Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI

Berna, 1° giugno 2023

Modifica dell'ordinanza del DFI sulla cartella informatizzata del paziente

Revisione annuale 2023 (allegati 2–5, inclusi i complementi 1 e 2.1–2.3 agli allegati 5, 8 e 9)

Rapporto esplicativo

BK-D-BF8A3401/507

1 Situazione iniziale

Il 19 giugno 2015, il Parlamento ha adottato la legge federale sulla cartella informatizzata del paziente (LCIP RS 816.1, FF 2015 3951) che disciplina in qualità di legge quadro le condizioni per il trattamento dei dati della cartella informatizzata del paziente (CIP).

Con decisione del 22 marzo 2017, il Consiglio federale ha posto in vigore la LCIP e il relativo diritto d'esecuzione dal 15 aprile 2017. L'ordinanza del 22 marzo 2017 sulla cartella informatizzata del paziente (OCIP, RS 816.11) delega al DFI determinate competenze di legiferare per definire i dettagli delle condizioni di certificazione per le comunità e le comunità di riferimento nonché per gli emittenti degli strumenti di identificazione.

2 Necessità di revisione

Con la presente revisione degli allegati 2, 3, 4, 5, 8 e 9 nonché dei complementi 1, 2.1, 2.2 e 2.3 all'allegato 5 dell'OCIP-DFI si intende precisare alcuni aspetti tecnici poco chiari o rettificare errori nelle prescrizioni che sono emersi nel quadro delle procedure di certificazione in corso o che sono stati rilevati da specialisti tecnici di fornitori di piattaforme e di sistemi primari.

2.1 Medication Card Document

La disponibilità e lo scambio di dati relativi ai trattamenti farmacologici sono – nel quadro della CIP – tra le informazioni più frequenti e importanti per tutti i pazienti e i professionisti della salute coinvolti. Attraverso la CIP, pazienti e professionisti della salute dovrebbero avere in qualsiasi momento accesso al trattamento farmacologico nello stato più aggiornato possibile. Inoltre, la mozione Stöckli 18.3512 «Diritto a un piano di trattamento farmacologico per una maggiore sicurezza dei pazienti» richiede di presentare al Parlamento una base giuridica che conferisca ai pazienti il diritto di ricevere in formato cartaceo o elettronico un piano di trattamento farmacologico in caso di assunzione parallela di almeno tre medicamenti.

Il Medication Card Document fornisce una panoramica il più possibile completa sull'attuale trattamento farmacologico del paziente e costituisce la base per un'anamnesi ottimale del trattamento farmacologico, oltre che per un controllo delle interazioni esaustivo. Grazie al Medication Card Document il paziente ha un quadro d'insieme di tempi e modalità di assunzione di ciascun medicamento, oltre che degli aspetti da osservare nell'assunzione.

2.2 Open ID Connect

Il protocollo Open ID Connect (OIDC) è uno standard moderno che permette la comunicazione tra diverse applicazioni e che risulta particolarmente adatto per consentire a un utente di accedere a diversi ulteriori sistemi di servizio a seguito di un'autenticazione unica su di un sistema centrale. La procedura, definita anche *Identity Federation* o *Single Sign-On (SSO)*, semplifica in modo significativo per l'utente l'utilizzo di un sistema, in quanto non occorre più gestire parametri di accesso individuali per ciascun sistema ed è sufficiente un unico accesso a un solo sistema.

L'OIDC offre quindi un'alternativa al già affermato Security Assertion Markup Language (SAML), che svolge le stesse funzioni del SAML a parità di livello di sicurezza, ma è attualmente più diffusa sul mercato. Segnatamente, l'integrazione dell'OIDC nei sistemi primari è più semplice rispetto a quella del SAML e quindi può indurre potenzialmente un maggior numero di fornitori di prestazioni a un'integrazione profonda nei propri sistemi primari.

Per garantire la sicurezza del traffico di dati nell'utilizzo dell'OIDC sono necessarie misure nell'attuazione del protocollo: tra queste, risultano importanti la firma crittografata di messaggi scambiati tra i sistemi partecipanti e la verifica della firma da parte del destinatario di tali messaggi. Queste misure sono state documentate nella presente versione dell'allegato 8.

L'implementazione dell'OIDC è onerosa. Pertanto, tenendo conto degli Identity Provider e in accordo con essi, nella presente versione la sua implementazione è classificata come opzionale.

3 Commento ai singoli articoli

3.1 Allegato 2: Condizioni tecniche e organizzative di certificazione delle comunità e delle comunità di riferimento

N. 2.3.2 Attuazione della decisione di accesso

Questo numero è stralciato. La verifica della correttezza delle decisioni di accesso è già sufficientemente coperta attraverso i requisiti dell'allegato 5 nei relativi profili tecnici e mediante SIAS e test dei casi di applicazione complessi.

N. 2.6 Distruzione di dati

Nella versione tedesca, è utilizzato il termine «Vernichtung» (distruzione) in luogo di «Löschen» (cancellazione). Tale modifica non ha alcun effetto sui requisiti, che restano invariati.

