Norme per l’uso della CIP

ID documento:	TA_A08-04
Versione:	V05
Stato:	Approvato
Classificazione:	INTERNO

Sono riservate le modifiche imposte dalla legge o dall’organismo di certificazione

Informazioni Documentali:

Titolo:	Norme per l'uso della CIP
Proprietario:	Direzione
Revisione:	05
Note:	
Rif. DIN EN ISO/IEC 27001:2017-06	A.6.2.1 A.8.3
Rif. OCIP	Art. 12 cpv. 1
Rif. OCIP-DFI	Allegato 2: 4.2 Sistema di gestione della protezione e della sicurezza dei dati

Documenti correlati:

Titolo	Note

Cronologia delle revisioni

Vers.	Data	Autore	Riepilogo delle modifiche
01	14.02.2020	Daniele Della Bruna	Prima stesura
02	04.11.2020	Paolo Gasperi	Cambio ID documento (ex T022)
03	11.11.2020	Paolo Gasperi	Aggiornamento
04	17.08.2021	RPSD/DPO	Revisione
05	25.08.2021	RPSD/DPO	Revisione

Approvazione

Nome	Posizione	Firma	Data
Valeria Belloni	Direttrice		25.08.2021

Lista di distribuzione

Nome	Titolo/funzione

NORME PER L'USO DELLA CIP

LA DIREZIONE DELL'ASSOCIAZIONE EHTI

In osservanza dell'articolo 12 cpv. 1 dell' Ordinanza sulla cartella informatizzata del paziente (OCIP), che recita:

> *Art. 12 Protezione e sicurezza dei dati*
>
> *Le comunità devono dotarsi di un sistema di gestione della protezione e della sicurezza dei dati adeguato ai rischi.*

dell'articolo 4.2 delle condizioni tecniche e organizzative di certificazione delle comunità e comunità di riferimento (CTO), che recita:

> *4.2 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;*

e dell'articolo 4.7 delle condizioni tecniche e organizzative di certificazione delle comunità e comunità di riferimento (CTO), che recita:

> *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)*

Risolve:

Scopo

Art. 1. Questo documento illustra:
- il corretto utilizzo delle dotazioni informatiche
- le disposizioni necessarie per l'utilizzo della Cartella Informatizzata del Paziente (CIP).

Destinatari

Art. 2. Tutti gli utenti interni all'associazione eHTI e tutti gli utenti dei fornitori di cura affiliati a eHTI.

Definizioni

Art. 3.
Intranet: accesso ai servizi informatici limitato alla sola rete aziendale;
Internet: accesso ai servizi informatici di dominio pubblico;
Utente: chiunque dispone di credenziali di accesso alla rete dell'Associazione eHTI;
Utente CIP: chiunque dispone di credenziali di accesso alla rete piattaforma CIP;

Accesso da remoto: è la possibilità di accedere a un computer, dispositivo o applicazione da un altro dispositivo, in qualsiasi momento e da qualsiasi luogo;
Telelavoro: per telelavoro si intende l'attività lavorativa svolta regolarmente o in maniera sporadica da casa o in sede di servizio alternativa.

Premessa

Art. 4. Il presente documento stabilisce le norme comportamentali relative all'utilizzo delle risorse informatiche e telematiche e della CIP, a cui ciascun utente dell'associazione eHTI, o utente di un fornitore di cura (professionista della salute, struttura) affiliato all'associazione eHTI si deve attenere.
L'utilizzo delle strumentazioni informatiche e telematiche deve sempre ispirarsi ai principi di diligenza e correttezza, che sono alla base di ogni rapporto di lavoro.
La progressiva e capillare diffusione delle tecnologie informatiche e dell'accesso alla rete Internet può esporre l'associazione eHTI, la struttura affiliata e i dati contenuti della Cartella Informatizzata del Paziente (CIP) a numerosi rischi, sia in termini di riservatezza, integrità e disponibilità dei dati stessi, sia in termini di conseguenze finanziarie, penalistiche, reputazionali e di sicurezza interna.

Durata

Art. 5. Le norme per l'uso delle dotazioni informatiche devono essere applicate dal primo giorno in cui l'utente ha accesso alle risorse informatiche e telematiche e alla CIP tramite il suo account e devono perdurare fino alla cancellazione definitiva del suo accesso alle risorse informatiche e telematiche ed alla CIP.

