Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Scheda informativa

CIP: le dieci principali misure di sicurezza

La protezione e la sicurezza dei dati rivestono un'importanza fondamentale per la cartella informatizzata del paziente (CIP). Le condizioni tecniche e organizzative di certificazione delle comunità e delle comunità di riferimento («CTO»; allegato 2 OCIP-DFI) contengono più di cento requisiti per la protezione e la sicurezza dei dati. La procedura formale di certificazione garantisce l'effettivo rispetto di questi requisiti.

La CIP è protetta dai più elevati standard di sicurezza, applicabili anche a livello giuridico grazie alla loro base legale. La presente scheda informativa descrive le dieci principali misure di sicurezza a livello dell'applicazione («A»), della tecnica («T») e dell'organizzazione («O»).

Misure di sicurezza a livello dell'**applicazione (A)**:

A1	Identificazione sicura e autenticazione a due fattori di tutti gli utenti
A2	I pazienti gestiscono da soli l'accesso alla loro CIP
A3	Ogni accesso a una CIP è verbalizzato
A4	I pazienti decidono liberamente per quanto tempo conservare i propri dati nella CIP

Misure di sicurezza a livello **tecnico (T)**:

T1	Individuazione delle anomalie e allarme automatico
T2	Conservazione criptata dei dati in Svizzera
T3	Comunicazioni sicure

Misure di sicurezza a livello **organizzativo (O)**:

O1	Gestione continua della sicurezza e obbligo di notifica nel caso di incidenti legati alla sicurezza
O2	Selezione e formazione degli utenti e del personale amministrativo
O3	Verifiche della sicurezza

Il presente elenco non è esaustivo. Dovrebbe tuttavia riuscire a illustrare i motivi per cui attualmente la CIP è una delle applicazioni più sicure in assoluto e lo sarà anche in futuro.

Ogni misura di sicurezza ha i propri limiti e ciò vale anche per la CIP. Pertanto, nella tabella seguente vengono descritti i pregi in termini di sicurezza delle dieci misure principali relative alla CIP, ma anche i loro limiti.

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Schwarzenburgstrasse 157
CH-3003 Berna

www.e-health-suisse.ch

Misure di sicurezza a livello dell’applicazione («A»)

A1	Identificazione sicura e autenticazione a due fattori di tutti gli utenti
Per accedere alla CIP, oltre a una password o a una caratteristica biometrica (fattore «conoscere» o «essere»), occorre possedere uno strumento di identificazione sicuro (fattore «avere»). Tale strumento deve corrispondere all'(elevato) livello di garanzia 3 della Norma ISO/IEC 29115:2013 ed essere emesso da un emittente certificato (detto anche *Identity Provider* o IdP).	
Sicurezza	La cosiddetta autenticazione a due fattori è una misura efficace contro il furto d’identità, poiché impedisce in particolare agli hacker di accedere alla CIP di un paziente tramite credenziali rubate.
Limiti	Gli utenti sono responsabili della conservazione sicura del loro strumento d’identificazione e devono quindi stare attenti a non lasciarsi convincere da e-mail di phishing a rivelare informazioni confidenziali (ad es. password) oppure a scaricare software dannosi.
Riferimenti	LCIP art. 7, OCIP art. 9, 17, 23 - 27 e 31, CTO n. 1.4, 1.6.2, 4.13.1 e 8.3

A2	I pazienti gestiscono personalmente l’accesso alla propria CIP
Prima di poter accedere a un documento contenuto nella CIP viene verificata l’esistenza del diritto d’accesso. Soltanto i pazienti hanno pieno accesso alla propria CIP. Solo loro possono decidere a quali professionisti della salute accordare il diritto d’accesso alla propria CIP, per quale grado di riservatezza dei documenti e se autorizzarli a trasferire il diritto d’accesso loro accordato ad altri professionisti della salute. Altri gruppi di persone (ad es. assicuratori malattia, ricercatori, autorità) non sono autorizzati ad accedere alla CIP. Se lo desiderano, i pazienti possono delegare i propri diritti (incluso il diritto a trasferirli) a uno o più rappresentanti (ad es. familiari). Per una descrizione dettagliata della concessione del diritto d’accesso si rimanda al sito della CIP all’indirizzo: https://www.patientendossier.ch/it/popolazione/informazioni/funzioni/accordare-i-diritti-daccesso.	
Sicurezza	Il sistema di controllo degli accessi alla CIP offre ai pazienti lo strumento dell’autodeterminazione informativa dei propri dati sanitari in essa contenuti. Il legislatore sostiene l’applicazione di tale diritto anche attraverso la comminazione ai sensi dell’articolo 24 LCIP di una multa cospicua in caso di accesso abusivo a una CIP.
Limiti	I professionisti della salute devono inserire nei propri sistemi i documenti consultati per il trattamento del paziente. Una volta scaricati, questi documenti escono dall’ambito del controllo degli accessi CIP e soggiacciono alle procedure interne stabilite dalla rispettiva struttura sanitaria (ospedale, studio medico ecc.). L’autodeterminazione in materia di comunicazione dei propri dati sanitari va di pari passo con una maggiore responsabilità personale. Nell’accordare i diritti d’accesso alla propria CIP i pazienti devono infatti prestare la massima attenzione e poter fare affidamento sui propri rappresentanti.
Riferimenti	LCIP art. 9 e 24, OCIP art. 1 - 4, CTO n. 2.1 - 2.3

