Le comunità devono riconoscere l'autenticazione di cui al numero 1.4.1 di un'altra comunità o comunità di riferimento certificata.

1.4.4 Le comunità devono garantire che l'identificatore univoco di cui all'articolo 25 capoverso 1 OCIP venga collegato con il paziente giusto e il suo numero d'identificazione.

1.5 Gestione di gruppi di professionisti della salute (art. 9 cpv. 2 lett. a, c, d ed f OCIP)

1.5.1 Le comunità sono responsabili della gestione dei gruppi di professionisti della salute e stabiliscono il processo per la loro gestione.

1.5.2 Il processo deve garantire che:

a. venga assegnato ai gruppi di professionisti della salute un OID che si basi sull'OID della struttura sanitaria;

b. siano aggiornati i dati nel servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP;
c. i pazienti che lo richiedono siano informati sull'ingresso di professionisti della salute in gruppi di professionisti della salute.

1.6 Gestione degli ausiliari dei professionisti della salute

1.6.1 Le comunità stabiliscono il processo per la gestione degli ausiliari.

1.6.2 Per accedere alla cartella informatizzata del paziente, gli ausiliari devono autenticarsi mediante uno strumento d'identificazione valido, rilasciato da un emittente certificato secondo l'articolo 31 OCIP.

1.6.3 Per la gestione degli ausiliari si applicano per analogia i numeri 1.3 e 1.4.2, fatto salvo l'aggiornamento del servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute di cui all'articolo 41 OCIP.

2 Conservazione e trasmissione di dati (art. 10 OCIP)

2.1 Applicazione dei gradi di riservatezza (art. 10 cpv. 1 lett. a OCIP)

Le comunità devono garantire che:
a. il paziente possa attribuire i gradi di riservatezza ai dati medici della sua cartella informatizzata in base alle prescrizioni dell'articolo 1 OCIP;
b. ai nuovi dati configurati sia attribuito il grado di riservatezza secondo l'articolo 1 capoverso 2 OCIP o secondo l'opzione scelta dal paziente come previsto all'articolo 4 lettera a OCIP;
c. i professionisti della salute possano attribuire ai nuovi dati configurati il grado di riservatezza «limitatamente accessibile».

2.2 Accesso di emergenza (art. 10 cpv. 1 lett. a OCIP)

In caso di accesso per situazioni di emergenza medica, le comunità devono garantire che:
a. il professionista della salute che accede ai dati debba confermare l'accesso in modo tale da evitare efficacemente gli abusi, in particolare quelli causati da un software dannoso installato sul terminale;
b. il paziente venga informato entro un termine adeguato;
c. nel caso in cui l'informazione sull'accesso di emergenza venga trasmessa elettronicamente al di fuori della cartella informatizzata del paziente (p. es. SMS, e-mail), che non contenga dati particolarmente degni di protezione.

2.3 Attuazione della decisione di accesso (art. 10 cpv. 1 lett. a OCIP)

2.3.1 Le comunità devono garantire che l'accesso ai dati dei loro archivi e registri di documenti possa avvenire solo previo ottenimento della decisione di accesso da parte della comunità di riferimento del paziente.

2.3.2 L'amministrazione dei diritti deve offrire la possibilità di verificare la correttezza delle decisioni di accesso nell'ambito della procedura di certificazione mediante il sistema di test di certificazione.

2.4 Archivio di documenti (art. 10 cpv. 1 lett. b e cpv. 3 OCIP)

2.4.1 Le comunità devono garantire che:

a. le strutture sanitarie affiliate siano dotate di regole che consentano di mettere a disposizione nella cartella informatizzata del paziente solo i dati provenienti dall'anamnesi del paziente che sono rilevanti per la terapia;

b. i dati medici della cartella informatizzata del paziente siano memorizzati negli archivi di documenti separatamente da altre raccolte di dati e in modo tale da non poter essere utilizzati in modo abusivo per altri scopi;

c. negli archivi di dati siano memorizzati solo i tipi di media («*MIME MediaType*») ammessi secondo il numero 2.13 dell'allegato 3 dell'OCIP-DFI;

d. i file in formato «Portable Document Format» (PDF) siano memorizzati esclusivamente in versione PDF/A-1 o PDF/A-2;

e. i file del tipo «Portable Document Format» (PDF) non possano contenere né scaricare codici eseguibili oppure garantire in altro modo che non contengano un codice dannoso;

f. nei dati medici visualizzabili venga impiegato Unicode UTF-8 come codifica dei caratteri.

2.5 Memorizzazione e trasferimento di dati criptati (art. 10 cpv. 1 lett. c OCIP)

Le comunità devono adottare misure di criptaggio adeguate e conformi allo stato attuale della tecnica, tenendo conto delle prescrizioni di cui al numero 4.12, affinché i dati della cartella informatizzata del paziente:

a. siano protetti dalla perdita di riservatezza, autenticità e integrità durante ogni trasmissione;

b. siano memorizzati criptati e protetti da modifiche abusive o inosservate.

2.6 Distruzione di dati (art. 10 cpv. 1 lett. d ed e OCIP)

Le comunità devono prevedere procedure per garantire che:

a. i dati registrati presso di esse dai professionisti della salute nella cartella informatizzata del paziente siano distrutti dopo 20 anni, fatto salvo il numero 2.7 lett. b;

b. in caso di soppressione secondo l'articolo 21 OCIP, vengano distrutti tutti i dati della cartella informatizzata del paziente. In particolare bisognerà distruggere i relativi dati negli elementi della struttura informatica menzionati nel numero 4.6.2. lettere a-i dell'«inventario dell'infrastruttura informatica» e cancellare il numero d'identificazione del paziente da tutti i sistemi.

2.7 Opzioni per i pazienti (art. 10 cpv. 2 OCIP)

Le comunità devono prevedere procedure tecniche e organizzative in modo che su richiesta del paziente determinati dati medici a lui riferiti:

a. non vengano registrati nella cartella informatizzata del paziente;
b. siano esclusi dalla distruzione secondo l'articolo 10 capoverso 1 lettera d OCIP;
c. siano distrutti nella cartella informatizzata del paziente.

2.8 Metadati (art. 10 cpv. 3 lett. a OCIP)

Le comunità devono garantire che vengano utilizzati i metadati di cui all'allegato 3 dell'OCIP-DFI.

2.9 Prescrizioni per la gestione e il trasferimento dei dati della cartella informatizzata del paziente (art. 10 cpv. 3 lett. c OCIP)

Interfaccia standard per la banca dati d'identificazione dell'Ufficio centrale di compensazione (UCC)

2.9.1 I punti di accesso delle comunità possono utilizzare unicamente le seguenti interfacce tecniche per la banca dati d'identificazione fornite dall'UCC per l'emissione e l'impiego del numero d'identificazione del paziente:

a. interfaccia standard eCH-0213 Annunci UPI/SPID (versione 1.0 del 13 settembre 2017);
b. interfaccia standard eCH-0214 Interrogazione UPI/SPID (versione 2.0 del 3 dicembre 2018);
c. interfaccia standard eCH-0215: Broadcast di mutazioni UPI/SPID (versione 2.0 del 3 dicembre 2018).

2.9.2 Le comunità devono rispettare le prescrizioni dell'UCC sull'impiego tecnico corretto delle interfacce e le prescrizioni organizzative secondo il regolamento di utilizzazione. Le comunità devono in particolare adottare misure adeguate onde assicurarsi di non modificare in modo abusivo o scorretto i dati della banca dati d'identificazione dell'UCC.

Profili d'integrazione IHE, adeguamenti nazionali dei profili d'integrazione IHE e profili d'integrazione nazionali

2.9.3 Per la trasmissione delle informazioni, le comunità devono utilizzare i profili d'integrazione IHE, i loro adeguamenti nazionali e i profili d'integrazione nazionali secondo l'allegato 5 dell'OCIP-DFI.

Comunicazione intercomunitaria

2.9.4 Gli attori IHE *Initiating Gateway* e *Responding Gateway* devono supportare le seguenti transazioni dei profili d'integrazione IHE XCA, IHE XCPD e IHE XDS nelle versioni di cui all'allegato 5 dell'OCIP-DFI:

a. Cross Gateway Query [ITI-38];
b. Cross Gateway Retrieve [ITI-39];
c. Cross Gateway Patient Discovery [ITI-55];

d. Registry Stored Query [ITI-18];
e. Retrieve Document Set [ITI-43].

2.9.5 Gli attori IHE *Initiating Gateway* e *Responding Imaging Gateway* devono supportare le seguenti transazioni dei profili d'integrazione IHE XCA-I, XDS-I.b e IHE XCPD nelle versioni di cui all'allegato 5 dell'OCIP-DFI:

a. Cross Gateway Retrieve Image Document Set [RAD-75];
b. Retrieve Image Document Set [RAD-69];
c. Cross Gateway Patient Discovery [ITI-55].

Consultazione di dati verbalizzati da parte dei pazienti

2.9.5*a* Gli attori *Patient Audit Consumer* e *Patient Audit Record Repository* devono supportare la transazione *Retrieve Audit Event* [ITI-81] del profilo d'integrazione nazionale ATC secondo l'allegato 5 dell'OCIP-DFI ed essere raggruppati con la transazione *Incorporate Authorization Token* [ITI-72] del profilo IHE-IUA.

