

GUIDA DI RIFERIMENTO

Cibersicurezza & nLPD

Proteggere i dati dei vostri pazienti.

Mettere in sicurezza la vostra infrastruttura informatica.

Comprendere i vostri obblighi legali.

DentalSystems Sàrl

Thomas Alvino, tecnico IT

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

Ottobre 2026. Conforme alla nLPD (RS 235.1)

INDICE

Introduzione	7
Capitolo 1. Il quadro legale: la nLPD	8
1.1 Che cos'è la nLPD?	8
1.2 Quali dati sono interessati?	8
1.3 I tre obblighi fondamentali	9
1.4 Notifica delle violazioni (art. 24 LPD)	9
1.5 Diritti dei pazienti (art. 25 LPD)	11
Comunicazione dei dati sulla salute (art. 25 cpv. 3)	11
Responsabilità in caso di ricorso a un responsabile del trattamento (art. 25 cpv. 4).....	11
Carattere imperativo del diritto d'accesso (art. 25 cpv. 5).....	11
Gratuità e termine (art. 25 cpv. 6 e 7).....	11
Rimedi del paziente in caso di inosservanza	11
1.6 Registro delle attività di trattamento (art. 12 LPD)	13
1.7 Sanzioni (art. 60–66 LPD)	13
1.8 Differenze principali rispetto al vecchio diritto (LPD 1992)	15
1.9 Privacy by Design e Privacy by Default (art. 7 LPD)	15
1.10 Valutazione d'impatto sulla protezione dei dati (art. 22 LPD)	16
Esempi che richiedono una VIPD	16
Contenuto della valutazione d'impatto	16
1.11 Giurisprudenza recente	16
Statthalteramt Bezirk Zürich, marzo 2025 (ST.2024.1046/ZM)	16
1.12 Buone pratiche per la gestione delle richieste d'accesso	17
Capitolo 2. Posta elettronica sicura	18
2.1 Il problema.....	18
2.2 Le soluzioni conformi.....	18
Capitolo 3. Aggiornamenti.....	20
3.1 Sistema operativo.....	20

3.2 Applicazioni e software gestionali	20
Capitolo 4. Backup	21
4.1 La regola 3-2-1	21
4.2 Perché la copia immutabile è essenziale	21
4.3 Testare il ripristino	22
Capitolo 5. Password e autenticazione a due fattori	23
5.1 Il problema delle password deboli	23
5.2 Creare una password robusta	23
5.3 Usare un gestore di password	23
5.4 Autenticazione a due fattori (2FA)	23
Capitolo 6. Crittografia dei dischi e degli archivi	24
6.1 Crittografia delle postazioni di lavoro	24
6.2 Contenitori crittografati per archivi sensibili	24
Capitolo 7. Rete Wi-Fi	25
7.1 La configurazione raccomandata: tre reti separate	25
Capitolo 8. Accesso remoto sicuro	26
8.1 Il rischio delle versioni gratuite sempre in standby	26
8.2 Soluzioni raccomandate	26
Capitolo 9. Phishing	27
9.1 Riconoscere un'e-mail di phishing	27
9.2 Protezione avanzata: il filtraggio tramite etichette	27
Capitolo 10. Gestione degli accessi degli utenti	28
10.1 Principio del privilegio minimo	28
10.2 Regole di gestione degli account	28
10.3 Gestione degli arrivi e delle partenze	28
10.4 Verifica periodica dei diritti d'accesso	30
10.5 Strumenti che facilitano la gestione degli accessi	30
Capitolo 11. Malware polimorfici e protezione EDR	31
11.1 Perché l'antivirus classico non basta più	31

11.2 La soluzione: l'EDR (Endpoint Detection and Response)	31
11.3 EDR, EPP, antivirus: capire le differenze	32
11.4 Il ruolo del fornitore di servizi informatici	32
Capitolo 12. Modernizzazione del parco informatico	33
12.1 Perché un computer obsoleto è pericoloso	33
12.2 Ciclo di rinnovo raccomandato	33
12.3 Caso particolare: iMac con Boot Camp	34
12.4 Pianificare la migrazione	35
12.5 Distruzione sicura delle vecchie apparecchiature	35
Capitolo 13. Il contratto con il responsabile del trattamento (art. 9 LPD)	36
13.1 Condizioni preliminari per affidare un trattamento	36
13.2 Chi riguarda il contratto con il responsabile del trattamento?	36
13.3 Che cosa deve contenere il contratto	38
13.4 Verificare gli strumenti del vostro fornitore	40
13.5 Responsabilità nei confronti dei pazienti (art. 25 cpv. 4)	40
13.6 Il mio fornitore attuale non ha un contratto: che fare?	40
Capitolo 14. Formazione del personale	41
14.1 Un obbligo implicito della nLPD	41
14.2 Contenuto raccomandato di una formazione	41
14.3 Apparecchi personali e BYOD	44
14.4 Personale temporaneo e terzi	44
14.5 La politica interna di sicurezza scritta	45
14.6 Frequenza, formato e valutazione	45
14.7 Responsabilità condivisa	45
Capitolo 15. Assicurazioni cyber	47
15.1 Che cosa copre un'assicurazione cyber	47
15.2 Principali assicuratori in Svizzera	47
15.3 Punti a cui prestare attenzione	47
Capitolo 16. Cosa fare in caso di incidente	49