N. 2.9 Prescrizioni per la gestione e il trasferimento dei dati della cartella informatizzata del paziente

Diversi numeri in questo capitolo sono stati stralciati in quanto già sufficientemente coperti attraverso il rimando all'allegato 5 OCIP-DFI. Sono stati stralciati i seguenti numeri: 2.9.4, 2.9.5, 2.9.5*a*, 2.9.6, 2.9.7, 2.9.7*b*, 2.9.7*c*, 2.9.8, 2.9.9, 2.9.10, 2.9.11, 2.9.12, 2.9.13, 2.9.13*a*, 2.9.14, 2.9.15, 2.9.16, 2.9.16*a*, 2.9.17, 2.9.18, 2.9.19, 2.9.19*a*, 2.9.20, 2.9.21, 2.9.22, 2.9.23, 2.9.24, 2.9.25, 2.9.27 e 2.9.28.

N. 2.9.3 *Profili d'integrazione IHE, adeguamenti nazionali dei profili d'integrazione IHE e profili d'integrazione nazionali*

Ora, nell'allegato 5 OCIP-DFI si fa espressamente riferimento anche agli attori e alle transazioni, oltre che ai profili.

N. 2.9.7a *Comunicazione di identità autenticate*

Il numero è stralciato in quanto i requisiti sono inseriti nell'allegato 5 complemento 1.

N. 2.9.26a *Autenticazione con certificati validi*

Si parla unicamente di punti di accesso e non più di endpoint. Tale modifica non ha alcun effetto sui requisiti, che restano invariati.

N. 2.10 *Dati verbalizzati*

Per maggiore chiarezza si dichiara espressamente che i dati verbalizzati qui descritti corrispondono alla verbalizzazione secondo i profili ATNA e CH:ATC secondo l'allegato 5 dell'OCIP-DFI. In passato non era del tutto chiaro se ciò valesse anche per i log di sistema.

N. 2.10.5 *Dati verbalizzati*

Il numero è stralciato in quanto nell'allegato 5 è indicata l'esatta entità della verbalizzazione.

N. 2.10.7 *Dati verbalizzati*

Nella *lettera a* è stato chiarito che si tratta di dati verbalizzati secondo il profilo CH:ATC. Nella *lettera e* si utilizza l'espressione «utenti amministrativi» in luogo di «amministratori del sistema». Il nuovo termine include oltre agli amministratori del sistema anche tutti gli altri utenti che svolgono lavori amministrativi per una comunità.

N. 3.1b *Affidabilità dei portali di accesso*

Questo disciplinamento derogatorio è eliminato poiché sinora non è mai stato attuato da nessuna comunità. Le informazioni rilevanti ai fini dei diritti devono pertanto essere sempre verificate da una fonte affidabile. Questo rafforza la sicurezza dell'infrastruttura CIP.

N. 3.4.2 *Requisiti tecnici*

Questo numero è stralciato e i requisiti sono ora inseriti nel numero 4.4.3 lettera d.

N. 4.2.1 *Sistema di gestione della protezione e della sicurezza dei dati*

Il riferimento alla norma ISO/IEC 27002, Tecnologie Informatiche – Tecniche di sicurezza – Codice di pratica per la gestione della sicurezza delle informazioni è aggiornato dalla versione 2017-06 alla versione 2022.

N. 4.4.3 *Gestione di vulnerabilità informatiche*

La *lettera c* è riformulata in modo che non menzioni un solo scenario di attacco specifico, bensì tutti i tipi di attacco e di compromissione correnti. Insieme alla nuova *lettera d* comprende ora anche i numeri stralciati 3.4.2, 4.18 lettera f e 9.6.2.

N. 4.6.2 *Gestione dei mezzi informatici e delle raccolte di dati degni di protezione*

Si rinuncia a elencare i relativi attori IHE. Tale modifica non ha alcun effetto sui requisiti, che restano invariati.

N. 4.6.5 *Gestione dei mezzi informatici e delle raccolte di dati degni di protezione*

Si precisa che in fase di verifica l'«inventario dell'infrastruttura informatica» deve essere anche aggiornato.

N. 4.7.1 *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*

Si richiede ora che le comunità e le comunità di riferimento richiedano alle strutture sanitarie di obbligarsi per scritto a rispettare i requisiti di protezione e sicurezza dei dati.

N. 4.18 *Disponibilità*

Con la *lettera* a^{bis} si introduce un nuovo requisito secondo il quale i dati devono essere disponibili anche nel caso in cui una comunità cessi la sua attività. La nuova *lettera* a^{ter} richiede che, in caso di migrazione di dati, i metadati e in particolare il ruolo del fornitore siano mantenuti. La *lettera f* è stralciata e il requisito è ora inserito nel numero 4.4.3 lettera d.