Regole generali

Art. 6.
Il Centro Sistemi Informativi del cantone Ticino (CSI) ha il compito di gestire ed aggiornare regolarmente con le nuove versioni e/o patch di sicurezza rilasciate i sistemi informatici dell'associazione eHTI, in particolare i sistemi di informatica individuale tipo PC, stampanti, scanner, schermi e tablet.
Il fornitore di cura deve assumersi il compito di gestire ed aggiornare regolarmente con le nuove versioni e/o patch di sicurezza rilasciate i sistemi informatici, in particolare i sistemi di informatica individuale tipo PC, stampanti, scanner, schermi e tablet e utilizzare sistemi di protezione delle reti informatiche.

Accesso alla CIP

Art. 7. In caso di accesso alla CIP in telelavoro o da remoto, lo stesso è permesso solo su territorio svizzero.

Condizioni generali uso CIP

Art. 8.
L'accesso alla CIP per gli utenti dell'Associazionoe eHTI è consentito a condizione che:

- il dispositivo sia fornito e amministrato dall'associazione eHTI;
- il dispositivo sia inserito in un inventario in gestione dell'associazione eHTI;
- l'utilizzatore non accede alle impostazioni con i privilegi di amministratore.

L'accesso alla CIP per gli utenti dei fornitori di cura è consentito a condizione che:

- il dispositivo sia fornito e amministrato dal fornitore di cura;
- il dispositivo sia inserito in un inventario in gestione del fornitore di cura;
- l'utilizzatore non accede alle impostazioni con i privilegi di amministratore.

Condizioni generali telelavoro

Art. 9. Premesso che il telelavoro o accesso da remoto alla CIP sono a carattere volontario, esso può essere applicato solo ed esclusivamente alle seguenti condizioni:

- la postazione di lavoro è fornita e amministrata dall'associazione eHTI (per gli utenti di eHTI) e dai fornitori di cura (per gli utenti del personale di cura);
- la postazione di lavoro non viene utilizzata per scopi privati
- è garantito un livello di connessione adeguato della postazione di lavoro adottando una tra le seguenti soluzioni:
  - ✓ attivazione di una VPN (Virtual Private Network, una rete privata virtuale che garantisce privacy, anonimato e sicurezza) verso la struttura
  - ✓ accesso in desktop remoto ad una postazione (virtuale o non) all'interno della struttura
- l'ambiente di lavoro (fisico) è idoneo allo svolgimento della professione; in particolare è garantita la riservatezza dei dati dei pazienti verso terze persone.

Utilizzo del posto di lavoro fisso (personal computer)

Art. 10. Il computer in dotazione è uno strumento di lavoro da utilizzarsi nel rispetto dei principi di correttezza e diligenza.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi e minacce alla sicurezza.

La postazione di lavoro non deve essere lasciata incustodita o facilmente accessibile. Il dispositivo implementa un sistema di disconnessione automatica in caso di inattività dopo al massimo 10 minuti. Tale sistema attiva lo screen saver e la necessità di inserire la password per sbloccare il dispositivo.

La postazione di lavoro deve essere spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

È espressamente vietato l'uso di supporti rimovibili per la memorizzazione di dati sensibili.

Non è consentita/o:

- l'installazione di programmi diversi da quelli autorizzati da CSI (per quanto riguarda gli utenti di eHTI) o dal servizio informatico del fornitore di cura (per quanto riguarda gli utenti del fornitore di cura);
- aprire, smontare, manomettere o spostare qualsiasi tipo di apparecchio hardware
- modificare i parametri tecnici e le impostazioni di sicurezza hardware e software (posta elettronica, web browser, sistema operativo, firewall, antivirus, ecc.).

Utilizzo di pc portatili / tablet aziendali

Art. 11. Ai portatili e ai tablet si applicano le stesse regole di utilizzo previste per i computer fissi (cfr. art. 10).

L'utente è responsabile del portatile e/o tablet assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo. Il portatile/tablet deve essere presidiato direttamente oppure riposto in luogo sicuro.

