

POLITICA INTERNA

Sicurezza informatica e protezione dei dati

[Nome dello studio dentistico]

[Indirizzo completo]

Versione 1.0 | [Data]
Conforme alla nLPD (RS 235.1)

1. Oggetto e campo d'applicazione

La presente politica stabilisce le regole di sicurezza informatica e di protezione dei dati applicabili a tutto il personale dello studio. Rientra negli obblighi previsti dalla legge federale sulla protezione dei dati (nLPD, RS 235.1), in particolare dall'art. 8 sulla sicurezza dei dati.

Si applica a tutte le persone che hanno accesso ai sistemi informatici o ai dati dello studio: medici dentisti, assistenti dentali, personale amministrativo, stagisti, sostituti e qualsiasi fornitore esterno che intervenga nei locali o sui sistemi dello studio.

2. Responsabilità

Il titolare dello studio è il titolare del trattamento ai sensi della nLPD. È personalmente responsabile dell'attuazione, della comunicazione e del rispetto della presente politica.

Ogni collaboratore è tenuto a rispettare le regole seguenti. Qualsiasi violazione può comportare misure disciplinari interne, fatte salve le sanzioni penali previste dalla nLPD (art. 60–63) e dal Codice penale (art. 321).

3. Accesso ai sistemi informatici

- Ogni collaboratore dispone di un account nominativo personale. Gli account condivisi («studio», «admin», «accettazione») sono vietati.
- Le credenziali di accesso sono strettamente personali e non devono mai essere comunicate, nemmeno a un collega o a un superiore.
- Le password devono contenere almeno 12 caratteri e combinare maiuscole, minuscole, cifre e simboli. Devono essere conservate esclusivamente nel gestore di password messo a disposizione dallo studio.
- L'autenticazione a due fattori (2FA) deve essere attivata su tutti gli accessi critici: posta elettronica professionale, software gestionale, backup nel cloud, accesso remoto.
- Gli account dei collaboratori che lasciano lo studio vengono disattivati immediatamente, il giorno stesso della partenza.

4. Utilizzo delle postazioni di lavoro

- Le postazioni di lavoro sono destinate a un uso esclusivamente professionale.
- Lo schermo deve essere bloccato ogni volta che ci si allontana dalla postazione, anche solo per pochi istanti
Windows: *Windows+L*
Apple macOS: *Ctrl+Comando+Q*
- È vietato installare software non autorizzati. Solo il fornitore di servizi informatici è abilitato a installare o aggiornare software.
- Gli aggiornamenti del sistema operativo e delle applicazioni devono essere installati non appena sono disponibili. Le postazioni devono essere riavviate almeno una volta alla settimana per permettere l'installazione delle correzioni di sicurezza.

5. Posta elettronica e comunicazioni

- Qualsiasi comunicazione contenente dati identificabili dei pazienti (radiografie, diagnosi, numeri AVS, referti) deve passare dalla posta elettronica crittografata dello studio (HIN Mail, ProtonMail o un equivalente conforme).
- L'invio di dati dei pazienti tramite servizi di messaggistica di largo consumo (Gmail, Hotmail, Bluewin, WhatsApp, SMS, social network) è severamente vietato.
- Gli allegati e i link contenuti in e-mail inattese non devono mai essere aperti. In caso di dubbio, contattare il titolare dello studio o il fornitore di servizi informatici prima di qualsiasi azione.

6. Dati dei pazienti e riservatezza

- I dati dei pazienti non devono mai essere copiati su supporti personali: chiavette USB, dischi rigidi, telefoni, tablet o servizi cloud personali.
- I documenti cartacei contenenti dati dei pazienti devono essere distrutti con un distruggidocumenti. Non devono mai essere gettati nella spazzatura.
- Nessuna cartella clinica, radiografia stampata o documento amministrativo contenente dati personali deve essere lasciato in vista su un bancone, su una scrivania o vicino a zone accessibili ai pazienti.
- Tutto il personale è soggetto al segreto professionale (art. 321 del Codice penale). Quest'obbligo vale durante e dopo il contratto di lavoro.

7. Dispositivi personali (BYOD)

[Scegliere l'opzione applicabile allo studio:]

Opzione A: L'uso di dispositivi personali (telefoni, tablet, computer portatili, chiavette USB) per accedere ai dati o ai sistemi dello studio è severamente vietato.

Opzione B: L'uso di dispositivi personali è consentito alle seguenti condizioni: [precisare le condizioni, per esempio: solo per consultare l'agenda, con crittografia attivata, blocco con codice e senza archiviazione locale di dati dei pazienti].