N. 8.2.1 *Identificazione dei pazienti*

Le prescrizioni del numero 8.2.1 della precedente versione dell'allegato 2 sono inserite nei numeri 8.2.1–8.2.1*b*. Il numero 8.2.1 contiene ora esclusivamente le possibilità di identificazione di persone che desiderano aprire una CIP in virtù dell'articolo 17 capoverso 1 lettera b OCIP. Inoltre nella *lettera a* il rimando all'articolo 24 OCIP è eliminato e sostituito da un elenco esplicito degli strumenti d'identificazione riconosciuti nel processo per l'apertura di una CIP.

Dal punto di vista materiale, i requisiti relativi all'identificazione sono stati ampliati di due fattispecie. Secondo la *lettera d* sono ora riconosciuti per l'identificazione anche i passaporti svizzeri e le carte d'identità svizzere non più in corso di validità, se integrati con ulteriori documenti o mediante la dichiarazione dell'identificazione da parte di familiari o di un'autorità. Il passaporto o la carta d'identità scaduti in combinazione con ulteriori documenti o con la dichiarazione devono permettere un'identificazione affidabile. Possono essere considerati ulteriori documenti per esempio la tessera dell'assicurazione malattie, un permesso di domicilio e le carte bancarie. Le comunità di riferimento restano competenti per la definizione dei dettagli e del processo di identificazione delle persone. Rientra in questa competenza in particolare anche la definizione dei tipi di ulteriori documenti da richiedere per effettuare un'identificazione sicura. Con questa modifica si vuole soprattutto semplificare l'apertura di una CIP per le persone che hanno difficoltà ad accedere a un documento valido (per esempio per le persone costrette a letto nelle case di cura e per anziani).

Secondo la *lettera m* è ora possibile aprire una CIP con una carta d'identità straniera, se questa autorizza all'entrata in Svizzera e se il titolare può dimostrare alla comunità di riferimento che vive in comunione domestica con una persona titolare di una carta di legittimazione secondo l'articolo 17 dell'ordinanza sullo stato ospite.

N. 8.2.1a *Identificazione dei pazienti (bambini fino al 12° anno d'età)*

Con il numero 8.2.1*a* si introduce una regolamentazione speciale per l'identificazione dei bambini fino al compimento del 12° anno d'età. Sulla base di questa disposizione si può effettuare l'identificazione dei bambini per mezzo della tessera d'assicurato di un'assicurazione malattie svizzera in combinazione con l'atto di nascita o altri documenti idonei per l'identificazione. La disposizione è stata volutamente formulata in maniera aperta affinché le comunità di riferimento, analogamente all'identificazione con un passaporto svizzero o una carta d'identità svizzera scaduti, possa definire autonomamente i requisiti specifici e soddisfare così le esigenze emerse nella prassi.

N. 8.2.1b *Identificazione dei pazienti (altri processi)*

Nel numero 8.2.1*b* sono disciplinati gli altri requisiti per il processo d'identificazione contenuti in precedenza nel numero 8.2.1 lettere b–e.

N. 8.6.3 *Amministrazione dei diritti*

Nella *lettera c* si precisa che l'informazione sull'adesione di professionisti della salute ai gruppi aventi diritto di accesso deve avvenire solo su richiesta dei pazienti.

N. 9.1a *Affidabilità dei portali di accesso*

Questo disciplinamento derogatorio è eliminato poiché sinora non è mai stato attuato da nessuna comunità. Le informazioni rilevanti ai fini dei diritti devono pertanto essere sempre verificate da una fonte affidabile. Questo rafforza la sicurezza.

N. 9.6.2 *Requisiti tecnici*

Questo numero è stralciato e i requisiti sono ora inseriti nel numero 4.4.3 lettera d.

3.2 Allegato 3: Metadati per lo scambio di dati medici

N. 1.1 *Abbinamento degli attributi dei metadati secondo l'allegato 3 agli attributi dei metadati dei profili d'integrazione secondo l'allegato 5*

La denominazione dell'attributo dei metadati «Specializzazione dell'autore» è adattata all'IHE IT Infrastructure Handbook versione 2.1.

N. 2.2 *Specializzazione dell'autore*

La modifica al numero 1.1 (v. sopra) richiede anche una modifica del numero 2.2. Sono stati inoltre precisati alcuni termini e corrette le maiuscole e minuscole.

N. 2.3 *Tipo organizzativo della struttura sanitaria*

È stata aggiunta una nuova struttura sanitaria: Free-standing birthing center (environment).

N. 2.4 *Specializzazione della struttura sanitaria*

Sono state aggiunte quattro nuove specializzazioni: Obstetrics (qualifier value), Vascular surgery (qualifier value), Emergency medicine (qualifier value) e Dentistry (qualifier value).

N. 2.6 *Tipo di documento*

È stato aggiunto un nuovo tipo di documento: Digital representation of specimen (record artifact). Inoltre sono stati corretti diversi errori di ortografia.

N. 2.7 *Tipi di documenti consentiti in base alla relativa classe*

La modifica secondo il numero 2.6 è ripresa in questo numero per la mappatura del tipo di documento in base alla relativa classe. Inoltre sono stati corretti diversi errori di ortografia.