Comunicazione di identità autenticate

2.9.6 Gli attori IHE *X-Service Provider* e *X-Service User* del profilo d'integrazione XUA sono raggruppati con altri attori in base alle prescrizioni dei profili d'integrazione nazionali e agli adeguamenti dei profili d'integrazione secondo l'allegato 5 dell'OCIP-DFI.

2.9.7 L'attore IHE *X-Service User* deve supportare le seguenti transazioni del profilo d'integrazione XUA nella versione di cui all'allegato 5 dell'OCIP-DFI:

a. Authenticate User;
b. Get X-User Assertion;
c. Provide X-User Assertion [ITI-40].

2.9.7*a* L'attore IHE *X-Service Provider* deve verificare le informazioni rilevanti ai fini dei diritti («claim») fornite dall'attore IHE *X-Service User*, in particolare i dati su identificatori o correlazioni tra di essi, consultando fonti affidabili (cfr. n. 3.1b.1).

2.9.7*b* L'attore IHE *X-Service Provider* deve supportare la transazione *Provide X-User Assertion* [ITI-40] del profilo d'integrazione XUA nella versione di cui all'allegato 5 dell'OCIP-DFI.

2.9.7*c* L'attore IHE *X-Assertion Provider* deve supportare la transazione *Get X-User Assertion* del profilo d'integrazione XUA nella versione di cui all'allegato 5 dell'OCIP-DFI.

Servizio di ricerca di dati per strutture sanitarie e professionisti della salute

2.9.8 Gli attori IHE *Provider Information Consumer* e *Provider Information Source* devono supportare le seguenti transazioni del profilo d'integrazione IHE HPD nella versione di cui all'allegato 5 dell'OCIP-DFI:

a. Provider Information Query [ITI-58];
b. Provider Information Feed [ITI-59];
c. Provider Information Delta Download (CH:PIDD).

Consultazione di dati medici

2.9.9 L'attore IHE *Document Consumer* deve supportare le seguenti transazioni del profilo d'integrazione IHE XDS nella versione di cui all'allegato 5 dell'OCIP-DFI:

a. Registry Stored Query [ITI-18];
b. Retrieve Document Set [ITI-43].

2.9.10 L'attore IHE *Imaging Document Consumer* deve supportare la transazione *Retrieve Imaging Document Set* [RAD-69] del profilo d'integrazione IHE XDS-I.b nella versione di cui all'allegato 5 dell'OCIP-DFI.

Messa a disposizione di dati medici

2.9.11 L'attore IHE *Document Source* deve supportare le transazioni *Provide and Register Document Set-b* [ITI-41] del profilo d'integrazione IHE XDS.b nella versione di cui all'allegato 5 dell'OCIP-DFI.

2.9.11*a* Se l'attore IHE *Document Source* fornisce dati medici in differita senza che l'utente responsabile della fornitura possa autenticarsi validamente o nuovamente, devono essere soddisfatte le prescrizioni di cui al numero 1.6.4.2.4.2.3 (*Technical User Extension*) del profilo d'integrazione XUA di cui all'allegato 5 dell'OCIP-DFI.

2.9.12 L'attore IHE *Imaging Document Source* deve supportare le seguenti transazioni del profilo d'integrazione IHE XDS-I.b nella versione di cui all'allegato 5 dell'OCIP-DFI:

a. Provide and Register Imaging Document Set – MTOM/XOP [RAD-68];
b. Retrieve Imaging Document Set [ITI-69].

Mutazione di metadati dei dati medici

2.9.13 L'attore IHE *Document Administrator* deve supportare la transazione *Update Document Set* [ITI-57] del profilo d'integrazione IHE XDS Metadata Update nella versione di cui all'allegato 5 dell'OCIP-DFI.

2.9.13*a* Gli attori IHE *Update Initiator* e *Update Responder* devono supportare la transazione *Restricted Update Document Set* [ITI-92] del profilo d'integrazione IHE *Restricted Metadata Update* (RMU) secondo l'allegato 5 dell'OCIP-DFI.

Registro dei documenti

2.9.14 L'attore IHE *Document Registry* deve supportare le seguenti transazioni dei profili d'integrazione XDS e XDS Metadata Update nelle versioni di cui all'allegato 5 dell'OCIP-DFI:

a. Register Document Set-b [ITI-42];
b. Registry Stored Query [ITI-18];
c. Update Document Set [ITI-57];
d. Patient Identity Feed HL7 V3 [ITI-44].

Sistema di archiviazione dei documenti

2.9.15 L'attore IHE *Document Repository* deve supportare le seguenti transazioni del profilo d'integrazione IHE XDS nella versione di cui all'allegato 5 dell'OCIP-DFI:

a. Provide and Register Document Set-b [ITI-41];
b. Retrieve Document Set [ITI-43].

2.9.16 Gli attori IHE *Portable Media Creator* e *Portable Media Importer* devono supportare la transazione *Distribute Document Set on Media* [ITI-32] del profilo d'integrazione XDM nella versione di cui all'allegato 5 dell'OCIP-DFI.

Messa a disposizione dei dati per l'indice dei pazienti

2.9.17 L'attore IHE *Patient Identity Source* deve supportare la transazione *Patient Identity Feed HL7 V3 [ITI-44]* del profilo d'integrazione PIX V3 nella versione di cui all'allegato 5 dell'OCIP-DFI.

Messa a disposizione e consultazione dell'indice dei pazienti

2.9.18 Gli attori IHE *Patient Demographics Supplier* e *Patient Demographics Consumer* devono supportare la transazione *Patient Demographics Query V3 [ITI-47]* del profilo d'integrazione PDQ V3 nella versione di cui all'allegato 5 dell'OCIP-DFI:

Gestione dell'indice dei pazienti

2.9.19 L'attore IHE *Patient Identifier Cross-reference Manager* deve supportare le seguenti transazioni del profilo d'integrazione IHE PIX V3 nelle versioni di cui all'allegato 5 dell'OCIP-DFI:

a. Patient Identity Feed HL7 V3 [ITI-44];
b. PIX V3 Query [ITI-45];
c. PIX V3 Update Notification [ITI-46].

Autenticazione di sistemi e verbalizzazione delle transazioni IHE

2.9.20 Gli attori IHE *Secure Application* e *Secure Node* del profilo d'integrazione IHE ATNA (o del suo adeguamento nazionale) vengono raggruppati con altri attori IHE in base alle prescrizioni dei profili d'integrazione IHE, dei profili d'integrazione nazionali e degli adeguamenti dei profili d'integrazione secondo l'allegato 5 dell'OCIP-DFI.

2.9.21 Tutti gli attori IHE nel ruolo *Secure Node* di cui al numero 2.9.20 devono supportare le seguenti transazioni del profilo d'integrazione IHE ATNA e del suo adeguamento nazionale secondo l'allegato 5 dell'OCIP-DFI:

a. Maintain Time [ITI-1];
b. Authenticate Node [ITI-19];
c. Record Audit Event [ITI-20].

2.9.22 Gli attori IHE nel ruolo *Secure Application* devono supportare le seguenti transazioni del profilo d'integrazione IHE ATNA e del suo adeguamento nazionale secondo l'allegato 5 dell'OCIP-DFI:

a. Maintain Time [ITI-1];
b. Record Audit Event [ITI-20].

Consultazione della decisione di autorizzazione

2.9.23 L'attore *Authorization Decision Consumer* del profilo d'integrazione nazionale CH:ADR deve essere raggruppato con altri attori IHE in base alle prescrizioni del profilo d'integrazione nazionale CH:ADR secondo l'allegato 5 dell'OCIP-DFI.

2.9.24 Gli attori *Authorization Decision Provider* e *Authorization Decision Consumer* devono supportare la transazione *Authorization Decision Request* [CH:ADR] del profilo d'integrazione nazionale CH:ADR secondo l'allegato 5 dell'OCIP-DFI.

Amministrazione della configurazione dei diritti

2.9.25 Gli attori *Policy Source* e *Policy Repository* devono supportare la transazione *Privacy Policy Feed* [CH:PPQ-1] e gli attori *Policy Consumer* e *Policy Repository* la transazione *Privacy Policy Retrieve* [CH:PPQ-2] del profilo d'integrazione nazionale CH:PPQ secondo l'allegato 5 dell'OCIP-DFI.

2.9.25*a* Le comunità devono garantire che l'attore *Policy Repository* del profilo d'integrazione nazionale CH:PPQ secondo l'allegato 5 dell'OCIP-DFI:

a. ammetta unicamente i trattamenti delle configurazioni dei diritti da parte di sistemi registrati nella comunità e autorizzati a tale scopo (attori IHE Policy Source e Policy Consumer; cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.** lett. **Fehler! Verweisquelle konnte nicht gefunden werden.**);
b. ammetta unicamente trattamenti delle configurazioni dei diritti attribuite alle persone nelle identità autenticate o che possono essere trattate da tali persone;
c. adotti misure tecniche e organizzative per proteggere le configurazioni dei diritti da modifiche abusive non specificate o non conformi alle regole dell'amministrazione dei diritti secondo gli articoli 1-4 OCIP.

Autenticazione con certificati validi

2.9.26 Le comunità devono essere in possesso di un certificato elettronico valido, rilasciato da un prestatore di servizi di certificazione riconosciuto secondo la legge federale del 18 marzo 2016 sulla firma elettronica (FiEle; RS 943.03) per:

a. l'autenticazione reciproca dei loro endpoint e punti di accesso che comunicano a livello intercomunitario;
b. l'autenticazione reciproca dei loro punti di accesso nei confronti dei servizi di ricerca di dati secondo l'articolo 39 lettere a-c OCIP;
c. l'autenticazione reciproca dei loro punti di accesso nei confronti della banca dati d'identificazione dell'UCC.