16.1 Scenario A: attacco in corso (ransomware, intrusione).....	49
16.2 Scenario B: perdita o fuga accidentale.....	49
16.3 Cosa fa concretamente l'IFPDT	49
Capitolo 17. Casi reali nella Svizzera romanda	50
Groupe 3R, Réseau Radiologique Romand (aprile 2025 e aprile 2026).....	50
Vidymed, Losanna (dicembre 2024)	50
La Svizzera in cifre	50
Scenari tipici di attacco nel settore medico	51
Ransomware tramite accesso remoto non protetto	51
Phishing con una falsa fattura di un operatore di telecomunicazioni	51
Usurpazione d'identità del fornitore IT	51
Chiavetta USB infetta	51
Quanto costa un attacco	51
Checklist di conformità.....	52
Comunicazioni	52
Infrastruttura	52
Backup.....	52
Accessi e autenticazione	52
Conformità nLPD	52
Protezione e monitoraggio.....	53
Lessico della checklist.....	54
Contatti e risorse utili	56
Contatti d'emergenza	56
Testi legali	56
Risorse complementari.....	56
Domande frequenti	57
Una perdita accidentale di dati è una violazione ai sensi della nLPD?	57
Il mio fornitore IT ha cancellato dei dati. Chi è responsabile?	57

Sono in pensione da 3 anni e viene scoperta una fuga di dati risalente a 4 anni fa. Sono ancora coinvolto?	57
I miei iMac con Windows 10 tramite Boot Camp: si può tornare a macOS?	57
Quale software dentale scegliere?	57
Un'assistente invia una radiografia tramite WhatsApp. Chi è responsabile?	58
L'IFPDT effettua controlli negli studi?	58
La nLPD impone un termine di 72 ore come il RGPD?	58
Glossario	59
Note legali e condizioni di utilizzo	62
Proprietà intellettuale	62
Utilizzo autorizzato	62
Utilizzi vietati	62
Limitazione di responsabilità	62

Introduzione

Questa guida si rivolge ai medici dentisti, ai responsabili di studio e ai loro team. È stata redatta in seguito alla conferenza organizzata dalla Società svizzera odontoiatri, sezione di Neuchâtel (SSO-NE), il 12 marzo 2026, dedicata alla cibersecurity e alla conformità alla nuova legge federale sulla protezione dei dati (nLPD).

La nLPD, entrata in vigore il 1° settembre 2023, impone agli studi dentistici obblighi concreti in materia di protezione dei dati dei pazienti. I dati sulla salute (radiografie, diagnosi, piani di trattamento) sono dati personali degni di particolare protezione ai sensi della legge, soggetti a regole più severe.

Il presente documento tratta tutti i temi affrontati durante la conferenza, approfonditi e completati da due argomenti supplementari: la formazione del personale e le assicurazioni cyber. È concepito come un'opera di riferimento duratura, da conservare e da consultare quotidianamente.

Informazioni su questa guida

Il presente documento è fornito a scopo informativo ed educativo. Non costituisce una consulenza legale. Per qualsiasi questione specifica alla vostra situazione, rivolgetevi a un giurista specializzato in protezione dei dati. Questa versione italiana è una traduzione; fa fede la versione francese.

Capitolo 1. Il quadro legale: la nLPD

1.1 Che cos'è la nLPD?

La nuova legge federale sulla protezione dei dati (nLPD, RS 235.1) è entrata in vigore il 1° settembre 2023. Sostituisce integralmente la vecchia legge del 1992, un'epoca in cui le cartelle dei pazienti erano ancora su carta e Internet non esisteva negli studi medici.

La nLPD modernizza il quadro giuridico svizzero per adeguarlo alle realtà digitali odierne. Si allinea agli standard europei del RGPD pur mantenendo specificità svizzere, in particolare in materia di sanzioni e di termini di notifica.

Punto essenziale: è il titolare dello studio (il medico dentista) a essere personalmente responsabile della protezione dei dati dei suoi pazienti. Non il fornitore di servizi informatici, non il software gestionale, non il fornitore di hosting cloud.

1.2 Quali dati sono interessati?

Uno studio dentistico tratta quotidianamente dati personali, molti dei quali sono dati personali degni di particolare protezione ai sensi dell'art. 5 lett. c LPD:

- Dati sulla salute: radiografie panoramiche, radiografie periapicali, CBCT / scansioni 3D, foto intraorali ed extraorali, diagnosi, piani di trattamento, prescrizioni, anamnesi medica (allergie, malattie croniche, trattamenti in corso), referti operatori, note cliniche, cronologia completa delle cure, corrispondenza medica con altri professionisti, laboratori o specialisti
- Impronte e modelli digitali: impronte dentali digitali, impronte ottiche ottenute da scanner intraorali, modelli 3D digitali (dati sulla salute)
- Dati genetici: risultati di analisi genetiche, se la cartella ne contiene (art. 5 lett. c n. 3 LPD)
- Dati amministrativi: numeri AVS, date di nascita, recapiti, consensi firmati, dati assicurativi (LAMal, assicurazioni complementari); i questionari anamnestici, invece, sono dati sulla salute
- Dati finanziari: fatture, estratti assicurativi, modalità di pagamento, cronologia della fatturazione
- Corrispondenza: scambi con i pazienti via e-mail o messaggistica, scambi con le assicurazioni, buoni d'ordinazione ai laboratori odontotecnici contenenti dati dei pazienti

I dati personali degni di particolare protezione sono soggetti a regole più severe e richiedono misure di sicurezza rafforzate; lo studio e il suo personale sono inoltre tenuti al segreto professionale (art. 321 CP).

1.3 I tre obblighi fondamentali

1. Sapere dove si trovano i vostri dati e come sono protetti. Sul server dello studio, su un portatile che la sera torna a casa, in un software cloud di cui ignorate dove si trovino i server, nella vostra posta elettronica non crittografata, su una chiavetta USB in un cassetto, in un vecchio disco rigido mai cancellato, sul telefono personale di un'assistente, nelle e-mail inviate a un laboratorio tramite Gmail, nei backup che nessuno verifica da mesi. Spesso questi dati sono protetti da una password Windows «1234», da un antivirus gratuito scaduto, o da nulla.
2. Notificare le violazioni all'IFPDT in caso di incidente. L'art. 24 LPD impone al titolare del trattamento di notificare quanto prima ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. La notifica deve indicare almeno la natura della violazione, le sue conseguenze e i provvedimenti adottati o previsti (art. 24 cpv. 2). Il responsabile del trattamento (ad esempio il vostro fornitore IT) deve notificarvi quanto prima ogni violazione, qualunque ne sia la gravità (art. 24 cpv. 3). Se la protezione dei pazienti lo esige, o se l'IFPDT lo richiede, dovete anche informare direttamente le persone interessate (art. 24 cpv. 4).
3. Poter dimostrare la vostra conformità. In caso di inchiesta, l'IFPDT può chiedervi di provare di aver adottato i provvedimenti tecnici e organizzativi necessari (art. 8 e 49 cpv. 3 LPD). Concretamente, ciò significa disporre di una documentazione aggiornata: registro delle attività di trattamento, contratto con il responsabile del trattamento firmato dal vostro fornitore IT, politica interna di sicurezza, prova della formazione del personale, procedura di risposta agli incidenti, registro dei backup e dei relativi test di ripristino. L'assenza di documentazione non comporta necessariamente una sanzione, ma rende la vostra posizione indifendibile in caso di incidente.

1.4 Notifica delle violazioni (art. 24 LPD)

La legge svizzera impone una notifica «quanto prima», una formulazione volutamente flessibile, a differenza del RGPD europeo, che fissa un termine rigido di 72 ore. L'IFPDT raccomanda di agire il più rapidamente possibile dopo la scoperta della violazione.

Il portale ufficiale di notifica è accessibile all'indirizzo databreach.edoeb.admin.ch. Con il consenso del titolare del trattamento, l'IFPDT può trasmettere la notifica all'Ufficio federale della ciblesicurezza (UFCS) per l'analisi dell'incidente.

Importante

Una notifica effettuata in virtù dell'art. 24 non può essere utilizzata contro la persona che l'ha effettuata in un procedimento penale, salvo con il suo consenso (art. 24 cpv. 6 LPD). Notificare non vi espone. Non notificare, invece, sì.

1.5 Diritti dei pazienti (art. 25 LPD)

Ogni paziente può domandare allo studio se vengono trattati dati personali che lo riguardano. Lo studio deve allora fornire, entro 30 giorni e gratuitamente:

- L'identità e i dati di contatto del titolare del trattamento
- I dati personali trattati in quanto tali
- Lo scopo del trattamento
- La durata di conservazione o i criteri per determinarla
- La provenienza dei dati, se non sono stati raccolti presso il paziente
- L'eventuale esistenza di una decisione individuale automatizzata e la logica su cui si basa
- I destinatari a cui sono comunicati dati, anche all'estero

Comunicazione dei dati sulla salute (art. 25 cpv. 3)

I dati sulla salute possono essere comunicati al paziente, con il suo consenso, per il tramite di un professionista della salute da lui designato. Questa disposizione protegge il paziente da informazioni mediche difficili da interpretare senza accompagnamento.

Responsabilità in caso di ricorso a un responsabile del trattamento (art. 25 cpv. 4)

Se lo studio si avvale di un responsabile del trattamento (fornitore di hosting dei dati, fornitore di servizi informatici), lo studio resta tenuto a fornire le informazioni al paziente. Non potete rinviare il paziente al vostro fornitore IT.

Carattere imperativo del diritto d'accesso (art. 25 cpv. 5)

Nessun paziente può rinunciare preventivamente al proprio diritto d'accesso. Qualsiasi clausola contrattuale in tal senso è nulla e priva di effetti.