N. 2.12 *Formato tecnico dettagliato*

È stato aggiunto un nuovo formato tecnico per il Medication Card Document: CH EMED Medication Card document.

3.3 Allegato 4: Formati di scambio

N. 3 *Informazioni amministrative*

Nel numero 3 la versione di CH Core è modificata da 2.1.0 a 3.0.0. Le modifiche contengono adeguamenti tecnici dello standard, tra cui per esempio la verifica del numero GLN, la cui lunghezza può essere al massimo di 13 cifre. Sono state inoltre apportate modifiche alla specifica per renderla meglio leggibile.

N. 4 *Formato di scambio Cartella di vaccinazione informatizzata (CH VACD)*

Nel numero 4 la versione del formato di scambio CH VACD è modificata da 2.1.0 a 3.0.0. Con la nuova versione sono state apportate modifiche tecniche al formato di scambio.

La versione dei value set è portata da 2.1.0 a 3.0.0. Le modifiche riguardano l'aggiunta di vaccinazioni come per esempio Mpox e la correzione di errori ortografici.

N. 5 *Formato di scambio Cartella farmacologica informatizzata (CH EMED)*

Il formato di scambio Cartella farmacologica informatizzata permette la registrazione, gestione e rappresentazione dei dati di trattamento farmacologico di un paziente. L'attuazione tecnica deve avvenire secondo la specifica dettagliata CH EMED (n. 5) per documenti FHIR. In un primo momento si introduce il documento piano farmacologico (n. 5.1) del formato di scambio Cartella farmacologica informatizzata. Per il piano farmacologico sono definiti i metadati da assegnare tassativamente (n. 5.1.1). I metadati permettono tra l'altro il riconoscimento dei documenti.

3.4 Allegato 5: Profili d'integrazione

L'OCIP-DFI specifica nell'allegato 5 quali profili d'integrazione devono essere utilizzati nel contesto della CIP. Nel complemento 1 all'allegato 5 sono descritti gli adeguamenti nazionali ai profili IHE standard. Il complemento 2.1 contiene i profili d'integrazione nazionali CH:ADR e CH:PPQ, nel complemento 2.2 sono riportati i profili d'integrazione nazionali CH:ATC mentre il profilo d'integrazione nazionale CH:CPI è specificato nel complemento 2.3. Queste prescrizioni devono essere adeguate allo stato della tecnica.

3.4.1 Allegato 5 (parte pubblicata ufficialmente)

N. 1 e 2 *Profili d'integrazione IHE e profili d'integrazione nazionali*

Il 10 marzo 2022 è stata pubblicata la revisione 20.0 dell'IHE Radiology Technical Framework e il 17 giugno 2022 la revisione 19 dell'IHE IT Infrastructure Technical Framework. Nella nuova versione si trovano nuovi profili nonché richieste di adeguamenti (Change Proposals) da noi presentate rilevanti per la CIP e concernenti il Restricted Metadata Update (RMU) e la Healthcare Provider Directory (HPD).

Nelle tabelle dei profili d'integrazione dell'allegato 5 (n. 1 e n. 2), così come nel complemento 1 all'allegato 5 i riferimenti sono stati modificati in base ai summenzionati IHE Technical Frameworks.

3.4.2 Complemento 1 all'allegato 5: Adeguamenti nazionali dei profili d'integrazione secondo l'articolo 5 capoverso 1 lettera b OCIP-DFI

N. 1.3 *Requirements on XDS-I.b*

Il collegamento di archivi di immagini radiologiche alla CIP è previsto da quando è entrata in vigore la LCIP nel 2017. L'ordinanza è stata precisata affinché gli accessi agli studi DICOM negli archivi radiologici degli ospedali siano effettuati correttamente attraverso l'infrastruttura della CIP, impedendo gli abusi. In particolare sarà consentito solo all'utente tecnico di mettere a disposizione oggetti DICOM Key Object Selection (KOS) nella CIP. In questo modo si impedisce che pazienti e professionisti della salute archivino nella CIP oggetti KOS manipolati e ottengano così l'accesso non autorizzato agli studi di altri pazienti. In pratica, tuttavia, questo rischio non si è mai concretizzato, in quanto finora non esistono collegamenti di sistemi di archivi di immagini radiologiche.

N. 1.5.1 Precisions on Authenticate Node [ITI-19]

Con la nuova versione dell'IHE ITI Technical Framework (cfr. capitolo 3.4.1), nella transazione Authenticate Node [ITI-19] sono presenti più opzioni in relazione alla versione TLS. È precisato che deve essere utilizzata almeno la versione TLS 1.2 (STX: TLS 1.2 floor using BCP195 Option). A tal fine sono stati aggiunti i numeri 1.5.1 e 1.5.2.