2.9.26*a* Le comunità devono garantire che:

a. lo scambio intercomunitario di dati avvenga unicamente con gli endpoint autenticati secondo il numero **Fehler! Verweisquelle konnte nicht gefunden werden.** lettera a registrati nel servizio di ricerca di dati delle comunità e comunità di riferimento secondo l'articolo 40 capoverso 1 OCIP;
b. gli endpoint registrati nel servizio di ricerca di dati delle comunità e comunità di riferimento quali partner di comunicazione affidabili siano controllati periodicamente, in modo da poter interrompere rapidamente qualsiasi comunicazione con gli endpoint non più affidabili (cfr. art. 37 cpv. 1 lett. a OCIP).

Scambio di dati con i servizi di ricerca di dati secondo l'articolo 39

2.9.26*b* Per lo scambio di dati con il servizio di ricerca di dati secondo l'articolo 39 lettera a OCIP per l'attore *CPI Consumer*, le comunità devono utilizzare le seguenti transazioni del profilo d'integrazione nazionale CH:CPI secondo l'allegato 5 dell'OCIP-DFI:

c. Community Information Query (CH:CIQ);

d. Community Information Delta Download (CH:CIDD).

2.9.27 Per lo scambio di dati con il servizio di ricerca di dati secondo l'articolo 39 lettera c OCIP per l'attore IHE *Value Set Consumer*, le comunità devono utilizzare la transazione *Retrieve Value Set* [ITI-48] del profilo d'integrazione IHE SVS secondo l'allegato 5 dell'OCIP-DFI.

2.9.28 Per lo scambio di dati con i servizi di ricerca di dati secondo l'articolo 39 lettere a e c OCIP, le comunità devono utilizzare le seguenti transazioni del profilo d'integrazione IHE ATNA secondo l'allegato 5 dell'OCIP-DFI:

a. Maintain Time [ITI-1];

b. Authenticate Node [ITI-19];

c. Record Audit Event [ITI-20].

2.9.29 Per lo scambio di dati con la banca dati d'identificazione dell'UCC, le comunità devono utilizzare la piattaforma per lo scambio dati SEDEX (*«secure data exchange»*) dell'Ufficio federale di statistica.

Ora determinante

2.9.30 Per la marca temporale impiegata nella comunicazione e verbalizzazione è determinante l'ora ufficiale in Svizzera del METAS (cfr. n. 2.9.21 e 2.9.22).

2.10 Dati verbalizzati (art. 10 cpv. 3 lett. d OCIP)

2.10.1 Ogni trattamento di dati della cartella informatizzata del paziente deve essere verbalizzato e recare una marca temporale aggiornata.

2.10.2 Il trattamento dei seguenti dati deve essere verbalizzato sia per i tentativi riusciti che per quelli respinti:

a. dei dati medici negli archivi di documenti;

b. delle iscrizioni nel registro di documenti;

c. della configurazione dell'amministrazione dei diritti;

d. dei dati dell'indice dei pazienti.

2.10.3 Devono inoltre essere verbalizzati i seguenti eventi:

a. le autenticazioni nel sistema (login/logout);

b. le transazioni intercomunitarie attraverso i punti di accesso delle comunità;

c. la ricerca di un paziente;

d. la ricerca di dati medici di una cartella informatizzata del paziente;

e. un accesso di emergenza a una cartella informatizzata del paziente;

f. gli accessi e i tentativi di accesso a dati medici di una cartella informatizzata del paziente.

2.10.4 In ogni caso è necessario verbalizzare almeno:

a. l'evento stesso («*Event Identification*») e il contesto nel quale si è verificato (esercizio normale, accesso di emergenza, utilizzo di diritti di accesso speciali privilegiati);
b. il momento in cui si è verificato l'evento («*Event Timestamp*»);
c. la persona che ha attivato l'evento («*Active Participant Identification*»);
d. il luogo in cui l'evento è stato attivato («*Network Access Point Identification*»);
e. la causa dell'evento («*Audit Source Identification*»);
f. i record dati interessati («*Participant Object Identification*»);
g. l'esito dell'evento («*Event Outcome Indicator*»).

2.10.5 Per una ricerca è necessario verbalizzare almeno i criteri della ricerca.

2.10.6 I dati verbalizzati devono essere limitati allo stretto necessario e non devono contenere documenti.

2.10.7 La verbalizzazione deve soddisfare i seguenti requisiti:

a. oltre agli identificatori si deve verbalizzare un testo leggibile dall'essere umano che designa l'entità referenziata al momento della verbalizzazione;
b. non deve essere possibile aggirare le verbalizzazioni prescritte;
c. le modifiche a posteriori dei dati verbalizzati devono essere riconoscibili e rintracciabili;
d. nella verbalizzazione si devono distinguere gli accessi risultanti dall'impiego della cartella informatizzata del paziente e gli accessi tecnico-amministrativi effettuati nell'ambito dell'esercizio del sistema;
e. gli amministratori del sistema non devono avere la possibilità di cancellare o disattivare la verbalizzazione delle proprie attività.

2.10.8 I dati verbalizzati secondo i numeri da 2.10.1 a 2.10.3 devono essere conservati per 10 anni e in seguito devono essere distrutti.

2.10.9 La consultazione e la visualizzazione di informazioni verbalizzate visionabili dal paziente si basano sul profilo d'integrazione nazionale CH:ATC secondo l'allegato 5 dell'OCIP-DFI.

2.10.10 Le comunità devono garantire che i trattamenti di dati siano verbalizzati in modo che i dati possano essere messi a disposizione per la valutazione secondo l'articolo 6 OCIP-DFI.

2.11 Collegamento del numero d'identificazione del paziente con dati medici (art. 10 cpv. 3 OCIP)

Le comunità devono garantire che il numero d'identificazione del paziente attribuito dall'UCC non venga memorizzato negli archivi dei documenti o nei registri dei documenti.

3 Portale di accesso per i professionisti della salute (art. 11 OCIP)

3.1 Visualizzazione

La visualizzazione sull'interfaccia utente del portale di accesso deve essere corretta e completa e indicare chiaramente:

a. se i dati medici sono stati messi a disposizione da un professionista della salute o dal paziente stesso;
b. quali dati medici sono stati messi a disposizione dal professionista della salute autorizzato all'accesso;
c. quali dati medici sono stati annullati;
d. quali versioni dei dati medici sono disponibili;
e. se il professionista della salute tratta dati della cartella informatizzata del paziente.

3.1.2 L'interfaccia utente del portale di accesso può visualizzare dati medici o metadati solo se il professionista della salute dispone dei relativi diritti di accesso.

3.1*a* Marchio di certificazione

3.1*a*.1 Il portale di accesso alla cartella informatizzata del paziente deve essere contrassegnato con uno dei seguenti due marchi di certificazione:

3.1*a*.2 Il marchio deve essere riprodotto a colori.

3.1*a*.3 Le comunità certificate non possono utilizzare il marchio di certificazione in un modo o in un contesto che possa indurre in inganno.

3.1*b* Affidabilità dei portali di accesso

3.1*b*.1 Previa approvazione del responsabile della protezione e della sicurezza dei dati, per le informazioni rilevanti ai fini dei diritti pubblicate dai portali di accesso è possibile rinunciare alla verifica di cui al numero 2.9.7a.

3.2 Assenza di barriere

Il portale di accesso deve soddisfare i requisiti di conformità stabiliti dalle *Web Content Accessibility Guidelines* (WCAG) 2.0 e raggiungere almeno il livello di conformità AA.

3.3 Consultazione e tipi di media dei dati medici

Il portale di accesso deve:

a. supportare i tipi di media di cui al numero 2.8 dell'allegato 3 OCIP-DFI;
b. supportare l'importazione di dati medici e la consultazione di dati medici da memorizzare nel sistema primario della struttura sanitaria;
c. offrire la possibilità di importare o scaricare dati medici singolarmente o raggruppati;
d. presentare in modo corretto e completo dati strutturati leggibili dall'essere umano;
e. supportare il download di dati strutturati sia nel formato originale che in un formato leggibile dall'essere umano;
f. per la consultazione dei dati medici destinati a essere visualizzati o memorizzati, prevedere un limite massimo ammissibile di dati medici per unità temporale, al superamento del quale si attivano idonee misure di blocco o misure di sicurezza supplementari.

3.4 Requisiti tecnici

3.4.1 Oltre ai requisiti in materia di protezione e sicurezza dei dati di cui al numero 4, il portale di accesso deve:

a. effettuare una verifica attiva mediante test di penetrazione per individuare eventuali lacune di sicurezza almeno dopo ogni modifica rilevante per la sicurezza dei mezzi informatici del portale di accesso;
b. essere concepito in modo da escludere l'accesso al funzionamento interno e manipolazioni abusive.

3.4.2 Il portale di accesso deve essere protetto dalle forme note di attacco e compromissione.

3.4.3 L'autenticazione mediante il portale di accesso è disciplinata conformemente all'allegato 8 OCIP-DFI.

4 Protezione e sicurezza dei dati (art. 12 OCIP)

4.1 Requisiti per terzi

Le comunità devono assicurare il rispetto dei requisiti stabiliti in questo capitolo anche quando fanno eseguire prestazioni da terzi (in particolare le organizzazioni di gestione, i fornitori e i gestori di piattaforme, i fornitori e i gestori di periferiche e terminali).