Utilizzo di apparecchiature mobili private

Art. 12. Per quanto concerne gli utenti di eHTI, CSI permette l'accesso con gli smartphone e i tablet al server di posta elettronica; il fornitore di cura deve valutare se consentire tale tipo di accesso ai propri utenti.
Devono pertanto essere adottate tutte le misure necessarie onde evitare che terzi possano accedere ai dati della posta elettronica aziendale.

Gestione account / password / eID

Art. 13. La password di accesso al PC e alla rete è nominale ed è distribuita dal CSI (per gli utenti di eHTI) e dal servizio informatico del fornitore di cura (per gli utenti del fornitore di cura). Il profilo e la password di accesso alla CIP è distribuita dall'associazione eHTI. Il profilo di identità elettronica è distribuito dal provider di identità elettronica accreditato.
Il regolamento per le password dell'identità elettronica è descritto nelle regole del provider dell'identità elettronica.
La password di accesso alla CIP deve essere composta da almeno otto caratteri (sia lettere che numeri).
L'utente deve creare una password priva di riferimenti banali (è sconsigliato indicare il proprio nome, la propria data di nascita, il nome del coniuge, ecc.) e non deve comunicarla a terzi.
Il collaboratore deve modificare la password al primo utilizzo e, successivamente scadenza regolare, almeno ogni 180 giorni (la nuova password deve essere diversa dalle 5 password precedenti).
L'utente autorizzato a trattare dati personali deve adottare le necessarie cautele per assicurare la segretezza, l'esclusività della password (ad es. non scrivere la password su promemoria da attaccare al computer tipo "post-it" o archiviarla in file sui sistemi aziendali). Nel caso si sospetti che la password abbia perso la segretezza, deve essere immediatamente sostituita.
Il proprio account interno e la propria password utilizzata per collegarsi ai pc aziendali e alla CIP non devono essere utilizzati su siti esterni.

Dati sensibili

Art. 14. Qualsiasi dato riguardante i pazienti, il collaboratore dell'associazione eHTI, o degli istituti affiliati è da considerare sensibile.
Il trattamento dei dati deve essere conforme al principio della buona fede e della proporzionalità.
I dati possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge.
La raccolta di dati sensibili e in particolare le finalità del loro trattamento devono essere riconoscibili da parte della persona interessata. Quando il trattamento di dati sensibili è subordinato al consenso della persona interessata, il consenso è valido soltanto se espresso liberamente e dopo debita informazione. Trattandosi di dati personali degni di particolare protezione o di profili della personalità, il consenso deve essere esplicito.
Chi tratta dati sensibili deve accertarsi della loro esattezza e deve prendere tutte le misure adeguate per assicurare che dati non pertinenti o incompleti in considerazione dello scopo per cui sono stati raccolti o elaborati vengano cancellati o rettificati.
I dati sensibili devono essere protetti contro ogni trattamento non autorizzato.

Uso di internet

Art. 15. L'utilizzo inadeguato di Internet da parte dei collaboratori potrebbe cagionare un danno all'associazione eHTI, al fornitore di cura, alla sua immagine e reputazione, nonché far sorgere in capo all'associazione eHTI, al fornitore di cura e/o al collaboratore responsabilità a carattere civile e/o penale. Pertanto, non è consentito:

- l'utilizzo di Internet a fini privati
- registrarsi su siti i cui contenuti non siano strettamente legati all'attività lavorativa, partecipare a forum non professionali e utilizzare chat line
- l'accesso e/o l'uso di social networks/social media, come pure di servizi e programmi di messaggistica istantanea, video e/o audio conferenza, file transfer, desktop sharing e simili non autorizzati
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti e risorse che consentono lo scambio, la distribuzione o il downloading di dati tra utenti privati (es. reti peer-to-peer), come pure l'installazione e l'uso di browser non approvati
- introdursi abusivamente in un sistema informatico o telematico (sia che sia protetto da misure di sicurezza, oppure no) e accedere a dati, informazioni o programmi in esso contenuti, non avendone l'autorizzazione.

Qualora un collaboratore dovesse trovarsi accidentalmente e senza sua specifica volontà collegato ad un sito dai contenuti inappropriati dovrà scollegarsi immediatamente e informare senza indugio il CSI (per gli utenti di eHTI) o il servizio informatico del fornitore di cura (per gli utenti del fornitore di cura), il quale verificherà se sussistono rischi per la sicurezza dei dati e adotterà le misure adeguate.