N. 1.6.2 Actors / Transactions

Gli attori IHE sono componenti software che comunicano tra di loro attraverso interfacce standardizzate (transazioni). Secondo la convenzione IHE, gli attori possono essere raggruppati. In tal caso, devono essere implementate sempre tutte le transazioni degli attori raggruppati. I raggruppamenti esistenti hanno portato all'obbligo di implementare transazioni inutili. Con la presente modifica è stato ridefinito il raggruppamento degli attori, il che corrisponde a un adeguamento alla realtà.

N. 1.6.3 Actor Grouping

La modifica nel numero 1.6.2 (v. sopra) richiede anche la modifica del numero 1.6.3: nella tabella 7 sono stati aggiunti i corretti raggruppamenti degli attori.

N. 1.6.4 Transactions

Nell'edizione 3 dell'allegato 8 OCIP-DFI, è stato sancito a livello normativo in aggiunta a SAML anche lo standard OpenID Connect per rendere possibile il collegamento di dispositivi mobili alla CIP attraverso interfacce mobili.

Affinché OpenID Connect funzioni anche per le comunità (di riferimento) e i sistemi primari è stato aggiunto come opzione per il profilo XUA (sottonumero del numero 1.6.4).

N. 1.6.4.3.4.2 Message Semantics

Nelle prescrizioni relative alla transazione Provide X-User Assertion nel profilo XUA (necessaria per esempio per la ricerca di documenti per determinare i diritti di accesso) sono state corrette le prescrizioni di strutturazione degli attributi di «organization» e «organization-id». Questa precisazione ha lo scopo di impedire implementazioni errate e promuove pertanto l'interoperabilità.

N. 1.11.5.1.2 Attribute

Le prescrizioni svizzere relative al profilo Health-Provider-Directory (HPD) sono state precisate affinché nel «prefix» la comunità (di riferimento) sia la Assigning Authority e possa essere utilizzato complessivamente solo una volta il segno dei due punti per non violare la norma ISO 21091. Inoltre nell'HPD per il campo UID sono ora consentiti solo i seguenti caratteri: caratteri alfanumerici, segno meno «-», due punti «:», punto esclamativo «!», barra verticale «|», trattino basso «_», punto «.». Sinora la presenza di caratteri non ammessi poteva causare problemi, per esempio il fatto di non trovare una voce HPD in una ricerca.

N. 1.14 Requirements on Medication Card document

I numeri 1.13 e 1.14 contengono la descrizione degli attori IHE necessari per la visualizzazione e la validazione del Medication Card document. A questo scopo gli attori IHE Content Consumer e Content Creator sono stati inseriti nel complemento 1 all'allegato 5 OCIP-DFI.

3.4.3 Complemento 2.1 all'allegato 5: Profili d'integrazione nazionale secondo l'articolo 5 capoverso 1 lettera c OCIP-DFI – Authorization Decision Request (CH:ADR) and Privacy Policy Query (CH:PPQ)

Questo complemento specifica le prescrizioni tecniche relative al controllo delle autorizzazioni della CIP. Le prescrizioni si sono evolute nel tempo e sono state completamente rielaborate e corrette sulla base delle conoscenze via via raccolte nella prassi e ora dichiarate vincolanti. Tale sviluppo avrà effetti positivi sulla sicurezza e la protezione dei dati. In particolare, le prescrizioni nel complemento sono state ridotte all'essenziale e gli esempi di codice sono stati tolti dal documento. Inoltre gli schemi XML per la definizione dei diritti di accesso alla CIP sono stati ulteriormente sviluppati e l'obbligo di utilizzarli è ora sancito a livello normativo. Contestualmente è stato sviluppato anche uno schema di verifica a cui si fa riferimento nell'allegato (n. 4.1). Con l'introduzione di queste prescrizioni si vuole impedire che nella concessione o nella modifica di diritti di accesso siano forniti dati non consentiti.

Inoltre sono precisate le disposizioni dettagliate relative al collegamento di archivi di immagini all'infrastruttura CIP di una comunità (di riferimento). In questo modo si garantisce che solo gli utenti CIP autorizzati possano consentire l'accesso ai contenuti dagli archivi di immagini attraverso la CIP. In particolare sarà consentito solo all'utente tecnico di mettere a disposizione oggetti DICOM Key Object Selection (KOS) nella CIP. In questo modo si impedisce che pazienti e professionisti della salute archivino nella CIP oggetti KOS manipolati e ottengano così l'accesso non autorizzato agli studi di altri pazienti.

Infine sono state apportate numerose piccole modifiche, per esempio per eliminare complessità inutili dal sistema o per rendere possibile una migliore gestione degli errori. La seguente tabella di corrispondenze fornisce una panoramica della nuova struttura del complemento 2.1 all'allegato 5.