4.2 Sistema di gestione della protezione e della sicurezza dei dati (art. 12 cpv. 1 OCIP)

4.2.1 Le comunità devono sviluppare, mantenere e controllare periodicamente un sistema di gestione della protezione e della sicurezza dei dati nonché migliorarne continuamente l'idoneità, l'adeguatezza e l'efficacia conformemente alla norma DIN EN ISO/IEC 27001:2017-06. Il sistema deve essere adeguato al rischio e:

a. definire misure adeguate, in particolare direttive, processi, procedure, strutture organizzative nonché funzioni di software e hardware, volte a soddisfare le disposizioni qui menzionate;
b. stabilire le responsabilità generali e specifiche per la gestione della protezione e della sicurezza dei dati per determinate funzioni e attribuirle alle persone responsabili;
c. proteggere da smarrimento, distruzione e falsificazione tutte le registrazioni rilevanti nel rispetto dei requisiti legali.

4.2.2 Il sistema di gestione della protezione e della sicurezza dei dati deve essere reso noto all'interno della comunità a tutte le strutture sanitarie e ai professionisti della salute. Per i professionisti della salute occorre in particolare svolgere e documentare corsi di formazione sulle prescrizioni a cui sono soggetti nonché esercitare i processi critici.

4.2.3 Il sistema di gestione della protezione e della sicurezza dei dati deve comprendere almeno:

a. un catalogo dei rischi valutato dal responsabile della protezione e della sicurezza dei dati (cfr. n. 4.11), compreso un registro dei rischi;
b. un piano di trattamento dei rischi;
c. un inventario aggiornato delle risorse della comunità rilevanti per la valutazione e il trattamento del rischio. Questo comprende in particolare:
    i. i dati e le identità della cartella informatizzata del paziente e i processi per la loro elaborazione (oggetti primari da proteggere);
    ii. i sistemi, le infrastrutture, le applicazioni, le interfacce, i dispositivi, le strutture organizzative, le persone e i processi dai quali dipende la protezione degli oggetti primari.
d. l'accettazione documentata dei rischi residui da parte della comunità.

4.2.4 Le modifiche rilevanti per la sicurezza apportate alle risorse devono essere valutate e documentate.

4.2.5 Le comunità devono mantenere aggiornati e verificare almeno una volta all'anno il catalogo dei rischi e il piano di trattamento dei rischi.

4.3 Monitoraggio e gestione di incidenti di sicurezza (art. 12 cpv. 1 lett. a OCIP)

4.3.1 Le comunità devono istituire, amministrare e migliorare continuamente procedure tecniche e organizzative coordinate intese a monitorare e gestire gli incidenti di sicurezza, affinché:

a. controllino in modo commisurato al rischio almeno gli elementi definiti come rilevanti per il rischio nell'«inventario dell'infrastruttura informatica» di cui al numero 4.6;

b. individuino anomalie nel sistema;

c. registrino gli eventi di protezione e sicurezza dei dati in modo da proteggere i dati da modifiche abusive o inosservate.

4.3.2 Le procedure per l'individuazione, l'analisi e la documentazione delle anomalie e degli incidenti di sicurezza devono essere definite in modo specifico per ogni comunità, essere adeguate al rischio nonché riconoscere e gestire almeno le seguenti anomalie:

a. attacchi provenienti da Internet rivolti a portali di accesso o al punto di accesso della comunità;

b. schemi inusuali di accessi di lettura o scrittura agli archivi dei documenti, ai registri dei documenti o all'indice dei pazienti, che potrebbero indicare un impiego abusivo o attacchi automatizzati;

c. mutazioni inusuali e critiche di dati relativi ai diritti di accesso nell'amministrazione dei diritti, nel sistema di gestione delle identità e degli accessi (IAM) o, se presente, nel servizio interno della comunità per la gestione delle strutture sanitarie e dei professionisti della salute.

4.3.3 Nell'ambito delle misure illustrate al numero 4.3.1, le comunità devono:

a. prevedere procedure per la notifica immediata di eventi di protezione e sicurezza dei dati agli appositi servizi competenti della comunità e all'UFSP (art. 12 cpv. 3 OCIP);

b. prevedere processi per reagire tempestivamente agli eventi e affrontare le cause che minacciano la protezione o la sicurezza dei dati;

c. in caso di eventi critici per la sicurezza di un determinato livello, prevedere processi di emergenza adeguati volti a mitigare gli effetti nocivi, in particolare definire come e a quali condizioni i sistemi della comunità critici per la sicurezza debbano essere isolati dall'esterno o dall'interno da accessi pericolosi.

4.4 Gestione delle lacune di sicurezza (art. 12 cpv. 1 lett. a OCIP)

4.4.1 Le comunità devono essere dotate di una gestione delle lacune di sicurezza che raccolga periodicamente e in tempo utile informazioni sulle lacune di sicurezza tecniche dei mezzi informatici utilizzati per la cartella informatizzata del paziente, valuti la vulnerabilità dei mezzi informatici allo sfruttamento di tali lacune e adotti misure adeguate per gestire i rischi connessi.

4.4.2 Se per l'eliminazione delle lacune di sicurezza non è ancora disponibile un'apposita correzione del software («p*atch*»), si devono contemplare e se possibile adottare misure di sicurezza alternative. I rischi residui devono essere identificati e accettati espressamente.

4.4.3 Le comunità devono garantire che:

a. la superficie di attacco dei mezzi informatici sia ridotta al minimo («hardening» dei sistemi). Devono definire le procedure necessarie a tal fine e garantirne lo l'esecuzione e il controllo;

b. le funzioni e le interfacce inutilizzate siano disattivate;

c. i mezzi informatici siano protetti dagli attacchi e dalle compromissioni mediante file XML e avvisi.

4.5 Protezione da software dannosi (art. 12 cpv. 1 lett. a OCIP)

4.5.1 Le comunità devono pianificare l'applicazione periodica di misure volte a proteggere dai software dannosi e verificarne periodicamente l'esecuzione effettiva. In particolare devono:

a. adottare misure per proteggere da software dannosi in particolare gli elementi degni di protezione dell'infrastruttura informatica indicati al numero 4.6.2 lettere a-i e k-l. Le misure devono consentire soprattutto di riconoscere tempestivamente ed eliminare tali software;

b. verificare periodicamente i software impiegati per individuare ed eliminare i software dannosi e garantirne l'aggiornamento.

4.6 Gestione dei mezzi informatici e delle raccolte di dati degni di protezione («inventario dell'infrastruttura informatica») (art. 12 cpv. 1 lett. b OCIP)

4.6.1 Le comunità devono garantire che tutti i dati, sistemi e dispositivi degni di protezione della cartella informatizzata del paziente vengano identificati in modo univoco, classificati, registrati in un «inventario dell'infrastruttura informatica» e mantenuti aggiornati.

4.6.2 Negli «inventari dell'infrastruttura informatica» si devono registrare e amministrare almeno i seguenti elementi dell'infrastruttura informatica della comunità per la cartella informatizzata del paziente:

a. i punti di accesso (attori IHE *Initiating Gateway, Responding Gateway*, *Initiating Imaging Gateway*, *Responding Imaging Gateway*);

b. gli archivi dei documenti (attore IHE *Document Repository*);

c. il registro dei documenti (attore IHE *Document Registry, Update Responder*);

d. i sistemi e i supporti di memoria per i dati verbalizzati (attori IHE *Audit Repository* e *Patient Audit Record Repository*);

e. i sistemi per l'amministrazione dei diritti (attori IHE *Policy Source, Policy Repository, Authorization Decision Provider, Authorization Decision Consumer)* e la comunicazione delle identità autenticate (*X-Assertion Provider, X-Service User, X-Service Provider*);

f. se presenti, i sistemi del servizio di ricerca di dati interno della comunità per le strutture sanitarie e i professionisti della salute (attori IHE *Provider Information Directory*, *Provider Information Source*, *Provider Information Consumer*);

g. il sistema di gestione delle identità e degli accessi (IAM);

h. l'indice dei pazienti (attori IHE *Patient Demographics Supplier, Patient Identifier Cross-reference Manager, Patient Identity Source*);

i. i portali di accesso per i professionisti della salute o i pazienti;

j. i sistemi primari collegati, a condizione che svolgano il ruolo di uno dei seguenti attori IHE o funzionalità analoghe: *Document Source, Document Consumer, Imaging Document Source, Imaging Document Consumer, Update Initiator, Provider Information Source, Provider Information Consumer, Patient Demographics Consumer, Patient Identifier Cross-reference Consumer, Patient Identity Source, X-Service User*;

k. i sistemi, le applicazioni e le raccolte di dati per l'esercizio del sistema, fra cui quelli per i dati verbalizzati, i backup e la gestione degli accessi per gli amministratori del sistema;

l. i sistemi realizzati da attori con funzioni amministrative (Document Administrator IHE, Policy Administrator);

m. i sistemi e i supporti di memoria utilizzati per convalidare gli attributi dell'identità rilevanti per la sicurezza forniti («claim») (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**a e **Fehler! Verweisquelle konnte nicht gefunden werden.**b);

n. i sistemi necessari per comunicare con la banca dati d'identificazione dell'UCC e i servizi di ricerca di dati della Confederazione.

