# ALLEGATO
# RIGUARDANTE I DIRITTI DI AUDIT E I REQUISITI DI SICUREZZA PER CLIENTI GATEWAY

**Versione:** 1.0

**Data:** 17.01.2024

## 1. Introduzione

Health Info Net AG (di seguito denominata «HIN») si impegna a rispettare i requisiti per la protezione dei dati e la sicurezza delle informazioni in leggi, regolamenti, norme e contratti. Si tratta dei seguenti:

- Legge federale sulla protezione dei dati (LPD), RS 235.1
- Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD), RS 235.11
- Legge federale sulla cartella informatizzata del paziente (LCIP), RS 816.1
- Ordinanza sulla cartella informatizzata del paziente (OCIP), RS 816.11
- Ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI), RS 816.111
- Allegato 2 dell'OCIP-DFI
- Allegato 8 dell'OCIP-DFI
- ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements
- ISO/IEC 27002, Information security, cybersecurity and privacy protection – Information security controls

HIN governa un sistema di gestione della protezione dei dati e della sicurezza delle informazioni che include una gestione dei rischi e della conformità.

Questo sistema di gestione è influenzato da fornitori e clienti definiti, il che richiede un relativo auditing.

HIN viene sottoposta regolarmente ad auditing da parte di organismi di certificazione accreditati e finora è stata certificata secondo la norma ISO/IEC 27001 e l'Allegato 8 dell' Ordinanza del DFI sulla cartella informatizzata del paziente. La certificazione dell'IdP HIN include l'Access Gateway.

## 2. Diritti di audit di HIN

A partire dalla data della firma, il cliente Gateway assegna a HIN i diritti di audit descritti di seguito.

Il presente Allegato contiene inoltre requisiti di sicurezza specifici per Access Gateway (AGW) e Mail Gateway (MGW).

## 3. Responsabilità nell'auditing

Il Responsabile di HIN informa il rispettivo cliente Gateway sull'imminente audit con almeno un mese di anticipo e organizza il colloquio preliminare.

Il cliente Gateway nomina un Responsabile interno che, insieme all'auditor, stabilisce le scadenze, fornisce i documenti necessari, accompagna l'audit, prende in consegna i risultati e coordina le eventuali misure correttive necessarie.

## 4. Ambito dell'audit

Sulla base di ISO/IEC 27001, Allegato 2 OCIP-DFI e Allegato 8 OCIP-DFI viene verificata una selezione ridotta di argomenti particolarmente critici, basata su documenti, interviste e controlli sui sistemi pertinenti:

**1. Sicurezza fisica**

- Linee guida o concetto per la sicurezza fisica
- Responsabilità per la sicurezza fisica
- Zone e autorizzazioni di accesso effettive
- Controlli regolari delle autorizzazioni di accesso

**2. Sicurezza della rete**

- Linee guida o concetto per la sicurezza della rete
- Responsabilità per la sicurezza della rete
- Zone di rete
- Collegamento del Gateway all'ActiveDirectory
- Attributi dei certificati del server
- Ev. configurazione del cluster
- Controlli regolari della sicurezza della rete

**3. Accessi logici**

- Linee guida o concetto per accessi logici
- Responsabilità per accessi logici
- Autorizzazioni di accesso privilegiate
- Controlli regolari delle autorizzazioni di accesso

**4. Registrazione (logging)**

- Linee guida o concetto per la registrazione
- Responsabilità per la registrazione
- Fonti degli eventi
- Tipi e attributi di eventi
- Controlli regolari dei protocolli

**5. Gestione di accadimenti correlati alla sicurezza**

- Linee guida o concetto per la gestione di accadimenti correlati alla sicurezza
- Responsabilità nella gestione di accadimenti correlati alla sicurezza
- Tipi e valutazione di accadimenti correlati alla sicurezza
- Regole sulla notifica di accadimenti correlati alla sicurezza
- Ev. esempi di accadimenti correlati alla sicurezza

**6. Sistema di gestione della protezione dei dati e della sicurezza delle informazioni**

- Linee guida per la sicurezza delle informazioni
- Linee guida nella gestione del rischio
- Rischi legati al Gateway

## 5. Risultati dell'audit ed ev. misure correttive

I risultati dell'audit vengono forniti al cliente Gateway sotto forma di tabella attraverso un canale sicuro (ad esempio e-mail HIN). Non possono essere divulgati a terzi né da HIN né dai clienti Gateway. L'unica eccezione sono gli organismi di certificazione accreditati.

In caso di misure correttive necessarie viene definito un termine, solitamente tre mesi dopo l'audit.

Il Responsabile del cliente Gateway coordina queste misure correttive e riferisce i risultati a HIN che li verifica.

## 6. Costo dell'audit

Il costo dell'audit presso HIN e presso il cliente Gateway viene fatturato al cliente in base al relativo tariffario.

Per il lavoro preliminare, lo svolgimento dell'audit e l'elaborazione dei dati si prevede una mezza giornata.

# REQUISITI DI SICUREZZA

I seguenti requisiti di sicurezza possono essere aggiornati periodicamente, in modo unilaterale, in funzione di leggi, regolamenti, norme o altre disposizioni modificati o nuovi.

Il cliente è tenuto a:

- Gestire i HIN Gateway in un ambiente fisico protetto.
- Gestire i HIN Gateway in un ambiente logico protetto.
- Adottare una politica di password forte e all'avanguardia (nessun account senza password, nessuna password predefinita, nessuna password identica per account diversi, password extra-lunghe per account di assistenza e account privilegiati ecc.).
- Bloccare gli utenti finali e gli account di assistenza dopo un numero definito di tentativi di accesso falliti (inferiore a 20).
- Impostare dei timeout di inattività.
- Prevedere e svolgere il prima possibile aggiornamenti del software, soprattutto quelli dichiarati critici da HIN.
- Registrare eventi rilevanti per la sicurezza dei HIN Gateway (Audit trail) e, se necessario, metterli a disposizione di HIN o concedere l'accesso a HIN.
- Segnalare immediatamente a HIN eventuali rischi per la sicurezza e accadimenti correlati alla sicurezza in relazione agli HIN Gateway.