Capitolo	**Numero nell'edizione 4**	**Corrispondenza nell'edizione 5**
Introduction	1	1
Definitions of terms	1.1	-
EPR circle of trust	1.1.1	-
Patient Identifiers (EPR-SPID, MPI-PID)	1.1.2	-
Terminology	1.1.3	-
Volume 1 – Integration Profiles	2	2
Overview	2.1	-
Authorization Decision Request (CH:ADR)	2.2	2.1
Motivation	2.2.1	-
Objectives and Constraints	2.2.2	-
Actors / Transactions	2.2.3	-
Privacy Policy Query (CH:PPQ)	2.3	2.2
Motivation	2.3.1	-
Objectives and Constraints	2.3.2	-
Actors / Transactions	2.3.3	-
Volume 2 – Transactions	3	3
Denominazione (precedente): Authorization Decision Request (CH:ADR) *Denominazione (nuova):* Authorization Decision Request [CH:ADR]	3.1	3.1
Scope	3.1.1	3.1.1
Referenced Standards	3.1.2	3.1.2
Nuovo capitolo: XML Namespaces	-	3.1.3
Interaction Diagram	3.1.3	3.1.4
Descrizione (precedente): XACMLAuthzDecisionQuery Request *Descrizione (nuova):* CH:ADR Request	3.1.4	3.1.5
Trigger Events	3.1.5	
Message Semantics	3.1.6	-
Expected Actions	3.1.7	-
Denominazione (precedente): XACMLAuthzDecision Response *Denominazione (nuova):* CH:ADR Response	3.1.8	3.1.6
Nuovo capitolo: Indirect decision queries	-	3.1.7
Trigger Events	3.1.9	-
Message Semantics	3.1.10	-
Expected Actions	3.1.11	-
Enforcement of XDS Retrieve Document Set transactions	3.1.12	-
Enforcement of XDS-I.b "Imaging Retrieve" transactions	3.1.13	-
Security Considerations	3.1.14	3.1.8
Authorization Decision Consumer Audit Message	3.1.15	-
Authorization Decision Provider Audit Message	3.1.16	-
Cross-Community Authorization Decision Request (CH:XADR)	3.2	-
Denominazione (precedente): Privacy Policy Feed (PPQ-1) *Denominazione (nuova):* Privacy Policy Feed [PPQ-1]	3.3	3.2
Scope	3.3.1	3.2.1
Use Case Roles	3.3.2	-
Referenced Standards	3.3.3	3.2.2
Nuovo capitolo: XML Namespaces	-	3.2.3
Interaction Diagrams	3.3.4	3.2.4
Message Semantics	3.3.5	-
Denominazione (precedente): EPR AddPolicyRequest and EPR UpdatePolicyRequest *Denominazione (nuova):* AddPolicyRequest and UpdatePolicyRequest	3.3.6	3.2.5
Denominazione (precedente): EPR AddPolicyRequest Response and EPR UpdatePolicyRequest Response *Denominazione (nuova):* AddPolicyRequest Response and UpdatePolicyRequest Response	3.3.7	3.2.6

Capitolo	Numero nell'edizione 4	Corrispondenza nell'edizione 5
Denominazione (precedente): EPR DeletePolicyRequest *Denominazione (nuova):* DeletePolicyRequest	3.3.8	3.2.7
Denominazione (precedente): EPR DeletePolicyRequest Response *Denominazione (nuova):* DeletePolicyRequest Response	3.3.9	3.2.8
Security Considerations	3.3.10	3.2.9
Denominazione (precedente): Privacy Policy Retrieve (PPQ-2) *Denominazione (nuova):* Privacy Policy Retrieve [PPQ-2]	3.4	3.3
Scope	3.4.1	3.3.1
Use Case Roles	3.4.2	-
Referenced Standards	3.4.3	3.3.2
Nuovo capitolo: XML Namespaces	-	3.3.3
Interaction Diagrams	3.4.4	3.3.4
Denominazione (precedente): XACMLPolicyQuery *Denominazione (nuova):* Policy Query Request	3.4.5	3.3.5
Denominazione (precedente): XACMLPolicyQuery Response *Denominazione (nuova):* Policy Query Response	3.4.6	3.3.6
Security Considerations	3.4.7	3.3.7
Volume 3 – Content Profiles	4	4
XACML EPR Access Policies	4.1	-
EPR Access Policy Stack	4.2	-
Entry Policies for the Evaluation of Access Decisions	4.2.1	-
Access Constraints	4.3	-
Read and Write Access Rights Overview	4.4	-
Enforcement of EPR transactions	4.4.1	-
Read EPR	4.4.2	-
Write EPR	4.4.3	-
Detailed Privacy Policy Format definitions	4.4.4	-
Value-Sets	4.4.5	-
Nuovo capitolo: Submission Rules for Policies and Policy Sets	-	4.1
Nuovo capitolo: Base Policies and Base Policy Sets	-	4.1.1
Nuovo capitolo: Patient Bootstrap Policy Sets and Patient User Assignment Policy Sets	-	4.1.2
Figures	5	5
Tables	6	6
Listings	7	-

3.4.4 Complemento 2.2 all'allegato 5: Profili d'integrazione nazionali secondo l'articolo 5 capoverso 1 lettera c OCIP-DFI – Audit Trail Consumption (CH:ATC)

Il profilo CH:ATC utilizzato per i dati verbalizzati nel portale per i pazienti è portato da *Fast Healthcare Interoperability Resources* (FHIR) STU3 a FHIR Release 4. Dato che i futuri formati di scambio saranno pubblicati anche su FHIR Release 4, mantenere una vecchia versione renderebbe inutilmente complesso il sistema e obbligherebbe a supportare due versioni. La modifica si ripercuote sull'intero documento.