4.6.3 Per tutti gli attori IHE nel ruolo di *Secure Node* secondo il numero 2.9.20, l'«inventario dell'infrastruttura informatica» deve inoltre comprendere almeno il certificato client per la sicurezza a livello di trasporto (certificato client TLS) del rispettivo attore IHE o del rispettivo elemento dell'infrastruttura informatica.

4.6.4 A ogni elemento dell'inventario deve essere attribuito un proprietario responsabile.

4.6.5 Il responsabile della protezione e della sicurezza dei dati deve verificare l'«inventario dell'infrastruttura informatica» almeno una volta all'anno.

4.7 Requisiti in materia di protezione e sicurezza dei dati per le strutture sanitarie affiliate e i loro professionisti della salute nonché per i loro terminali (art. 12 cpv. 1 lett. c OCIP)

4.7.1 Le comunità devono chiedere alle strutture sanitarie di impegnarsi a:

a. definire, applicare e verificare periodicamente i requisiti di protezione e sicurezza dei dati (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.** lett. **Fehler! Verweisquelle konnte nicht gefunden werden.**);

b. informare i professionisti della salute che accedono alla cartella informatizzata del paziente sui loro diritti e doveri nell'ambito del trattamento dei dati della cartella informatizzata del paziente e a rispettare le misure prescritte;

c. garantire una configurazione sicura dei terminali utilizzati dai professionisti della salute per accedere alla cartella informatizzata del paziente.

4.7.2 Le prescrizioni per la configurazione dei terminali devono comprendere almeno:

a. l'impiego di un software contro codici dannosi aggiornato periodicamente;

b. l'impiego di sistemi di protezione delle reti informatiche;

c. un aggiornamento periodico del sistema operativo e dei componenti critici del software;

d. una gestione restrittiva dei diritti di amministratore del sistema.

4.7.3 Le comunità devono garantire che i terminali con una configurazione considerata non sicura non possano trattare dati della cartella informatizzata del paziente.

4.8 Requisiti in materia di protezione e sicurezza dei dati per il personale tecnico o amministrativo (art. 12 cpv. 1 lett. c OCIP)

4.8.1 Per l'accesso e il trattamento dei dati della cartella informatizzata del paziente da parte del personale tecnico e amministrativo delle comunità esse devono emanare prescrizioni e adottare i provvedimenti tecnici e organizzativi necessari al loro rispetto.

4.8.2 Le comunità devono garantire che:

a. le persone che trattano dati o sistemi della cartella informatizzata del paziente siano sufficientemente competenti per i compiti previsti e possano assumere le loro responsabilità nonché provvedere con diligenza alla protezione e alla sicurezza dei dati;
b. l'utilizzo di dati di autenticazione segreti sia controllato mediante un processo di gestione formale e che vengano richiesti e siano noti requisiti a garanzia di un impiego sicuro (p. es. confidenzialità, lunghezza della password, validità);
c. le persone che potrebbero ottenere l'accesso ai dati della cartella informatizzata del paziente siano soggette al segreto professionale medico secondo l'articolo 321 CP o siano obbligate per contratto a mantenere il segreto professionale;
d. si definiscano, applichino e rispettino processi per la gestione del personale orientati a soddisfare i requisiti in materia di protezione e sicurezza dei dati;
e. si preveda una procedura ufficiale per avviare misure o sanzioni disciplinari contro i collaboratori che hanno violato le disposizioni sulla protezione e la sicurezza dei dati.

4.8.3 Le comunità devono:

a. tenere un elenco, vistato dal responsabile della protezione e della sicurezza dei dati della comunità, di tutti gli amministratori di elementi infrastrutturali rilevanti per la sicurezza, come sistemi, componenti di rete, applicazioni e banche dati, che possono accedere ai dati della cartella informatizzata del paziente o potrebbero consentire accessi abusivi;
b. garantire che queste persone siano accuratamente selezionate, godano di un'ottima reputazione e soddisfino requisiti di sicurezza chiaramente definiti;
c. verificare periodicamente l'adempimento dei requisiti di sicurezza.

4.8.4 Le comunità devono definire un processo per gestire le seguenti funzioni amministrative speciali:

a. funzioni per gestire la configurazione dei diritti nell'ambito dei processi di apertura e soppressione di cartelle informatizzate del paziente;
b. funzioni per distruggere dati della cartella informatizzata del paziente.

4.8.5 Le comunità devono garantire che il trattamento di dati della cartella informatizzata del paziente da parte di persone in una delle funzioni amministrative di cui al numero 4.8.4:

a. avvenga solo in singoli casi definiti, in cui l'accesso a dati medici o la configurazione dei diritti sono indispensabili per garantire la protezione dei dati o il buon funzionamento della cartella informatizzata del paziente.

4.9 Requisiti in materia di protezione e sicurezza dei dati per terzi (art. 12 cpv. 1 lett. c OCIP)

4.9.1 Le comunità devono tenere un elenco, vistato dal responsabile della protezione e della sicurezza dei dati della comunità, di tutti i fornitori e prestatori di servizi («terzi») che potrebbero eventualmente accedere ai dati della cartella informatizzata del paziente, elaborarli, memorizzarli, trasmetterli ad altri oppure fornire componenti di infrastrutture informatiche a tale scopo.

4.9.2 Con i terzi si devono stabilire formalmente e concordare in contratti di fornitura tutti i requisiti rilevanti in materia di protezione e sicurezza dei dati.

4.9.3 I contratti di fornitura devono stabilire in modo inequivocabile gli obblighi e le responsabilità per soddisfare i requisiti rilevanti in materia di protezione e sicurezza dei dati.

4.9.4 Essi devono comprendere almeno le seguenti disposizioni:

a. l'obbligo del fornitore di rispettare in qualsiasi momento i requisiti della comunità rilevanti per la protezione e la sicurezza dei dati nell'impiego o nella fornitura di mezzi informatici, personale o servizi;
b. i requisiti e le procedure per la gestione degli incidenti di protezione e sicurezza dei dati;
c. l'indicazione di persone di contatto per domande e in caso di eventi nel settore della protezione e della sicurezza dei dati;
d. il diritto di verificare periodicamente, nell'ambito del contratto, i processi dei fornitori e le misure di controllo;
e. la trasmissione dell'obbligo di rispettare i requisiti della comunità in materia di protezione e sicurezza dei dati lungo tutta la catena di fornitura, nel caso in cui i fornitori diano incarichi in subappalto;
f. le prescrizioni e le misure di controllo per i subappalti;
g. l'obbligo di informare la comunità di ogni modifica nei rapporti contrattuali con i subappaltatori interessati.

4.10 Controllo e verifica dei servizi (art. 12 cpv. 1 lett. c OCIP)

I servizi, i rapporti e le registrazioni forniti da terzi e da eventuali subappaltatori devono essere controllati e verificati periodicamente dalle comunità in modo da garantire che:

a. le condizioni stabilite contrattualmente in materia di protezione e sicurezza dei dati vengano rispettate (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**);
b. gli incidenti di protezione e sicurezza dei dati vengano gestiti in modo adeguato;
c. le modifiche dei servizi siano soggette a una gestione delle modifiche controllata.

4.11 Responsabile della protezione e della sicurezza dei dati (art. 12 cpv. 2 OCIP)

4.11.1 Le comunità devono designare un responsabile della protezione e della sicurezza dei dati incaricato di amministrare il loro sistema di gestione della protezione e della sicurezza dei dati e devono definire il suo mansionario.

4.11.2 Il responsabile della protezione e della sicurezza dei dati deve:

a. controllare il rispetto delle prescrizioni in materia di protezione e sicurezza dei dati da parte della comunità, delle strutture sanitarie affiliate nonché di terzi (cfr. n. 4.1);
b. poter esercitare la sua funzione in modo tecnicamente indipendente;
c. disporre delle competenze e risorse tecniche necessarie all'adempimento dei suoi compiti;
d. garantire la comunicazione ai decisori responsabili e ad altri servizi che devono essere informati.

4.12 Gestione delle chiavi crittografiche (art. 9 cpv. 4)

Le comunità devono garantire che:

a. siano applicate procedure sicure secondo lo stato della tecnica per la creazione, la distribuzione, l'attivazione, l'aggiornamento, la revoca o la disattivazione e la cancellazione di chiavi crittografiche;
b. le chiavi crittografiche impiegate siano protette contro smarrimenti o modifiche;
c. le chiavi segrete e private siano protette da abusi e divulgazioni;
d. i dispositivi per la creazione, memorizzazione e archiviazione di chiavi siano protetti in modo adeguato.

4.13 Sicurezza di esercizio (art. 12 cpv. 4 OCIP)

4.13.1 Le comunità devono garantire che:

a. gli accessi con diritti speciali all'ambiente di produzione (p. es. da parte di amministratori del sistema operativo, della rete, della banca dati e delle applicazioni) richiedano un'autenticazione forte a 2 fattori, siano controllati e verbalizzati e non consentano esportazioni abusive, in particolare di dati appartenenti ai pazienti;
b. gli accessi dall'esterno della rete locale (accessi remoti) all'ambiente di produzione da parte di terzi e subappaltatori e in particolare gli accessi esterni privilegiati con diritti speciali siano impediti oppure adeguatamente protetti, controllati e verbalizzati nonché attivati solo a tempo determinato e se necessario;
c. le attività di sviluppo, test e messa in funzione di nuovi sistemi nel loro ambiente siano documentate in modo rintracciabile e avvengano in base a un processo controllato;
d. vengano effettuati backup completi e che i dati ivi contenuti siano criptati;
e. i backup siano memorizzati in modo da essere protetti contro modifiche abusive o inosservate;
f. le procedure per il ripristino del sistema siano sufficientemente documentate e testate periodicamente;
g. i log tecnici siano accessibili solo per le persone autorizzate;
h. i file di log rechino la marca temporale e siano memorizzati in modo da essere protetti contro modifiche abusive o inosservate;
i. i supporti di dati con informazioni sui pazienti vegano sempre smaltiti o distrutti correttamente in modo che i dati ivi contenuti diventino illeggibili e non possano più essere ripristinati;

j. gli orologi del sistema siano sincronizzati con l'ora ufficiale in Svizzera;
k. sia garantita una rigorosa separazione dei compiti («segregation of duties») per le attività e i processi che presentano una criticità particolarmente elevata per la protezione e la sicurezza dei dati.