Gratuità e termine (art. 25 cpv. 6 e 7)

Le informazioni sono fornite gratuitamente, entro 30 giorni. Se è impossibile rispettare questo termine (complessità, volume dei dati), il titolare del trattamento deve informare il paziente e motivare la proroga.

Rimedi del paziente in caso di inosservanza

Se lo studio rifiuta di rispondere o non rispetta i termini, il paziente dispone di diversi rimedi:

- Sollecito allo studio con lettera raccomandata

- Denuncia all'IFPDT
- Azione civile davanti al tribunale (art. 32 LPD)
- Querela penale se le informazioni fornite sono intenzionalmente false (art. 60 LPD)

Attenzione alle formulazioni ambigue

Un giurista d'impresa è stato condannato a una multa di CHF 600 nel marzo 2025 (Statthalteramt Bezirk Zürich, decisione ST.2024.1046/ZM) per aver risposto che una società «non aveva trovato alcun dato» mentre in realtà ne deteneva. La formulazione fuorviante bastava a configurare l'infrazione. Anche una risposta parzialmente esatta ma che dà una falsa impressione di completezza può essere sanzionata.

1.6 Registro delle attività di trattamento (art. 12 LPD)

In linea di principio, ogni titolare del trattamento tiene un registro delle proprie attività di trattamento (art. 12 cpv. 1 LPD). Le imprese con meno di 250 collaboratori ne sono esentate, ma l'esenzione decade se trattano dati personali degni di particolare protezione su vasta scala o effettuano una profilazione a rischio elevato (art. 12 cpv. 5 LPD e art. 24 OPDa). Ora, uno studio dentistico tratta per natura dati sulla salute, che sono dati degni di particolare protezione: a seconda del numero di pazienti e del volume dei dati, l'esenzione può quindi non applicarsi. In ogni caso, è vivamente raccomandato tenerne uno, anche per le piccole strutture.

Il registro deve contenere almeno: l'identità del titolare del trattamento, lo scopo dei trattamenti, le categorie di persone e di dati interessati, i destinatari, le durate di conservazione e una descrizione delle misure di sicurezza in atto.

1.7 Sanzioni (art. 60–66 LPD)

Le violazioni intenzionali della nLPD sono punibili con multe fino a CHF 250'000. Queste sanzioni colpiscono le persone fisiche responsabili, e non l'impresa. In uno studio dentistico, è il titolare dello studio a essere direttamente interessato.

Infrazione	Multa massima	Condizione
Informazioni intenzionalmente inesatte o incomplete	CHF 250'000	A querela di parte
Omissione intenzionale di informare la persona interessata	CHF 250'000	A querela di parte
Ricorso a un responsabile del trattamento senza contratto o senza verifica della sicurezza dei dati (art. 9)	CHF 250'000	A querela di parte
Comunicazione di dati all'estero senza garanzie	CHF 250'000	A querela di parte
Informazioni inesatte all'IFPDT durante un'inchiesta	CHF 250'000	D'ufficio
Rifiuto di collaborare con l'IFPDT	CHF 250'000	D'ufficio

Termine di prescrizione: 5 anni (art. 66 LPD). Il pensionamento o la cessazione dell'attività non elimina la responsabilità per fatti commessi durante l'esercizio della professione.

Solo le violazioni intenzionali sono punibili penalmente

La negligenza non è sanzionata penalmente dalla nLPD, ma può dar luogo ad azioni civili da parte dei pazienti danneggiati. La buona fede e la reattività sono sempre fattori attenuanti.

1.8 Differenze principali rispetto al vecchio diritto (LPD 1992)

La nLPD del 2023 costituisce una revisione totale della legge del 1992. Ecco le principali differenze:

Vecchia LPD (1992)	Nuova LPD (2023)
Protegge persone fisiche e giuridiche	Protegge unicamente le persone fisiche
Nessun obbligo di notifica	Notifica obbligatoria all'IFPDT in caso di violazione a rischio elevato
Multe limitate e rare	Multe fino a CHF 250'000 (responsabilità individuale)
Nessun obbligo di valutazione d'impatto	Valutazione d'impatto obbligatoria per i trattamenti a rischio elevato
Registro dei trattamenti facoltativo	Registro obbligatorio (salvo eccezioni limitate)
Nessuna Privacy by Design	Privacy by Design e Privacy by Default obbligatorie (art. 7)
Dati biometrici non protetti specificamente	Dati biometrici e genetici inclusi nei dati degni di particolare protezione

1.9 Privacy by Design e Privacy by Default (art. 7 LPD)

L'art. 7 impone due principi fondamentali che devono guidare ogni decisione informatica nello studio:

Privacy by Design (protezione dei dati sin dalla progettazione): le misure di protezione dei dati devono essere integrate fin dalla scelta di un software, di un'apparecchiatura o di un processo. Non si tratta di correggere a posteriori, ma di prevedere la sicurezza fin dall'inizio.

Privacy by Default (protezione dei dati per impostazione predefinita): le impostazioni predefinite di qualsiasi sistema devono limitare il trattamento dei dati allo stretto necessario. Un software dentale non dovrebbe, per impostazione predefinita, condividere i dati dei pazienti con terzi o memorizzare più informazioni del necessario.