Uso della posta elettronica

Art. 16. È suggerito l'uso della posta elettronica come normale strumento di comunicazione aziendale.

È tuttavia vietato l'invio di dati sensibili di pazienti registrati nella CIP attraverso la posta elettronica.

Ogni collaboratore è responsabile del corretto utilizzo della propria casella di posta. In tal senso, le principali regole di comportamento nell'utilizzo della posta elettronica aziendale prevedono che:

- il collaboratore verifichi attentamente, prima dell'invio, che l'indirizzo email del destinatario sia corretto e che lo stesso sia autorizzato a ricevere l'email e i suoi allegati
- è vietato l'uso dell'indirizzo email aziendale ai fini privati, pertanto è proibita la comunicazione a persone estranee all'attività aziendale, la pubblicazione o l'iscrizione a servizi online di suddetto indirizzo se non quando ciò sia strettamente necessario nell'interesse dell'associazione eHTI (per gli utenti di eHTI) o del fornitore di cura (per i suoi utenti)
- le informazioni contenute nei messaggi di posta elettronica sono da considerarsi informazioni aziendali, riservate e confidenziali, ne è quindi vietata la diffusione a persone non autorizzate
- è vietato aprire i file allegati a messaggi di posta elettronica di fonte sconosciuta, non richiesti o non riferibili ad una transazione nota.

Tali allegati potrebbero contenere o determinare lo scaricamento di un virus o altro software malevolo; non bisogna assolutamente aprire gli allegati che abbiano estensioni come, ad esempio, BAT, COM, DLL, EXE, PIF, SCR. Nel caso di dubbi contattare sempre il CSI

- è vietata la cancellazione dei messaggi email in entrata e in uscita, qualora il contenuto sia sottoposto a vincoli temporali di conservazione indicati dalla normativa vigente
- per gli utenti eHTI, è assolutamente vietata la trasmissione via email di dati confidenziali/riservati dei pazienti, se non in forma crittografata o altrimenti protetta, o se autorizzati per iscritto dalla Direzione eHTI;
- per gli utenti del fornitore di cura, si applicano i regolamenti interni della struttura che devono seguire le best practice di protezione e sicurezza dati e, in ogni caso, è concessa la trasmissione soltanto a destinatari che siano stati previamente autorizzati ad accedere a tali dati
- è assolutamente vietato l'inserimento di tali dati confidenziali/riservati su siti web, anche nel caso facessero riferimento a link ricevuti mediante posta elettronica dai clienti/partner
- in caso di assenza dal posto di lavoro, il collaboratore provvede a concordare con il CSI (per gli utenti di eHTI) e con il servizio informatico del fornitore di cura (per gli utenti del fornitore di cura) il programma di posta elettronica in modo che le comunicazioni in arrivo siano automaticamente deviate all'indirizzo email concordato.

Protezione antivirus

Art. 17. L'utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale. I dispositivi in dotazione sono protetto dall'esecuzione di software dannosi con un applicativo di sicurezza (antivirus); questo è aggiornato con regolarità.
Nel caso in cui il programma antivirus rilevi la presenza di un virus l'utente dovrà sospendere ogni attività, disattivare immedatamente la connessione ad internet e segnalare l'accaduto al CSI (per gli utenti di eHTI) e al servizio informatico del fornitore di cura (per gli utenti del fornitore di cura)
Ogni dispositivo di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.
Per quanto concerne i fornitori di cura, gli stessi devono considerare che abbinata alle funzionalità dell'antivirus è opportuno che vengano attivate e regolarmente aggiornate anche le funzionalità di firewall.

Salvataggio dei dati

Art. 18. Ogni collaboratore ha a disposizione un identificativo personale per accedere ai sistemi e alle applicazioni in base alla funzione.
I dati che saranno utilizzati sono posti in archivi dei sistemi server centrali la cui salvaguardia è garantita dal CSI tramite backup (per quanto riguarda gli utenti eHTI) e deve essere garantita dal servizio informatico della propria struttura (per quanto riguarda gli utenti dei fornitori di cura).
La confidenzialità di queste informazioni deve essere garantita.
Non deve essere consentita la memorizzazione di dati sensibili su supporti rimovibili (e in quanto tali asportabili dal proprio luogo di lavoro).