A3	**Ogni accesso a una CIP è verbalizzato**
Ogni accesso a un documento contenuto in una CIP è verbalizzato. Nel portale d'accesso per i pazienti, questi ultimi possono sempre vedere chi, in che momento ha consultato quale documento. I pazienti possono inoltre chiedere informazioni (ad es. via SMS) sugli accessi di emergenza o sulle modifiche intervenute nella composizione dei gruppi di professionisti della salute. I dati verbalizzati sono conservati per dieci anni e non possono essere distrutti (nemmeno dagli stessi pazienti).	
Sicurezza	La verbalizzazione dei dati nella CIP garantisce un elevato grado di tracciabilità ed esercita inoltre un effetto preventivo e dissuasivo, in quanto ogni persona che accede ai dati di una CIP deve aspettarsi di dover dimostrare la legalità del suo agire.
Limiti	La verbalizzazione dei dati consente di individuare accessi abusivi e di perseguirli penalmente, anche se non permette di evitarli né di tornare indietro.
Riferimenti	LCIP art. 10, OCIP art. 9 e 18, CTO n. 2.10 e 9.3

A4	**I pazienti decidono liberamente per quanto tempo conservare i propri dati nella CIP**
Se il paziente non ha previsto diversamente, i dati della sua CIP sono distrutti automaticamente dopo 20 anni. Il paziente può comunque cancellare personalmente i dati della sua CIP o escluderli dalla distruzione automatica in ogni momento.	
Sicurezza	Grazie alle procedure di backup attuate dalle comunità (di riferimento) i dati sanitari registrati nella CIP non vanno persi. Ciò non compromette tuttavia l'autodeterminazione informativa dei pazienti riguardo ai propri dati sanitari e in particolare il loro «diritto all'oblio».
Limiti	I professionisti della salute devono conservare nei propri sistemi i documenti consultati per il trattamento del paziente. Una volta scaricati, questi documenti escono dal quadro giuridico della CIP e soggiacciono ai termini legali cantonali di conservazione.
Riferimenti	OCIP art. 10, CTO n. 9.4.1 e 10

Misure di sicurezza a livello tecnico («T»)

T1	Individuazione delle anomalie e allarme automatico
Ogni comunità (di riferimento) dispone di software e servizi detti SIEM (*Security Information and Event Management)* che sorvegliano costantemente i dati verbalizzati, inclusi i verbali tecnici degli incidenti. Un'apposita procedura permette di individuare schemi inusuali (anomalie) riconducibili a un attacco informatico o a un impiego abusivo e innesca un allarme. Ogni comunità (di riferimento) appronta un sistema di gestione degli incidenti relativi alla sicurezza che permette di esaminare l'allarme scattato e se necessario di adottare le contromisure più opportune.	
Sicurezza	L'individuazione automatizzata dei potenziali incidenti relativi alla sicurezza consente di reagire rapidamente ai tentativi di attacco o di abuso.
Limiti	A volte l'«impianto di allarme CIP» riesce unicamente a contenere i danni ma non a evitarli.
Riferimenti	OCIP art. 12, CTO n. 4.3 e 4.15.6

T2	Conservazione criptata dei dati in Svizzera
I dati conservati nella CIP (inclusi tutti i backup) sono registrati in modo criptato e si trovano in Svizzera presso imprese che sottostanno al diritto svizzero. Queste imprese non sono autorizzate a utilizzare i dati per altri scopi e non possono essere obbligate da autorità estere a divulgarli.	
Sicurezza	Il criptaggio dei dati registrati protegge efficacemente contro l'elusione dei controlli di accesso alla CIP.
Limiti	Benché solo pochissime persone ben definite (in gergo *golden key holder*) abbiano la possibilità di ottenere l'accesso diretto ai dati, le CTO definiscono tutta una serie di misure tecniche e organizzative in termini di sicurezza operativa al fine di contenere nella misura del possibile i rischi derivanti dall'agire di questi «attori interni».
Riferimenti	OCIP art. 10 e 12, CTO n. 2.5.b, 13 - 15 e 19