4.13.2 Le comunità devono garantire che l'ambiente di produzione dell'infrastruttura informatica interna alla comunità utilizzato per la cartella informatizzata del paziente sia:
a. isolato da altri ambienti (p. es. ambiente di sviluppo, collaudo e test);
b. dotato di nuovi software esclusivamente nel quadro di processi controllati;
c. controllato periodicamente e attivamente in particolare mediante cosiddetti test di penetrazione per individuare eventuali lacune di sicurezza;
d. liberato dalle lacune di sicurezza individuate mediante un processo di patch management controllato.

4.13.3 Oltre agli eventi risultanti dal trattamento dei dati della cartella informatizzata del paziente da parte di professionisti della salute e pazienti secondo il numero 2.10.2, si devono registrare almeno i seguenti eventi verificatisi durante l'esercizio del sistema:
a. login e logout;
b. tentativi riusciti e respinti di accedere al sistema;
c. tentativi riusciti e respinti di accedere ai dati;
d. modifiche nella configurazione del sistema;
e. impiego di diritti di accesso speciali privilegiati;
f. indirizzi e protocolli di rete;
g. attivazione e disattivazione di sistemi di protezione o autenticazione;
h. modifica di diritti di accesso e di amministrazione del sistema;
i. creazione, modifica o cancellazione di account utente;
j. copia di dati classificati degni di protezione.

4.14 Acquisto, sviluppo e manutenzione dei sistemi (art. 12 cpv. 4 OCIP)

4.14.1 Le comunità devono garantire la protezione e la sicurezza dei dati durante l'intero ciclo di vita dei sistemi della cartella informatizzata del paziente. A tal scopo devono definire i processi per la documentazione, il disegno, la specificazione, i test, il controllo della qualità e l'applicazione controllata in caso di:
a. introduzione o sviluppo di nuovi sistemi;
b. notevoli modifiche o sviluppi di sistemi già esistenti;
c. cambiamento di piattaforma operativa.

4.14.2 Si deve almeno provare che in ogni ciclo di sviluppo:
a. siano stati definiti i requisiti di sicurezza già durante la progettazione e si sia effettuata un'analisi strutturata a riguardo prima di assegnare eventuali incarichi di sviluppo o procedere a estensioni di sistemi informatici esistenti;
b. le modifiche dei sistemi siano soggette a procedure formali e documentate di controllo delle modifiche;
c. l'accesso al codice sorgente del proprio software sia controllato e verbalizzato;

d. esistano direttive per uno sviluppo sicuro, anche in caso di esternalizzazione delle attività di sviluppo di sistemi, ed esse siano applicate e attuate nel ciclo di sviluppo;

e. negli ambienti di test non si trovino dati produttivi, soprattutto dati particolarmente degni di protezione;

f. lo sviluppo esternalizzato di software sia sottoposto alla vigilanza e al controllo dell'organizzazione di gestione;

g. sia elaborato e applicato un piano di test, che garantisca la verifica di tutti i requisiti, funzionali e non, prima della messa in funzione;

h. i risultati del test attesi e ottenuti siano documentati in modo rintracciabile;

i. la messa in funzione nell'ambiente di sistema produttivo avvenga solo dopo che i test sono stati completati con esito positivo oppure che i test senza esito positivo siano stati valutati e accettati quali rischio.

4.15 Sicurezza di comunicazione: gestione di reti e servizi di rete (art. 12 cpv. 4 OCIP)

4.15.1 Le comunità devono prevedere direttive per la sicurezza delle reti e stabilire le competenze per la gestione delle reti all'interno della comunità.

4.15.2 Le comunità devono garantire che, attraverso un adeguato design della rete e dei suoi componenti nonché attraverso una struttura e una configurazione adeguate dei servizi di rete, i dati della cartella informatizzata del paziente siano protetti nelle applicazioni e nei sistemi.

4.15.3 A tale scopo devono definire, rappresentare mediante progetti di rete e realizzare strutture di rete sicure, grazie alle quali si possa ottenere una separazione nelle reti tra gruppi di servizi d'informazione, utenti e sistemi informatici; in particolare devono configurare i firewall, i router, gli switch, ecc. e le realizzazioni tecnologiche per i servizi di rete in modo che:

a. alle interfacce tecniche dell'infrastruttura informatica interna a una comunità («services») possano collegarsi solo i sistemi che appartengono a una comunità certificata e soddisfano i requisiti applicabili (p. es. secondo i n. **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.** e **Fehler! Verweisquelle konnte nicht gefunden werden.**);

b. i sistemi che accedono a un servizio attraverso Internet si autentichino nei suoi confronti mediante sicurezza a livello di trasporto (TLS) con un certificato elettronico valido di un'autorità di certificazione affidabile (Certification Authority, CA) secondo lo stato della tecnica.

4.15.4 Le strutture di rete devono soddisfare i seguenti requisiti:

a. per i portali di accesso e i punti di accesso si utilizzano certificati TLS della classe 2 o superiore (secondo le classi di certificato PKI eCH-0048, versione 2.0 del 28 novembre 2018), per altri servizi certificati TLS almeno della classe 2 o certificati TLS validi solo all'interno della comunità;

b. tutti i servizi ai quali è possibile collegarsi attraverso Internet devono autenticare il sistema richiedente mediante TLS Client Authentication;

c. i punti di accesso rispondenti (Responding Gateways) o altri endpoint raggiungibili per la comunicazione intercomunitaria possono autorizzare il collegamento solo se il sistema richiedente appartiene a una comunità certificata ed è registrato nel servizio centrale di ricerca di dati delle comunità e comunità di riferimento secondo l'articolo 40 OCIP;

d. tutti i servizi interni alla comunità con i quali non è possibile collegarsi attraverso Internet possono autorizzare il collegamento solo se il sistema richiedente appartiene alla propria comunità certificata, è registrato nell'inventario della propria comunità ed è stato accettato dal responsabile della protezione e della sicurezza dei dati;

e. le procedure adottate devono essere documentate.

4.15.5 Le comunità devono:

a. separare a livello di tecnica di rete tutti i supporti di memoria delle comunità che contengono dati sul paziente della cartella informatizzata del paziente (fra cui gli elementi dell'«inventario della struttura informatica» secondo il n. 4.8) da tutti gli altri sistemi che hanno un livello di sicurezza inferiore;

b. documentare le procedure adottate a tale scopo.

4.15.6 Le comunità devono in particolare documentare le misure di sicurezza implementate per proteggere i portali di accesso. La documentazione comprende almeno:

a. la topologia della rete e il tipo di separazione della rete locale (LAN) da Internet;

b. le versioni e lo stato delle release dei software impiegati nel Web Application Firewall (WAF), nel (Reverse-)Proxy e nel web server, nonché le versioni delle componenti di software rilevanti per la sicurezza fornite da terzi;

c. le misure previste per il monitoraggio e la gestione degli attacchi e le lacune di sicurezza (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

4.16 Scadenza delle sessioni di rete («*session timeout*») (art. 12 cpv. 4 OCIP)

4.16.1 Le sessioni di rete inattive devono essere interrotte automaticamente dopo un periodo d'inattività definito dal responsabile della protezione e della sicurezza dei dati della comunità.

4.16.2 L'autenticazione sui portali di accesso e i terminali deve essere ripetuta prima del nuovo accesso se fino alla scadenza di un periodo predefinito non vi è più stata interazione dell'utente con la cartella informatizzata del paziente.

4.16.3 La gestione delle sessioni di rete (session management) per quanto riguarda l'autenticazione e l'autorizzazione sui portali di accesso o i terminali che accedono ai dati:

a. è di responsabilità dell'applicazione o del servizio web;

b. deve generare gli ID di sessione casualmente e proteggerli dalla perdita di riservatezza, autenticità e integrità mediante misure crittografiche adeguate e conformi allo stato attuale della tecnica;

c. deve sostituire eventuali ID di sessione dopo ogni accesso dell'utente;

d. deve offrire agli utenti la possibilità di interrompere espressamente una sessione in corso;

e. deve distruggere o annullare tutti i dati sulle sessioni di rete terminate.

4.17 Memorizzazione temporanea (art. 12 cpv. 4 OCIP)

Gli elementi dell'infrastruttura informatica interna alla comunità destinati alla trasmissione di dati medici della cartella informatizzata del paziente, segnatamente i punti di accesso, devono memorizzare tali dati solo per la durata della transazione e non in modo permanente.