In pratica, questi principi si applicano nella scelta di un software gestionale, nella configurazione di una rete, nell'allestimento di una nuova postazione di lavoro o nell'adozione di uno strumento cloud. In ogni decisione occorre porsi la domanda: «questa soluzione protegge i dati dei pazienti per impostazione predefinita?»

1.10 Valutazione d'impatto sulla protezione dei dati (art. 22 LPD)

La valutazione d'impatto sulla protezione dei dati (VIPD) è obbligatoria quando un trattamento previsto può comportare un rischio elevato per i diritti delle persone interessate. L'esistenza di un rischio elevato dipende dalla natura, dall'estensione, dalle circostanze e dallo scopo del trattamento.

Esempi che richiedono una VIPD

- Introduzione di un sistema di riconoscimento facciale nello studio
- Profilazione su vasta scala dei pazienti
- Trattamento massiccio di dati sulla salute con l'intelligenza artificiale
- Videosorveglianza estesa dello studio

Contenuto della valutazione d'impatto

La VIPD deve contenere una descrizione del trattamento previsto, una valutazione dei rischi per i diritti delle persone interessate e le misure previste per proteggere tali diritti. Se, nonostante le misure previste, il rischio rimane elevato, il titolare del trattamento deve consultare l'IFPDT prima del trattamento (art. 23 LPD).

In pratica per uno studio dentistico

La maggior parte degli studi dentistici non avrà bisogno di effettuare una VIPD nella propria attività corrente. Per contro, l'introduzione di un nuovo software che tratta dati dei pazienti su vasta scala, di uno strumento di IA per l'analisi delle radiografie o di un sistema biometrico di controllo degli accessi potrebbe far scattare questo obbligo.

1.11 Giurisprudenza recente

Benché la nLPD sia ancora recente, le prime decisioni cominciano a delinearne l'applicazione pratica.

Statthalteramt Bezirk Zürich, marzo 2025 (ST.2024.1046/ZM)

Un giurista d'impresa è stato condannato a una multa di CHF 600 per aver risposto a una richiesta d'accesso affermando che una società «non aveva trovato alcun dato» mentre in realtà ne deteneva. La formulazione fuorviante bastava a configurare l'infrazione ai sensi dell'art. 60 cpv. 1 lett. a LPD.

Questo caso dimostra che anche una risposta parzialmente esatta ma che dà una falsa impressione di completezza può essere sanzionata. Per uno studio dentistico, ciò significa

che la richiesta d'accesso di un paziente deve ricevere una risposta completa, precisa e verificabile entro 30 giorni.

1.12 Buone pratiche per la gestione delle richieste d'accesso

- Rispondere sempre entro 30 giorni
- Fornire una risposta completa fin dalla prima volta
- Evitare le formulazioni ambigue (non rispondere mai «non abbiamo trovato nulla» se esistono dati)
- Documentare ogni richiesta e ogni risposta in un registro interno
- Formare il personale a trattare correttamente queste richieste
- Designare una persona incaricata della gestione delle richieste d'accesso
- Verificare l'identità del richiedente prima di qualsiasi comunicazione di dati

Capitolo 2. Posta elettronica sicura

L'invio di dati dei pazienti via e-mail è una delle pratiche più comuni, e più rischiose, negli studi dentistici. Una radiografia inviata tramite Gmail, Bluewin o Hotmail transita senza crittografia end-to-end, su server spesso situati fuori dalla Svizzera.

2.1 Il problema

I servizi di posta elettronica destinati al grande pubblico non sono concepiti per i dati medici:

- **Gmail / Hotmail / Yahoo:** server fuori dalla Svizzera, nessuna crittografia end-to-end. Doppiamente non conforme.
- **Bluewin:** server in Svizzera, ma nessuna crittografia end-to-end. Swisscom può tecnicamente accedere al contenuto. Insufficiente per dati medici.
- **Infomaniak Mail:** meglio protetto di Gmail, ma senza crittografia end-to-end nativa. Adatto agli scambi interni non sensibili, non ai dati dei pazienti.

2.2 Le soluzioni conformi

- **HIN Mail:** il riferimento nel settore medico svizzero. Comunicazione sicura tra professionisti della salute, compatibile con la rete nazionale HIN. Soluzione ideale per gli scambi con medici, laboratori e specialisti.
- **Proton:** fondata nel 2014 al CERN di Ginevra da scienziati e ingegneri preoccupati per la sorveglianza di massa rivelata da Edward Snowden. L'obiettivo fondante era creare strumenti di comunicazione che nessuno, nemmeno Proton, potesse leggere. L'azienda ha sede a Ginevra ed è soggetta al diritto svizzero, una delle legislazioni più severe al mondo in materia di tutela della sfera privata. Secondo la sua informativa sulla privacy, i dati sono ospitati su server situati esclusivamente in Svizzera, in Germania o in Norvegia; la Germania e la Norvegia sono riconosciute dal Consiglio federale come Stati che offrono un livello di protezione adeguato (allegato 1 OPDa).