T3	Comunicazioni sicure
Le comunità (di riferimento) e le strutture sanitarie affiliate costituiscono un'area riservata, isolata da Internet mediante strumenti crittografici basati sui protocolli TLS (*Transport Layer Security*). La sicurezza della configurazione di tutti i punti di terminazione TLS è verificata regolarmente con l'ausilio di programmi di individuazione delle lacune (*vulnerability scanner*).	
Sicurezza	L'impiego coerente del protocolli MTLS (*Mutually authenticated Transport Layer Security*) impedisce che siano stabilite comunicazioni indesiderate con l'area riservata CIP o che siano intercettate le comunicazioni che avvengono in tale area.
Limiti	Un sistema di criptaggio efficace presuppone che tutte le parti che costituiscono l'area riservata CIP gestiscano correttamente le chiavi crittografiche segrete conformemente alle disposizioni legali.
Riferimenti	OCIP art. 10, CTO n. 2.5.a, 4.12 e 4.15

Sicurezza a livello organizzativo («O»)

O1	Gestione continua della sicurezza e obbligo di notifica nel caso di incidenti legati alla sicurezza
In ogni comunità (di riferimento) un responsabile della protezione e della sicurezza dei dati provvede affinché i rischi per la sicurezza siano continuamente identificati, valutati e contenuti. Egli si consulta regolarmente con le autorità e i suoi colleghi delle altre comunità (di riferimento). Se necessario può anche ordinare misure di sicurezza che travalicano le disposizioni legali. Al responsabile della protezione e della sicurezza dei dati compete per legge anche la notifica immediata all'UFSP di incidenti legati alla protezione e alla sicurezza dei dati.	
Sicurezza	Un'organizzazione della sicurezza sostenibile con processi consolidati crea una base imprescindibile per migliorare costantemente il dispositivo di sicurezza e adeguarlo a un contesto in continuo mutamento. Con la CIP si introduce per la prima volta nel sistema sanitario un obbligo di notifica a livello nazionale per incidenti legati alla sicurezza, il che migliora la trasparenza e il controllo delle misure di protezione e sicurezza dei dati.
Limiti	La sicurezza assoluta non esiste e nemmeno il sistema più sofisticato può garantirla.
Riferimenti	OCIP art. 12, CTO n. 4.2, 4.3.3.a e 4.11

O2	Selezione e formazione degli utenti e del personale amministrativo
La formazione in materia di protezione e sicurezza dei dati (*awareness training*) è una tappa obbligata dei corsi di formazione CIP di tutti i professionisti della salute e dell'intero personale amministrativo (ad es. servizi di supporto, gestori dei sistemi). Tutti questi gruppi di persone devono firmare una dichiarazione relativa all'obbligo di mantenere il segreto professionale, a meno che non soggiacciano già al segreto professionale medico. La selezione accurata del personale della comunità (di riferimento) e dei loro fornitori di piattaforme presuppone obbligatoriamente la verifica del registro delle esecuzioni e del casellario giudiziale.	
Sicurezza	Tutte le persone autorizzate ad accedere alla CIP sono consapevoli del fatto che trattano dati particolarmente degni di protezione. Dispongono di una formazione di base per il trattamento di tali dati e conoscono le disposizioni penali nel caso di comportamenti scorretti, il che riduce al minimo la probabilità di una violazione consapevole o inconsapevole delle regole.
Limiti	Non è possibile escludere totalmente possibili errori di utilizzo della CIP.
Riferimenti	CTO n. 4.2.2, 4.8, 4.9

O3	Verifiche della sicurezza
Ogni comunità (di riferimento) dispone di strumenti e processi atti a identificare e colmare lacune nel sistema di sicurezza (ad es. software obsoleti, p*atch* mancanti, configurazioni poco accurate). Dopo ogni modifica rilevante ai fini della sicurezza e soprattutto prima dell'introduzione di ogni nuovo software vengono inoltre verificati gli accessi alla CIP da parte di ditte specializzate (cosiddetti *white hat hacker*) in modo da individuare potenziali lacune nella sicurezza.	
Sicurezza	Gli errori nei programmi o nella configurazione vengono individuati e corretti prima che l'applicazione sia resa accessibile in Internet e quindi esposta a possibili attacchi.
Limiti	Nemmeno i programmi di individuazione delle lacune (*vulnerability scanner*) più recenti né gli *white hat hacker* più qualificati riescono a garantire l'identificazione di tutte le falle della sicurezza prima che le scopra qualcun altro. Le lacune più pericolose sono quelle appena emerse, per le quali non è ancora disponibile un *patch* di sicurezza (cosiddetti *zero day exploits*).
Riferimenti	CTO n. 3.4.1, 3.4.2, 4.4, 4.5