Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI

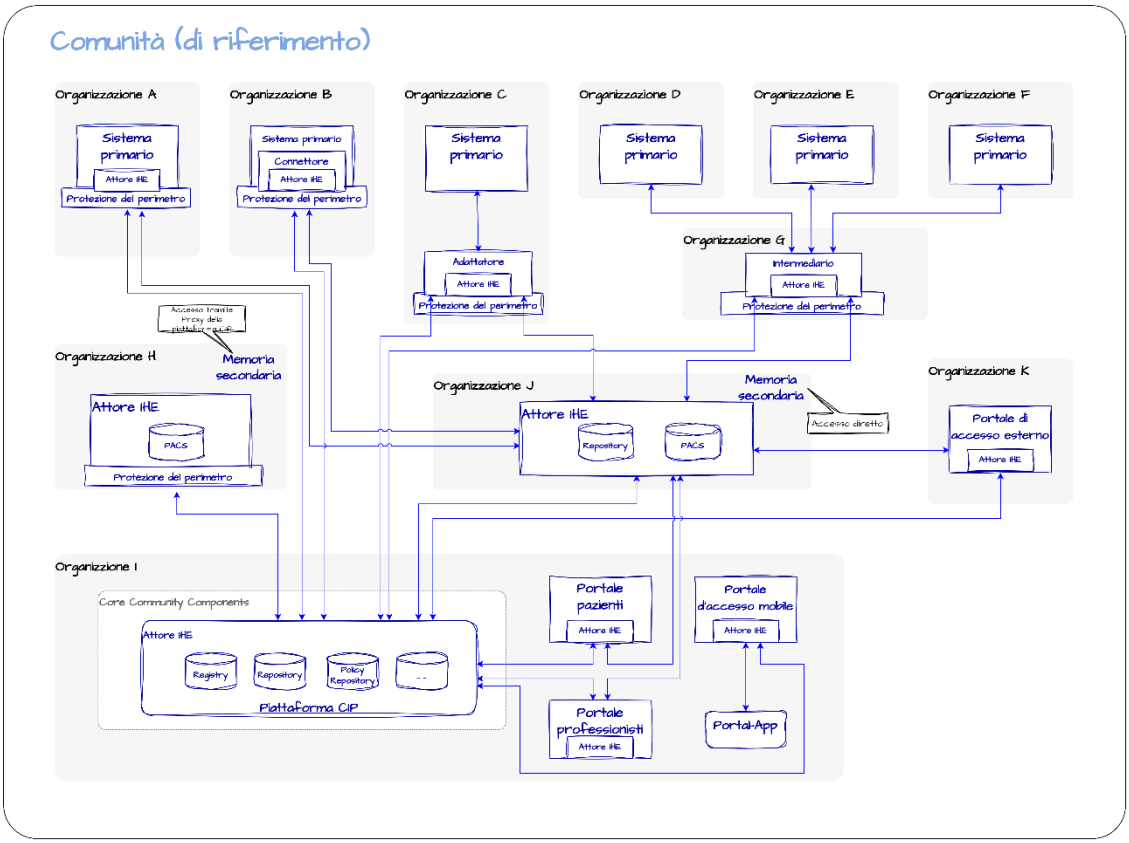
Ufficio federale della sanità pubblica UFSP
Divisione Trasformazione digitale

Scheda informativa

Data: 25.11.2024

Certificazione di sistemi esterni nel contesto della CIP

L'accettazione e la diffusione della cartella informatizzata del paziente (CIP) tra la popolazione e presso le strutture sanitarie e i professionisti della salute dipendono fondamentalmente dall'utilità della CIP e dalla fiducia della popolazione nella sua sicurezza. In linea di principio il collegamento di sistemi esterni dal valore aggiunto all'area riservata CIP[1] è pertanto desiderato, a condizione che il rispetto della protezione e della sicurezza dei dati, nonché l'interoperabilità con la CIP, siano garantiti. Svariati sistemi tecnici accedono alla CIP in modalità di lettura e/o scrittura e possono essere raffigurati nella seguente architettura dei sistemi:



[1] Nel contesto della presente scheda informativa, per «area riservata CIP» si intende la piattaforma CIP più le sue interfacce con i sistemi esterni. In altri contesti l'«area riservata CIP» indica la piattaforma CIP e tutti i sistemi collegati alla CIP. Quest'ultima definizione non è quella intesa nel presente documento.

Per maggiori informazioni:
La presente pubblicazione è disponibile anche in tedesco e francese.