Proton non si limita alla posta elettronica. L'ecosistema completo comprende

ProtonMail (posta elettronica crittografata, end-to-end tra utenti Proton), **Proton**

Drive (archiviazione cloud crittografata, alternativa conforme a Google Drive o Dropbox), **Proton Pass** (gestore di password crittografato), **Proton VPN** (rete privata virtuale per proteggere le connessioni remote) e **Proton Calendar** (agenda crittografata). Per uno studio dentistico, questo ecosistema permette di coprire diverse esigenze con un'unica soluzione: posta elettronica sicura per gli scambi con pazienti e fornitori al di fuori della rete HIN, archiviazione cloud per i documenti amministrativi sensibili, gestore di password per il team, e VPN. La crittografia end-to-end è automatica solo tra utenti Proton: verso un indirizzo che non è presso Proton (un laboratorio, un paziente), il messaggio è crittografato end-to-end solo se si sceglie l'e-mail protetta da password, che il destinatario deve inserire per aprirlo (il messaggio scade al più tardi dopo 28 giorni). Proton applica una politica di accesso zero (zero-access): non può decrittografare il contenuto crittografato end-to-end, nemmeno su richiesta di un'autorità. Può invece essere obbligata dalle autorità svizzere competenti a consegnare i dati in suo possesso, in particolare i metadati: indirizzi del mittente e dei destinatari, oggetto dei messaggi, date e ore di invio e di ricezione.

Regola pratica

Se il contenuto dell'e-mail comprende una radiografia, una diagnosi, un numero AVS o qualsiasi altro dato identificabile di un paziente, deve transitare tramite una posta elettronica crittografata end-to-end. Senza eccezioni.

Capitolo 3. Aggiornamenti

Gli aggiornamenti correggono le falle di sicurezza e impediscono la maggior parte degli attacchi più comuni. Un sistema non aggiornato è un sistema vulnerabile. Ogni giorno che passa senza correzione è una porta aperta in più per gli aggressori.

3.1 Sistema operativo

Windows e macOS devono assolutamente essere mantenuti aggiornati. Il supporto di Windows 10 è terminato nell'ottobre 2025: le falle scoperte dopo questa data non sono più corrette da Microsoft, salvo sui computer iscritti al programma a pagamento di aggiornamenti di sicurezza estesi (ESU).

Per una postazione di lavoro, Windows 11 è oggi l'unica versione di Windows che riceve ancora correzioni di sicurezza senza particolari accorgimenti. Le eccezioni sono limitate: il programma ESU prolunga Windows 10 di tre anni al massimo per le imprese (fino all'ottobre 2028), a un prezzo che raddoppia ogni anno; alcune edizioni specializzate Windows 10 LTSC, riservate alle imprese e ai dispositivi dedicati, restano supportate fino al 2027, 2029 o 2032 a seconda dell'edizione; i server seguono un proprio calendario (Windows Server). Sono soluzioni transitorie, non un'alternativa duratura: ogni computer con Windows 7, 8 o 10 deve essere sostituito o migrato.

3.2 Applicazioni e software gestionali

I software dentali, qualunque sia la soluzione utilizzata nel vostro studio, devono essere aggiornati regolarmente. Una versione vecchia può contenere falle sfruttabili o provocare corruzioni dei dati. Ciò riguarda sia i software di gestione dello studio sia i software di imaging e di radiologia.

Anche i browser web, i lettori PDF e le suite per ufficio devono essere mantenuti aggiornati. Sono vettori di attacco frequenti e spesso trascurati.

Verificate presso il produttore del vostro software che la versione installata sia ancora supportata e riceva correzioni di sicurezza. Se non è più così, pianificate la migrazione verso una versione recente o una soluzione alternativa.

Buona pratica

Attivate gli aggiornamenti automatici su tutti i computer. Pianificate un riavvio settimanale per consentire l'installazione delle correzioni in sospeso. Un computer mai riavviato accumula falle di sicurezza non corrette.

Capitolo 4. Backup

Il backup è la vostra ultima linea di difesa. In caso di ransomware, di errore umano o di guasto hardware, è il backup a determinare se perdete tutto o se riprendete l'attività in poche ore.

4.1 La regola 3-2-1

3 copie dei vostri dati (l'originale e due backup), su 2 supporti diversi, di cui 1 conservata fuori dallo studio, in un altro luogo, affinché un incendio, un danno causato dall'acqua o un furto non distruggano tutte le copie contemporaneamente. È la regola raccomandata dall'Ufficio federale della cibersecurity (UFCS). Si raccomanda inoltre che una delle copie sia scollegata o immutabile: una versione che nessuno può modificare o cancellare, nemmeno un ransomware (variante 3-2-1-1-0, vedi sotto).

La copia immutabile non significa necessariamente un disco rigido da scollegare ogni sera. Tecnologie come gli snapshot automatici, l'archiviazione cloud con conservazione immutabile o i backup con versioni permettono di proteggere i dati senza un intervento umano quotidiano. Il vostro fornitore di servizi informatici deve essere in grado di proporvi e di mettere in atto un sistema di backup adatto al vostro studio, conforme alla regola 3-2-1 e documentato per iscritto. Non spetta al medico dentista progettare l'architettura di backup; spetta invece a lui assicurarsi che esista, che funzioni e che venga testata.