4.18 Disponibilità (art. 12 cpv. 4 OCIP)

Le comunità devono garantire che:

a. i dati della cartella informatizzata del paziente siano disponibili;

b. i servizi tecnici e i sistemi per il trattamento e la protezione dei dati della cartella informatizzata del paziente siano sempre disponibili e protetti da interruzioni;

c. dopo un guasto si possa assicurare il ripristino del funzionamento del sistema;

d. i dati della cartella informatizzata del paziente siano protetti in ogni momento;

e. i servizi tecnici esposti dell'infrastruttura informatica siano dotati di una disponibilità definita per contratto di almeno il 98 per cento del tempo, anche in caso di carico eccezionale;

f. tutte le interfacce della cartella informatizzata del paziente accessibili da Internet siano protette dagli attacchi «*Denial of Service*» (DoS);

g. dispongano di processi collaudati con misure combinate di prevenzione e ripristino che consentano di ridurre a un livello accettabile i tempi di ripristino delle informazioni perse, per esempio in seguito a catastrofi naturali, incidenti, interruzioni delle applicazioni, del sistema e degli apparecchi oppure a danni intenzionali.

4.19 Supporti di memoria dei dati soggetti alla giurisdizione svizzera (art. 12 cpv. 5 OCIP)

La comunità deve garantire che:

a. i supporti di memoria dei dati della cartella informatizzata del paziente interni alla comunità (in particolare gli archivi dei dati, il registro dei dati, l'indice dei pazienti) siano gestiti da persone giuridiche soggette al diritto svizzero;

b. questi supporti di memoria dei dati si trovino in Svizzera.

5 Punto di contatto per i professionisti della salute (art. 13 OCIP)

5.1.1 Le comunità devono designare un punto di contatto per sostenere i professionisti della salute nell'impiego della cartella informatizzata del paziente.

5.1.2 Le comunità devono garantire almeno che:

a. i collaboratori del punto di contatto conoscano i loro diritti e doveri nonché i provvedimenti relativi alla protezione e sicurezza dei dati;

b. i collaboratori con accesso ai dati della cartella informatizzata del paziente siano selezionati con cura e siano soggetti al segreto professionale medico secondo l'articolo 321 CP o siano obbligati per contratto a mantenere il segreto professionale;

c. gli accessi dei collaboratori del punto di contatto ai terminali dei professionisti della salute avvengano esclusivamente previo consenso del professionista della salute interessato e siano documentati.

B. Condizioni supplementari per le comunità di riferimento

6 Informazione del paziente (art. 15 OCIP)

6.1 Informazione del paziente (art. 15 OCIP)

6.1.1 Il paziente deve essere informato su:

a. lo scopo della cartella informatizzata del paziente;
b. i principi fondamentali del trattamento dei dati;
c. l'ubicazione dei dati medici nei sistemi primari;
d. la memorizzazione e l'eventuale distruzione dei dati medici negli archivi dei documenti.

6.1.2 Il paziente deve in particolare essere informato sui seguenti punti:

a. che può revocare un presunto consenso secondo l'articolo 3 capoverso 2 LCIP a fornire dati medici in caso di cura;
b. che può nuovamente cancellare dati medici negli archivi dei documenti della cartella informatizzata del paziente;
c. di quali funzioni del portale di accesso per pazienti può disporre;
d. che può consultare i dati verbalizzati;
e. che può nominare un rappresentante;
f. che può stabilire di essere informato sull'adesione di professionisti della salute a gruppi ai quali ha concesso un diritto di accesso;
g. che può autorizzare i professionisti della salute della sua comunità di riferimento a trasferire i diritti di accesso ad altri professionisti della salute o a gruppi di professionisti della salute.

6.1.3 Il paziente deve essere informato delle conseguenze del consenso e della revoca, almeno su:

a. la volontarietà del consenso;
b. il fatto che si può tenere contemporaneamente una sola cartella per paziente;
c. le modalità di attribuzione e impiego del numero d'identificazione del paziente;
d. la possibilità di cambiare comunità di riferimento e le relative conseguenze per l'ubicazione dei dati e per eventuali rappresentanze e autorizzazioni a professionisti della salute;
e. la possibilità di revoca senza formalità e motivazione;
f. la soppressione, in caso di revoca, della cartella informatizzata del paziente e la cancellazione dei dati che vi sono contenuti;
g. la possibilità, anche dopo una revoca, di riaprire una cartella informatizzata del paziente, alla quale sarà attribuito un nuovo numero d'identificazione del paziente.

6.1.4 Il paziente deve essere informato sui gradi di riservatezza per i dati medici, almeno su:

a. la possibilità di attribuire in ogni momento ai dati medici della cartella informatizzata del paziente uno dei tre gradi di riservatezza;
b. il fatto che il grado di riservatezza attribuito automaticamente ai nuovi dati medici configurati è «normalmente accessibile»;
c. la possibilità per i professionisti della salute di attribuire ai nuovi dati medici configurati il grado di riservatezza «limitatamente accessibile»;
d. la possibilità di stabilire quale grado di riservatezza attribuire ai nuovi dati medici configurati e sul fatto che l'attribuzione scelta rimane successivamente valida (prevalenza sulle lettere b e c).

6.1.5 Il paziente deve essere informato su come attribuire i diritti di accesso, almeno sulla possibilità:

a. di negare l'accesso a singoli professionisti della salute (elenco delle esclusioni);
b. di negare l'accesso ai professionisti della salute attribuendo ai dati medici il grado di riservatezza «segreto»;
c. di concedere ai professionisti della salute e a gruppi di professionisti della salute il diritto di accesso al grado di riservatezza «normalmente accessibile» oppure ai gradi di riservatezza «normalmente accessibile» e «limitatamente accessibile»;
d. di modificare, limitare a una scadenza prestabilita o revocare tali diritti di accesso;
e. che anche gli ausiliari registrati dei professionisti della salute possono accedere ai dati mediante il diritto di accesso del relativo professionista della salute responsabile;
f. che nelle situazioni di emergenza i professionisti della salute accedano ai dati «normalmente accessibili»;
g. di estendere l'accesso nelle situazioni di emergenza medica al grado di «limitatamente accessibile» o di negarlo completamente;
h. di essere informato in caso di avvenuto accesso di emergenza.

6.1.6 Il paziente deve essere informato sulle misure consigliate per la protezione e la sicurezza dei dati, almeno su:

a. i rischi residui e le possibili misure preventive;
b. l'autenticazione sicura e l'uso di strumenti d'identificazione e di dati di accesso segreti;
c. le misure per un impiego sicuro dei terminali;
d. le raccomandazioni di comportamento per contrastare tentativi di frode.

7 Consenso (art. 16 OCIP)

7.1 Creazione di una cartella informatizzata del paziente

7.1.1 Per la creazione di una cartella informatizzata del paziente è necessaria la firma autografa del paziente.

8 Gestione (art. 17 OCIP)

8.1 Apertura, gestione e soppressione della cartella informatizzata del paziente (art. 17 cpv. 1 lett. a OCIP)

Le comunità di riferimento definiscono i processi per l'apertura, la gestione e la soppressione della cartella informatizzata del paziente.

8.2 Identificazione dei pazienti (art. 17 cpv. 1 lett. b e d OCIP)

8.2.1 Per l'identificazione dei pazienti si devono stabilire processi, i quali devono garantire che:

a. il paziente venga identificato mediante un apposito strumento rilasciato da un emittente certificato o secondo i requisiti dell'articolo 24 capoverso 1 OCIP;
b. il paziente non sia già in possesso di una cartella informatizzata del paziente;
c. il paziente sia iscritto nell'indice dei pazienti della comunità di riferimento;
d. il numero d'identificazione del paziente sia richiesto secondo le prescrizioni degli articoli 6 e 7 OCIP e che venga collegato correttamente alla cartella informatizzata del paziente da creare;
e. i dati demografici del paziente siano ripresi dalla banca dati d'identificazione dell'UCC e inseriti nell'indice dei pazienti della comunità di riferimento.

8.3 Identificazione e autenticazione per l'accesso (art. 17 cpv. 1 lett. c OCIP)

8.3.1 Per accedere alla loro cartella informatizzata, i pazienti devono autenticarsi mediante uno strumento d'identificazione valido, rilasciato da un emittente certificato secondo l'articolo 31 OCIP.

8.4 Rappresentanza (art. 17 cpv. 1 lett. c OCIP)

8.4.1 Il rappresentante di cui al numero 8.6.3 lettera f deve accedere alla cartella informatizzata del paziente rappresentato mediante uno strumento d'identificazione proprio rilasciato da un emittente certificato secondo l'articolo 31 OCIP.

8.4.2 La comunità di riferimento deve garantire che:

a. il rappresentante venga identificato mediante uno strumento d'identificazione proprio rilasciato da un emittente certificato o secondo l'articolo 31 OCIP o secondo l'articolo 24 capoverso 1 OCIP;
b. il rappresentante sia informato sui principi fondamentali del trattamento dei dati nonché sulle possibilità, i diritti e i doveri in materia di impiego della cartella informatizzata del paziente;
c. l'identificatore univoco secondo l'articolo 25 capoverso 1 OCIP del rappresentante sia collegato correttamente;
d. l'accesso del rappresentante alla cartella informatizzata del paziente sia consentito solo per la durata della rappresentanza.