N. 1.1 Definitions of terms

Il numero 1.1 è stralciato in quanto è identico ai numeri corrispondenti nel complemento 1 all'allegato 5.

N. 3.1.4 Security Considerations

Nell'attuale revisione 2.1 dell'IHE IUA Supplement l'attributo «Tipo di token» nell'HTTP Header «Authorization» è cambiato ed è stato trasposto nel CH:ATC Profile: nell'i HTTP Header «Authorization» come tipo di token è indicato «Bearer» e non più «IHE-SAML». Questa modifica serve all'adeguamento agli standard internazionali e non comporta alcuna variazione del livello di sicurezza.

N. 4.1 Audit Trail Consumption Event Types

La ricerca di documenti in una CIP è registrata nei dati verbalizzati tecnici (ATNA) ma non visualizzata nei dati verbalizzati nel portale per i pazienti. Per migliorare la tracciabilità, con questa modifica anche la ricerca di documenti è visualizzata

nei dati verbalizzati nel portale per i pazienti. In questo modo, anche un accesso di emergenza senza successiva ricerca di documenti è visualizzato in modo chiaro nei dati verbalizzati nel portale per i pazienti.

L'articolo 9 capoverso 2 lettera f OCIP stabilisce che le comunità devono informare i pazienti che lo richiedono sull'ingresso di professionisti della salute in gruppi di professionisti della salute. Per una più semplice tracciabilità, le comunità desiderano che questi eventi siano salvati in aggiunta nei dati verbalizzati nel portale per i pazienti. A questo scopo sono stati aggiunti i numeri 4.5 e 4.5.1 contenenti specifiche tecniche ed esempi.

N. 4.2 Document Audit Event Content Profile

Nella ricerca o nell'elaborazione di documenti o dei loro metadati, d'ora in poi nell'ATC-Log sarà visualizzato anche il titolo oltre all'ID, poco indicativo.

N. 4.2.1 Example of a Document Audit Event: Document upload

Nell'esempio nel numero 4.2.1 relativo alla voce ATC-Log è stato aggiunto il titolo del relativo documento.

3.4.5 Complemento 2.3 all'allegato 5: Profili d'integrazione nazionali secondo l'articolo 5 capoverso 1 lettera c OCIP-DFI – Community Portal Index (CH:CPI)

N. 1.1 Definitions of terms

Il numero 1.1 è stralciato in quanto è identico ai numeri corrispondenti nel complemento 1 all'allegato 5.

N. 3.1.4.2 Message Semantics

I provider della piattaforma CIP hanno richiesto che tutte le informazioni necessarie possano essere lette dal CH:CPI affinché una comunità certificata possa collegarsi automaticamente con tutte le altre comunità certificate nel CH:CPI attraverso tutti i gateway. Il modello di dati del CH:CPI è stato ampliato con il *CH:ATC Patient Audit Consumer*, un'informazione rilevante che finora mancava. Di conseguenza, ora i certificati non devono più essere scambiati al di fuori dell'area riservata. Questa modifica, che migliora la sicurezza, interessa anche i numeri 3.1.5.2.3, 4.1.3.2 e 4.1.3.3.9 contenenti la specifica tecnica. Sono inoltre stati corretti errori di ortografia.

N. 3.1.8 Security Considerations

Con la nuova versione dell'IHE ITI Technical Framework (cfr. capitolo 3.4.1), nella transazione Authenticate Node [ITI-19] sono presenti più opzioni in relazione alla versione TLS. È precisato che deve essere utilizzata almeno la versione TLS 1.2 (STX: TLS 1.2 floor using BCP195 Option).

3.5 Allegato 8: Condizioni tecniche e organizzative di certificazione poste agli strumenti d'identificazione e ai loro emittenti (profilo di protezione per strumenti d'identificazione)

L'allegato 8 è stato rielaborato come segue in due fasi.

Per prima cosa è stata modificata la sua struttura. Questo si è reso necessario in quanto nell'allegato 8 edizione 2.1 non sarebbe stato possibile, o lo sarebbe stato solo con un onere sproporzionato, implementare le modifiche e gli ampliamenti necessari per tenere conto del feedback dell'organismo di certificazione e dei fornitori d'identità nonché per la prevista aggiunta di Open ID Connect. In questa prima fase non sono state apportate modifiche al contenuto dell'allegato 8. È stata modificata la struttura dei capitoli e sono stati eliminati incoerenze e punti poco chiari.

In seguito alla modifica della struttura, l'allegato 8 è suddiviso come segue.