Un esempio concreto di attuazione: il server dello studio conserva i dati di lavoro (copia 1), un backup automatico viene replicato su un NAS o su un disco dedicato nello studio (copia 2), e una terza copia viene inviata ogni notte verso un'archiviazione cloud sicura in Svizzera con conservazione immutabile (copia 3). Se un ransomware crittografa le prime due copie, la terza rimane intatta e consente un ripristino completo.

La soluzione può essere personalizzata secondo le dimensioni dello studio e il volume dei dati. Alcuni fornitori applicano la regola 3-2-1-1-0, che aggiunge alla regola di base una copia offline o immutabile (il secondo «1») e mira a zero errori nei test di ripristino (lo «0»). L'importante non è la complessità del sistema, ma la garanzia che i dati dei vostri pazienti possano essere recuperati in caso di sinistro, in tempi compatibili con la continuità della vostra attività.

Se il vostro attuale fornitore IT non è in grado di spiegarvi chiaramente la vostra strategia di backup, dove si trovano le vostre copie, se una di esse è conservata fuori dallo studio, se una copia è scollegata o immutabile e quando sono state testate l'ultima volta, è un segnale d'allarme.

4.2 Perché la copia immutabile è essenziale

I ransomware moderni individuano e crittografano tutti i backup collegati alla rete. Anche un disco rigido esterno collegato in permanenza verrà crittografato durante l'attacco. Solo una copia fisicamente scollegata o logicamente isolata (versioning immutabile) resterà intatta.

4.3 Testare il ripristino

Un backup non testato è un'illusione di sicurezza

Testate regolarmente il ripristino effettivo di un campione di dati, ad esempio alcune cartelle dei pazienti o alcune radiografie. Le raccomandazioni della SSO e della FMH chiedono un test almeno una volta all'anno; un test ogni mese è una buona pratica, che permette di scoprire prima un problema. Verificate che i file si aprano correttamente e che i dati siano utilizzabili. Senza test regolari, scoprirete troppo tardi che i vostri backup sono corrotti o incompleti.

Capitolo 5. Password e autenticazione a due fattori

5.1 Il problema delle password deboli

Una password come «1234», il nome dello studio o una data di nascita si indovina in pochi secondi. Un account condiviso da tutto il team impedisce qualsiasi tracciabilità in caso di incidente. Senza autenticazione a due fattori, una sola password resta l'unica barriera tra un aggressore e i dati dei vostri pazienti.

5.2 Creare una password robusta

Almeno 12 caratteri, combinando maiuscole, minuscole, cifre e simboli. Un metodo concreto: scegliete due parole senza alcun legame logico, aggiungete un numero facile da ricordare e caratteri speciali consecutivi sulla tastiera.

Esempio

CarmolTroppen91()=. Facile da ricordare, nessun legame con il vostro studio o con voi stessi.

5.3 Usare un gestore di password

Un gestore di password conserva tutte le vostre credenziali in forma crittografata. Dovete ricordare una sola password principale.

- Proton Pass: crittografia end-to-end, server in Svizzera, in Germania o in Norvegia
- Bitwarden: open source, installabile sui propri server
- KeePass: archiviazione locale, nessun cloud

5.4 Autenticazione a due fattori (2FA)

La 2FA aggiunge una seconda verifica dopo la password: un codice temporaneo sul vostro telefono, una notifica push o una chiave fisica. Anche se la vostra password è compromessa, l'aggressore non può accedere all'account senza questo secondo fattore.

Da attivare su: posta elettronica professionale, software dentale (se disponibile), backup cloud, accesso remoto, conti bancari.

Capitolo 6. Crittografia dei dischi e degli archivi

6.1 Crittografia delle postazioni di lavoro

Un portatile rubato da un'auto o un server portato via durante un furto con scasso danno accesso immediato a tutti i dati se il disco non è crittografato. La crittografia rende i dati totalmente illeggibili senza la chiave di decrittografia.

- **Windows:** BitLocker, integrato in Windows Pro ed Enterprise, gratuito. Da attivare su tutti i computer.
- **macOS:** FileVault, integrato, gratuito. Da attivare nelle impostazioni di sistema.
- **Server:** crittografia hardware (TPM), BitLocker o software a seconda dell'infrastruttura.

6.2 Contenitori crittografati per archivi sensibili

Per i dischi esterni contenenti archivi dei pazienti, la contabilità o vecchi backup, un contenitore crittografato funziona come una cassaforte digitale: accessibile solo con una password robusta.

- **Windows:** BitLocker To Go (dischi esterni), VeraCrypt (contenitori crittografati)
- **macOS:** FileVault per dischi esterni
- **Multipiattaforma:** VeraCrypt: open source, robusto, gratuito

Capitolo 7. Rete Wi-Fi

Un'unica rete Wi-Fi condivisa tra il personale, le apparecchiature mediche e i pazienti è una grave falla di sicurezza. Senza separazione, un telefono infetto collegato alla rete ospiti può raggiungere il server dello studio.