8.5 Cambiamento di comunità di riferimento (art. 17 cpv. 1 lett. e OCIP)

8.5.1 Si deve stabilire un processo per il cambiamento di comunità di riferimento da parte di un paziente.

8.5.2 Il processo di cambiamento di comunità di riferimento deve garantire che:

a. la configurazione individuale dell'amministrazione dei diritti sia distrutta;
b. l'autorizzazione dei professionisti della salute secondo l'articolo 4 lettera g OCIP sia soppressa;
c. la possibilità di accesso del rappresentante del paziente sia soppressa.

8.6 Amministrazione dei diritti (art. 17 cpv. 2 OCIP)

8.6.1 I pazienti devono avere la possibilità di accordare, modificare e revocare i diritti di accesso dei professionisti della salute e dei gruppi di professionisti della salute, fermo restando che devono essere rispettate le prescrizioni degli articoli 2 e 3 OCIP.

8.6.2 Le comunità di riferimento devono garantire che la configurazione dell'amministrazione dei diritti possa essere elaborata solo secondo la volontà del paziente.

8.6.3 Le comunità di riferimento devono garantire che i pazienti possano avvalersi delle opzioni di cui all'articolo 4 OCIP. A tal scopo devono permettere al paziente di:

a. stabilire quale grado di riservatezza debba essere attribuito ai nuovi dati medici configurati;
b. negare a singoli professionisti della salute l'accesso alla sua cartella informatizzata;
c. essere informato sull'adesione di professionisti della salute ai gruppi aventi diritto di accesso;
d. fissare a sua discrezione una scadenza per i diritti di accesso accordati ai professionisti della salute;
e. estendere o negare l'accesso di emergenza;
f. nominare un rappresentante;
g. autorizzare i professionisti della salute a trasferire i diritti di accesso loro accordati ad altri professionisti della salute o a gruppi di professionisti della salute.

9 Portale di accesso per i pazienti (art. 18 OCIP)

9.1 Attuazione dell'amministrazione dei diritti (art. 18 lett. a OCIP)

Il portale di accesso deve:

a. offrire ai pazienti la possibilità di amministrare i diritti nel rispetto delle prescrizioni degli articoli da 1 a 4 OCIP;
b. indicare quali professionisti della salute dispongono di quali diritti;
c. indicare la composizione dei gruppi di professionisti della salute.

9.1*a* Affidabilità dei portali di accesso

9.1*a*.1 Previa approvazione del responsabile della protezione e della sicurezza dei dati, per le informazioni rilevanti ai fini dei diritti pubblicate dai portali di accesso è possibile rinunciare alla verifica di cui al numero 2.9.7a.

9.2 Presentazione (art. 18 lett. a OCIP)

9.2.1 La presentazione sull'interfaccia utente del portale di accesso deve essere corretta e completa e indicare chiaramente:

a. se i dati medici sono stati forniti da un professionista della salute o dal paziente stesso;
b. quali dati medici sono stati annullati;
c. quali versioni dei dati medici sono disponibili;
d. quali dati medici sono stati attribuiti a quale grado di riservatezza.

9.2.2 Il paziente deve poter riconoscere in ogni momento se tratta dati della cartella informatizzata del paziente.

9.2*a* Marchio di certificazione

9.2*a*.1 Il portale di accesso alla cartella informatizzata del paziente deve essere contrassegnato con uno dei seguenti due marchi di certificazione:

9.2*a*.2 Il marchio deve essere riprodotto a colori.

9.2*a*.3 Le comunità certificate non possono utilizzare il marchio di certificazione in un modo o in un contesto che possa indurre in inganno.

9.3 Presentazione dei dati verbalizzati (art. 18 lett. b OCIP)

I pazienti devono avere la possibilità di consultare in una forma per loro leggibile i dati verbalizzati concernenti la loro cartella informatizzata da tutte le comunità e comunità di riferimento.

9.4 Registrazione e consultazione dei dati (art. 18 cpv. c OCIP)

9.4.1 Il portale di accesso deve offrire al paziente la possibilità di:

a. escludere i dati registrati dai professionisti della salute dalla distruzione di cui all'articolo 10 capoverso 1 lettera d;

b. distruggere nella cartella informatizzata del paziente determinati dati medici che lo riguardano.

9.4.2 In materia di tipi di media, il portale di accesso interno deve soddisfare gli stessi requisiti del portale di accesso interno per professionisti della salute di cui al numero 3.3.

9.4.3 Per i dati che vengono registrati dal paziente stesso, il portale di accesso deve soddisfare almeno i seguenti presupposti:

a. i dati da esso forniti al di fuori della cartella informatizzata del paziente possono essere registrati nella cartella informatizzata del paziente solo previo consenso del paziente;

b. i dati forniti dal paziente stesso devono poter essere registrati nella cartella informatizzata del paziente sempre direttamente, ossia senza impiego di supporti di memoria intermedi.

9.5 Assenza di barriere (art. 18 lett. d OCIP)

Il portale di accesso deve soddisfare gli stessi requisiti del portale di accesso per professionisti della salute di cui al numero 0.

9.6 Requisiti tecnici

9.6.1 Oltre ai requisiti in materia di protezione e sicurezza dei dati di cui al numero 4, il portale di accesso deve:

a. effettuare una verifica attiva mediante test di penetrazione per individuare eventuali lacune di sicurezza almeno dopo ogni modifica rilevante per la sicurezza dei mezzi informatici del portale di accesso;

b. essere concepito in modo da escludere l'accesso al funzionamento interno e manipolazioni abusive.

9.6.2 Il portale di accesso deve essere protetto dalle forme note di attacco e compromissione.

9.6.3 L'autenticazione mediante il portale di accesso è disciplinata conformemente all'allegato 8 OCIP-DFI.

10 Dati registrati dai pazienti (art. 19 OCIP)

10.1 Archivi dei documenti per i dati medici dei pazienti

10.1.1 Le comunità di riferimento devono mettere a disposizione degli archivi dedicati interni alla comunità per i dati medici registrati dai pazienti stessi.

10.1.2 I dati medici non devono sottostare ad alcuna scadenza per la cancellazione.

10.1.3 Lo spazio di archiviazione deve essere sufficientemente grande.

10.2 Memorizzazione offline di dati medici e metadati

10.2.1 I pazienti devono avere la possibilità di scaricare i dati dalla loro cartella informatizzata del paziente in un formato elettronico interoperabile diffuso o di procurarseli in altro modo (cfr. n. 2.9.16).

10.2.2 I dati messi nuovamente a disposizione nella cartella informatizzata del paziente devono essere contrassegnati quali dati registrati dal paziente (cfr. n. **Fehler! Verweisquelle konnte nicht gefunden werden.** lett. **Fehler! Verweisquelle konnte nicht gefunden werden.**), a meno che non sia possibile garantire mediante procedure adeguate che i dati siano rimasti intatti dall'ottenimento secondo il numero **Fehler! Verweisquelle konnte nicht gefunden werden.**.

11 Punto di contatto per i pazienti (art. 20 OCIP)

11.1.1 Le comunità di riferimento devono designare un punto di contatto per sostenere i pazienti nell'impiego della cartella informatizzata del paziente.

11.1.2 Le comunità di riferimento devono garantire almeno che:

a. i collaboratori conoscano i loro diritti e doveri nonché i rischi e i provvedimenti relativi alla protezione e alla sicurezza dei dati;
b. i collaboratori con accesso ai dati della cartella informatizzata del paziente siano selezionati con cura e siano soggetti al segreto professionale medico secondo l'articolo 321 CP o siano obbligati per contratto a mantenere il segreto professionale;
c. i collaboratori del punto di contatto possano accedere ai terminali dei pazienti esclusivamente previo consenso del paziente e che gli accessi siano documentati.

12 Soppressione della cartella informatizzata del paziente (art. 21 OCIP)

12.1 Processo per la soppressione della cartella informatizzata del paziente (art. 21 OCIP)

Le comunità di riferimento devono prevedere dei processi per la soppressione della cartella informatizzata del paziente.

12.2 Revoca del consenso alla tenuta di una cartella informatizzata del paziente (art. 21 cpv. 1 OCIP)

12.2.1 Le comunità di riferimento devono garantire che la cartella informatizzata del paziente venga tempestivamente soppressa quando il paziente revoca il suo consenso.

12.2.2 Il processo di soppressione della cartella informatizzata del paziente in seguito a una revoca deve garantire che:

a. la persona revocante venga identificata mediante uno strumento di identificazione rilasciato da un emittente certificato e sia informata delle conseguenze della revoca;
b. la revoca sia documentata con validità giuridica;
c. la dichiarazione di revoca venga conservata per 10 anni.

12.3 Soppressione dopo il decesso del paziente (art. 21 cpv. 2 OCIP)

Le comunità di riferimento devono garantire che la cartella informatizzata del paziente possa essere soppressa non prima di due anni dal decesso del paziente.

12.4 Soppressione della cartella informatizzata del paziente (art. 21 cpv. 3 OCIP)

Il processo di soppressione della cartella informatizzata del paziente deve garantire che:

a. la cartella informatizzata del paziente da sopprimere venga identificata correttamente;
b. tutti i diritti di accesso alla relativa cartella del paziente vengano immediatamente annullati;
c. tutti i dati della relativa cartella del paziente vengano distrutti secondo il numero 2.6 lettera b e che il numero d'identificazione del paziente venga eliminato da tutti i sistemi;
d. tutte le comunità e comunità di riferimento vengano informate entro un termine adeguato della soppressione della cartella informatizzata del paziente;
e. l'UCC venga informato entro un termine adeguato della soppressione della cartella informatizzata del paziente.