8. Sicurezza fisica

- I locali che contengono server, backup o apparecchiature di rete devono essere chiusi a chiave e accessibili solo al personale autorizzato.
- Visitatori, fornitori e tecnici esterni non devono essere lasciati soli in zone in cui gli schermi mostrano dati dei pazienti o in cui sono accessibili documenti sensibili.
- Gli schermi visibili dalla sala d'attesa o dalle zone di passaggio devono essere posizionati in modo da non esporre i dati dei pazienti, oppure dotati di filtri privacy.

9. Rete Wi-Fi

- La rete principale dello studio (postazioni di lavoro, server, stampanti) è separata dalla rete ospiti destinata ai pazienti.
- La password della rete principale non deve mai essere comunicata ai pazienti né esposta nei locali accessibili al pubblico.
- Il collegamento di dispositivi personali alla rete principale è vietato, salvo autorizzazione esplicita del titolare dello studio.

10. Procedura in caso di incidente

In caso di sospetto attacco informatico, di perdita di dati o di qualsiasi evento insolito:

1. Isolare la postazione interessata: scollegare il cavo di rete, disattivare il Wi-Fi. Non spegnere la postazione.
2. Informare immediatamente il titolare dello studio.
3. Contattare il fornitore di servizi informatici dello studio.
4. Documentare l'incidente: fotografare gli schermi, annotare l'ora esatta, descrivere i sintomi osservati.
5. Non tentare mai di risolvere il problema da soli, non pagare alcun riscatto, non cancellare i messaggi sospetti.

I numeri d'emergenza sono affissi vicino a ogni postazione di lavoro.

11. Sanzioni in caso di mancato rispetto

Qualsiasi violazione della presente politica può comportare misure disciplinari interne fino al licenziamento, fatte salve le responsabilità penali personali previste dalla nLPD (art. 60–63, multe fino a CHF 250'000) e dal Codice penale (art. 321, violazione del segreto professionale).

12. Aggiornamento della politica

La presente politica è riesaminata e aggiornata almeno una volta all'anno, oppure a ogni cambiamento significativo dell'infrastruttura informatica, degli strumenti utilizzati o del quadro legale. Ogni aggiornamento viene comunicato nuovamente a tutto il personale e firmato di nuovo.

Dichiarazione di presa visione

Io sottoscritto/a dichiaro di aver letto, compreso e accettato la presente politica di sicurezza informatica e di protezione dei dati dello studio. Mi impegno a rispettare tutte le regole sopra indicate nell'ambito delle mie funzioni.

Cognome e nome: _____

Funzione: _____

Data: _____

Firma del collaboratore: _____

Firma del titolare dello studio: _____

Note legali e condizioni di utilizzo

Questo documento è stato redatto da **DentalSystems Sàrl** a scopo informativo e di sensibilizzazione. Non costituisce una consulenza legale. Le informazioni contenute in questo documento sono aggiornate a marzo 2026 e possono cambiare in seguito a modifiche legislative e regolamentari. Questa versione italiana è una traduzione; fa fede la versione francese.

Per qualsiasi questione giuridica relativa alla nLPD, al RGPD o alla protezione dei dati in ambito medico, rivolgetevi a un giurista specializzato.

Proprietà intellettuale

Questo documento è di proprietà esclusiva di DentalSystems Sàrl. L'intero contenuto (testi, struttura, impaginazione ed elementi grafici) è protetto dal diritto d'autore conformemente alla legge federale sul diritto d'autore e sui diritti di protezione affini (LDA, RS 231.1).

Utilizzo consentito

Questo modello è messo a disposizione gratuitamente. Può essere modificato e utilizzato a nome dello studio, anche nei confronti dei suoi pazienti, collaboratori e fornitori, senza conservare le nostre diciture.

Utilizzi vietati

Salvo previo consenso scritto di DentalSystems Sàrl, sono vietate:

- La vendita di questo documento, anche se modificato.
- La sua messa a disposizione per il download a terzi (siti di download, piattaforme di condivisione, rivenditori).

Si applicano le condizioni di utilizzo pubblicate su www.dentalsystems.ch; in caso di divergenza, esse prevalgono sul presente avviso.

Limitazione di responsabilità

Questo documento è fornito gratuitamente, a titolo informativo. Nei limiti consentiti dal diritto svizzero, DentalSystems Sàrl non risponde delle conseguenze del suo utilizzo; questa limitazione non si applica in caso di dolo o di colpa grave. L'utente resta responsabile del suo adattamento alla propria situazione. Il documento non sostituisce né un audit professionale né una consulenza legale.

DentalSystems Sàrl

Thomas Alvino, tecnico IT

www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44

© 2026 DentalSystems Sàrl. Tutti i diritti riservati.