1. Introduzione
2. Requisiti relativi al servizio rivolto agli utenti (pazienti, professionisti della salute e loro ausiliari)
3. Requisiti relativi all'attività operativa del fornitore d'identità
4. Requisiti tecnici relativi all'interfaccia e ai verbali.

Tutte le modifiche relative alla nuova struttura e all'eliminazione di incoerenze o punti poco chiari sono state presentate e discusse in un gruppo di accompagnamento temporaneo (gruppo di lavoro sugli strumenti d'identificazione a cui partecipano rappresentanti di comunità, piattaforme, dell'organismo di certificazione e dei fornitori d'identità). Le modifiche alla struttura e l'eliminazione di incoerenze o punti poco chiari sono state infine valutate, accolte favorevolmente e supportate dal gruppo di accompagnamento. La seguente tabella di corrispondenze fornisce una panoramica della nuova struttura dell'allegato 8.

Capitolo	Numero nell'edizione 2.1	Corrispondenza nell'edizione 3
PP Reference	1	3
TOE Definition	1.2.1	3.1.1
Operational Environment	1.3	3.1.1
Physical Protection of the TOE	1.4	3.1.3
Assets	1.5	3.1.4
External Entities and Subjects	1.6	3.1.5
Conformance Claims	2	obsoleto
Security Problem Definition	3	3.2
Assumptions	3.1	3.2.1
Organizational Security Policies	3.2	3.2.2
Threats	3.3	3.2.3
Security Objectives	4	3.3
Security Objectives for the TOE	4.1	3.3.1
Security Objectives for the operational environment	4.2	3.3.2
Security Objectives rationale	4.3	3.3.3
Countering the threats	4.3.2	3.3.3.1
Security Requirements	5	3.4
Overview	5.1	3.4.1
Security Functional Requirements for the TOE	5.2	3.4.2
Security Requirements rationale	5.3	3.4.3
Security Assurance Requirements Rationale	5.4	3.5
Appendix	6	5
Identity Proofing Requirements	**6.1**	**2.5**
Authentication Sequences (v2), SAML2.0 Binding (v3)	6.2	4.1
SAML Assertion Renewal	Tab. 12	4.1.1.2
Logout Sequence	6.2a	v.1.1.3
SAML Recommendations (v2), Protocol Requirements (v3)	6.3	4.1.2/.3
Open ID Connect	**n/a**	**4.2**
Protocol Requirements for Open ID Connect (v3)	**n/a**	**4.2.2**
WS Trust Recommendations	6.4	4.1.3.6, 4.1.3.7

Nella seconda fase di rielaborazione sono stati precisati o aggiunti i seguenti requisiti.

1. Armonizzazione dei requisiti relativi ai certificati X.509 di sistemi Relying Party (ovvero portali e sistemi primari) per l'autenticazione e la codifica sul Transport Layer TLS con le Condizioni tecniche e organizzative di certificazione delle comunità e delle comunità di riferimento (allegato 2 dell'OCIP-DFI).
2. Precisazione dei requisiti relativi ai certificati X.509 impiegati per la firma digitale dello scambio di messaggi tra fornitori d'identità e Relying Parties (portali e sistemi primari).
3. Per consentire l'integrazione di diversi fornitori di servizi (p. es. la pagina di registrazione per nuovi membri della comunità di riferimento o il portale d'accesso della CIP) all'interno di una comunità (di riferimento), è stato consentito l'impiego di NameID (*n. 4.1.3.5*) e Subject Identifier (*n. 4.2.3.5*) per i servizi che sottostanno all'autorità della comunità (di riferimento), a condizione che i fornitori di servizi impiegati siano elencati.

Per finire, con la presente modifica sono stati corretti elementi formali in diversi punti (uniformazione e integrazione di rimandi e indicazioni di fonti).

3.6 Allegato 9: Metadati per il servizio di ricerca di dati delle strutture sanitarie e dei professionisti della salute

N. 2.2 *Specializzazione del professionista della salute*

La correzione delle maiuscole e minuscole al numero 2.2 dell'allegato 3 OCIP-DFI richiede di modificare anche il numero 2.2.

Allegati

- Progetto dell'atto modificatore OCIP-DFI (RS *816.111*)
- Bozza dell'allegato 2 dell'OCIP-DFI, edizione 6
- Bozza dell'allegato 3 dell'OCIP-DFI, edizione 5
- Bozza dell'allegato 4 dell'OCIP-DFI, edizione 2
- Bozza dell'allegato 5 complemento 1 dell'OCIP-DFI, edizione 6
- Bozza dell'allegato 5 complemento 2.1 dell'OCIP-DFI, edizione 5
- Bozza dell'allegato 5 complemento 2.2 dell'OCIP-DFI, edizione 4
- Bozza dell'allegato 5 complemento 2.3 dell'OCIP-DFI, edizione 5
- Bozza dell'allegato 8 dell'OCIP-DFI, edizione 3
- Bozza dell'allegato 9 dell'OCIP-DFI, edizione 3
- Lettera d'accompagnamento