Il salvataggio dei propri dati su supporto rimovibile non deve essere effettuato (chiavi USB, …) in quanto ritenuti poco affidabili e/o soggetti a smarrimento.

Furto

Art. 19. In caso di furto o di perdita del possesso del dispositivo per qualsiasi motivo, il collaboratore deve avvertire immediatamente il CSI (per gli utenti di eHTI) e il servizio informatico del fornitore di cura (per gli utenti del fornitore di cura). Il collaboratore, inoltre, è tenuto a sporgere denuncia all'autorità di competenza nei termini di legge e presentarne copia all'Associazione eHTI/al fornitore di cura.
In caso di comportamento doloso o negligente del collaboratore nella gestione del dispositivo e/o nella tempestività nel denunciare il furto o la perdita del possesso del dispositivo, a seconda della gravità della colpa, delle circostanze e/o delle conseguenze effettive o potenziali per l' Associazione eHTI, o per il fornitore di cura o per terzi interessati, al collaboratore potranno essere applicati provvedimenti disciplinari, come indicato all'art. 25.

Guasto

Art. 20. In caso di guasto del dispositivo (ma anche per modifica delle impostazioni interne, oppure smaltimento) bisogna rivolgersi al CSI (per gli utenti di eHTI) o al servizio informatico del fornitore di cura (per gli utenti del fornitore di cura).

Smaltimento

Art. 21. Tutti i supporti contenenti dati riservati devono essere consegnati al CSI (per gli utenti di eHTI) o al servizio informatico del fornitore di cura (per gli utenti del fornitore di cura) per lo smaltimento sicuro degli stessi, in modo da evitare la divulgazione di informazioni riservate.

Segnalazioni anomalie/incidenti di sicurezza

Art. 22. Qualsiasi situazione a rischio, anomalia o incidente per la sicurezza dei dati, delle informazioni o degli strumenti informatici aziendali, deve essere sempre e tempestivamente segnalato al CSI (per gli utenti di eHTI) o al servizio informatico del fornitore di cura (per gli utenti del fornitore di cura.
Sono considerati incidenti di sicurezza:

- la perdita di riservatezza dei dati/informazioni/documenti (es. accesso ai dati da parte di persone non autorizzate)
- la compromissione dell'integrità dei dati/informazioni/documenti (es. errori causati da dati incompleti o inesatti)
- l'indisponibilità dei dati/informazioni/documenti (es. problemi di indisponibilità dei dati per effetto di un malfunzionamento/blocco del sistema informatico)
- la violazione delle normative in materia di protezione dei dati (es.: privacy, copyright, ecc.)
- i danni derivanti da attività non previste o inusuali sui server;
- il furto o lo smarrimento di dispositivi contenenti dati particolarmente rilevanti e/o sensibili
- il danneggiamento di sistemi.

Controlli

Art. 23. L'associazione eHTI e i fornitori di cura, rispettivamente ciascuno per il proprio personale, si riservano la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del collaboratore nell'uso della CIP.
Le verifiche si svolgeranno nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dalla legge.

A seguito delle verifiche informatiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza.
Eventuali informazioni di natura sensibile potranno essere trattate dall'associazione eHTI e dal fornitore di cura se necessario per far valere o difendere un diritto in sede giudiziaria.

Inosservanza delle disposizioni

Art. 25. Il personale deve attenersi scrupolosamente alle disposizioni normative vigenti sulla CIP e a quanto stabilito dalla Legge Federale sulla protezione dei dati, alle istruzioni e regole di condotta che gli vengono impartite in fase di sottoscrizione dell'Accordo sull'uso della CIP, alle procedure, politiche e regolamenti condivisi all'interno della Comunità e alle indicazioni fornite durante i corsi di formazione, o direttamente da eHTI o da eventuali superiori.
Il mancato rispetto di quanto stabilito sopra e nel presente documento comporta azioni disciplinari contro la persona in questione, in misura variabile a seconda della gravità del comportamento e del danno.

Entrata in vigore

Art. 26. La presente direttiva entra in vigore immediatamente.