Terminologia

Adattatore	Applicazioni che mettono a disposizione interfacce per la conversione dei protocolli da interfacce proprietarie a interfacce conformi con la CIP e che sono utilizzate dai sistemi primari per collegarsi alla CIP (collegamento 1:1 tra sistema primario e CIP).
Connettore	Librerie e componenti di software che mettono a disposizione funzioni predefinite per accedere alla CIP e che sono integrate nei prodotti (sistemi primari, adattatori, utenti tecnici, ecc.).
Intermediario	Applicazioni mediante le quali un numero qualunque di istituti può collegare i propri sistemi primari alla CIP per accedervi in modalità di lettura e scrittura (collegamento n:1 tra i sistemi primari e la CIP).
Memoria secondaria	Applicazioni gestite da istituti e in cui sono memorizzati dati della CIP.
Piattaforma CIP	Tutte le applicazioni o le componenti di applicazioni di cui necessita una comunità (di riferimento) per la gestione della CIP.
Portal-App	Client mobile dell'applicazione web, che comunica con il portale d'accesso mobile consentendo così l'accesso alla piattaforma CIP.
Portale d'accesso	Applicazioni gestite dalle comunità mediante le quali gli utenti CIP (p. es. professionisti della salute, pazienti) possono accedere alla CIP in modalità di lettura e scrittura.
Portale d'accesso esterno	Applicazioni gestite da terzi mediante le quali i pazienti possono accedere alla CIP in modalità di lettura.
Portale d'accesso mobile	Parte server di un'applicazione web gestita dalle comunità (di riferimento), che consente a una app che funge da portale (Portal-App) di accedere alla piattaforma CIP mediante interfacce conformi alla CIP.
Protezione del perimetro	Nel contesto della presente scheda informativa, con questo termine si intendono i seguenti sistemi di sicurezza: border access router (AR), web application firewall (WAF) con servizi proxy, sistemi di protezione antivirus, intrusion detection system (IDS), intrusion prevention system (IPS), zone demilitarizzate (DMZ).
Sistema primario	Sistema utilizzato in uno studio medico o in un ospedale per gestire dati medici, come per esempio il sistema informatico di uno studio medico o di una clinica.
Utente tecnico	Funzionalità all'interno di un sistema, che consente di caricare automaticamente documenti nella CIP.

Per maggiori informazioni:
La presente pubblicazione è disponibile anche in tedesco e francese.

Limite della certificazione

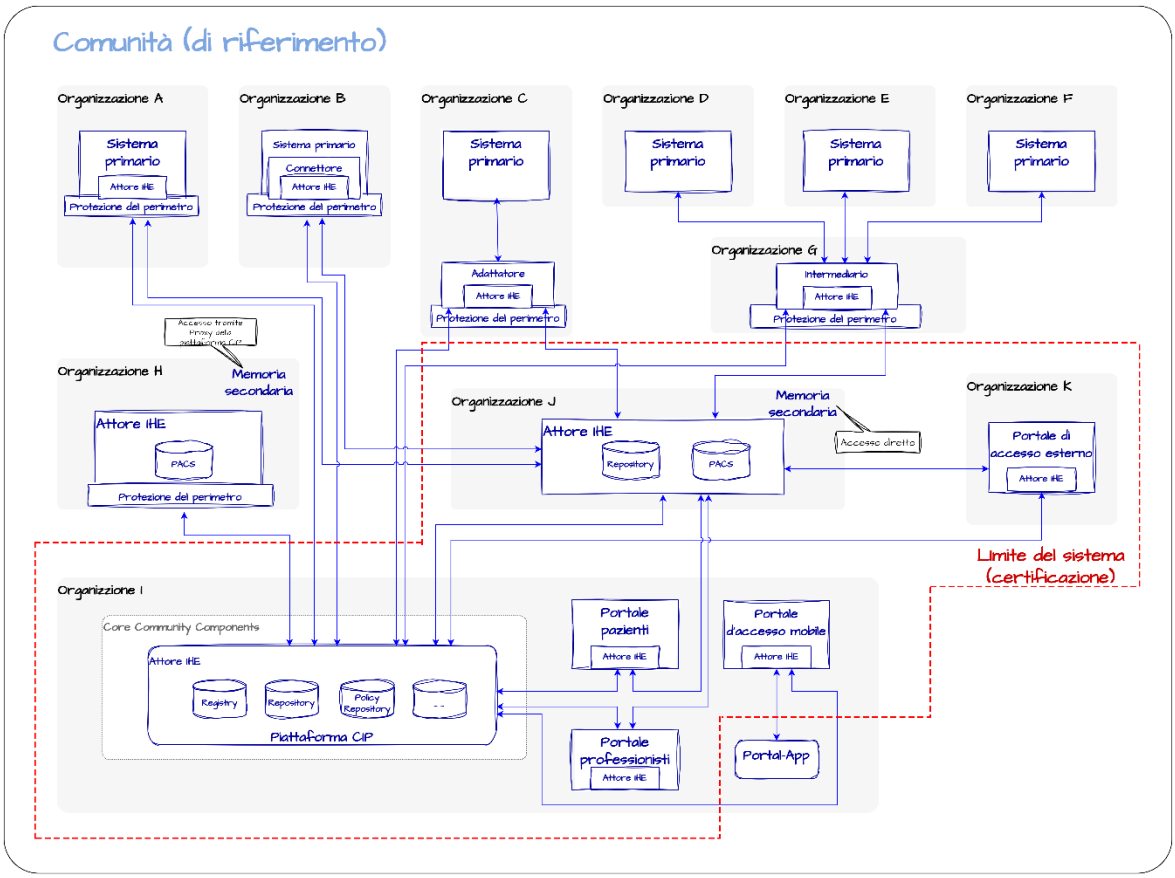
In seguito alla ponderazione dei rischi e dei benefici del collegamento dei sistemi esterni alla CIP, l'Ufficio federale della sanità pubblica (UFSP) ha deciso che, fino a nuovo avviso, i sistemi menzionati di seguito non sottostanno alla certificazione secondo la legge federale sulla cartella informatizzata del paziente (LCIP)[2,3]:

- sistema primario;
- connettore;
- adattatore;
- intermediario;
- memoria secondaria senza sistema di autorizzazione d'accesso integrato (accesso indiretto tramite proxy della piattaforma CIP);
- utente tecnico;
- Portal-App.

I seguenti sistemi delle comunità e delle comunità di riferimento continuano pertanto a sottostare alla certificazione:

- piattaforme CIP;
- portali d'accesso interni;
- portali d'accesso mobili;
- memoria secondaria con sistema di autorizzazione d'accesso integrato (accesso diretto);
- portali d'accesso esterni.

Il limite della certificazione corrisponde quindi al diagramma qui raffigurato:



[2] I sistemi che già ora sottostanno all'obbligo di certificazione ai sensi dell'allegato 2 dell'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI) non sono interessati da tale decisione.

[3] A seconda degli sviluppi in campo tecnologico, potrebbe essere necessario includere altri sistemi nell'allegato 2 dell'OCIP-DFI, assoggettandoli così all'obbligo di certificazione.

Per maggiori informazioni:
La presente pubblicazione è disponibile anche in tedesco e francese.

Per la valutazione dei rischi, l'UFSP parte dei seguenti presupposti:

- L'area riservata CIP è da considerare sicura secondo lo stato attuale della tecnica in virtù dei requisiti relativi alla protezione e alla sicurezza dei dati prescritti dalla legge.
- Il detentore di una CIP espone al rischio solo la propria CIP quando vi accede con una Portal-App. I dati di altre CIP non sono messi a rischio.
- Le strutture sanitarie e i professionisti della salute sono responsabili dei sistemi che utilizzano. Nel quadro del contratto per il collegamento alle comunità (di riferimento), queste ultime danno delle direttive alle strutture sanitarie in merito ai sistemi consentiti secondo le condizioni tecniche e organizzative di certificazione (CTO, Allegato 2 OCIP-DFI). Fornitori terzi che prestano servizi per strutture sanitarie o professionisti della salute agiscono sempre su incarico di una struttura o di un professionista, che sono sostanzialmente responsabili delle azioni degli incaricati.
- Tutti i fornitori dei sistemi menzionati agiscono responsabilmente e gestiscono la protezione e la sicurezza dei dati secondo lo stato attuale della tecnica (p. es. ISO/IEC 27001).
- Le comunità (di riferimento) impongono alle strutture sanitarie affiliate di applicare i requisiti relativi alla protezione e alla sicurezza dei dati dell'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI) a tutti i sistemi utilizzati per collegarsi alla CIP, come adattatori, intermediari o utenti tecnici.
- Nel caso di aspetti non disciplinati dalla LCIP, subentrano altri regolamenti come le disposizioni sulla protezione dei dati (a livello federale e cantonale), l'ordinanza relativa ai dispositivi medici (ODmed) e anche la legislazione in materia di diritto del lavoro.

Per maggiori informazioni:
La presente pubblicazione è disponibile anche in tedesco e francese.