7.1 La configurazione raccomandata: tre reti separate

- **Rete principale:** postazioni di lavoro, server, stampanti; isolata e protetta.
- **Rete medica:** apparecchi di radiologia, sensori, apparecchiature connesse, se necessario secondo l'infrastruttura.
- **Rete ospiti:** pazienti. Solo accesso a Internet, nessuna visibilità sulla rete interna dello studio.

La separazione delle reti è l'equivalente digitale della parete tra la sala d'attesa e la sala di cura. Il protocollo WPA3 è raccomandato se l'hardware lo supporta; WPA2 è il minimo accettabile.

Password Wi-Fi

Non esporre mai la password della rete principale in sala d'attesa. La rete ospiti può utilizzare un captive portal con un codice giornaliero o un codice unico consegnato su richiesta.

Capitolo 8. Accesso remoto sicuro

Gli strumenti di accesso remoto sono indispensabili per la teleassistenza informatica ma, se configurati male, rappresentano una delle principali porte d'ingresso per gli aggressori.

8.1 Il rischio delle versioni gratuite sempre in standby

Scenario tipico: uno strumento di controllo remoto, lasciato sempre in standby con una password debole, permette a un aggressore di entrare nello studio durante la notte e di installarvi un ransomware. Lo studio perde diversi giorni di attività, e solo i dati salvati in un luogo fuori portata possono essere recuperati.

Lasciare TeamViewer, AnyDesk o un altro strumento di accesso remoto attivo 24 ore su 24 senza una sicurezza rafforzata equivale a lasciare una porta del vostro studio sempre aperta.

8.2 Soluzioni raccomandate

Soluzione	Uso	Sicurezza	Raccomandazione
TeamViewer / AnyDesk gratuito	Occasionale	Bassa	Da evitare per i dati medici
TeamViewer Pro + 2FA	Ad hoc	Adeguate	Accettabile se ben configurato
VPN professionale	Permanente	Elevata	WireGuard o OpenVPN raccomandato
RMM aziendale	Teleassistenza	Molto elevata	NinjaOne, Datto, Atera

Regola d'oro

Nessun accesso remoto deve essere configurato come accesso libero permanente. Ogni connessione deve essere tracciata, autenticata e limitata nel tempo. Più il livello di privilegio è elevato (accesso al server, dati dei pazienti), più la soluzione deve essere sicura.

Capitolo 9. Phishing

Il phishing resta il vettore di attacco più comune contro gli studi medici. L'aggressore si fa passare per un contatto di fiducia (Swisscom, la vostra banca, il vostro fornitore IT) per ottenere credenziali o far aprire un file infetto.

9.1 Riconoscere un'e-mail di phishing

- Indirizzo del mittente sospetto (dominio insolito, errori di ortografia)
- Urgenza artificiale: «Il vostro account sarà bloccato entro 24 ore»
- Richiesta di cliccare su un link o di aprire un allegato inatteso
- Errori di ortografia o formulazione insolita
- Richiesta di credenziali, password o dati bancari

9.2 Protezione avanzata: il filtraggio tramite etichette

Le e-mail provenienti da mittenti abituali e di fiducia possono essere filtrate ed etichettate automaticamente. Qualsiasi e-mail che afferma di provenire da uno di questi contatti ma non è riconosciuta dal filtro deve destare immediatamente sospetti.

Questa configurazione è possibile tramite regole di filtraggio integrate nella vostra posta elettronica o tramite soluzioni anti-phishing professionali. Se optate per uno strumento di terzi per il filtraggio delle e-mail, verificate assolutamente dove si trovano i server che analizzano il contenuto dei vostri messaggi.

Una soluzione che fa transitare le vostre e-mail su server situati fuori dalla Svizzera può essere problematica alla luce dell'art. 16 LPD, in particolare se queste e-mail contengono dati dei pazienti. Privilegiate soluzioni il cui trattamento dei dati avviene in Svizzera o, in mancanza, in uno Stato riconosciuto dal Consiglio federale come Stato che offre un livello di protezione adeguato. Il vostro fornitore di servizi informatici deve essere in grado di confermarvi l'ubicazione dei server e le garanzie di protezione applicabili.

Capitolo 10. Gestione degli accessi degli utenti

Definire chi può accedere a cosa riduce fortemente i rischi interni e limita i danni in caso di compromissione di un account.

10.1 Principio del privilegio minimo

Ogni utente deve avere accesso solo ai dati strettamente necessari alla sua funzione. Questo principio, ampiamente riconosciuto nella sicurezza informatica, è direttamente legato all'art. 8 LPD, che impone provvedimenti organizzativi adeguati per garantire la sicurezza dei dati.

In uno studio dentistico, i ruoli sono chiaramente distinti e gli accessi devono rispecchiare questa realtà. Un'assistente dentale deve poter consultare le cartelle dei pazienti e fissare appuntamenti, ma non ha bisogno di accedere alla contabilità dello studio, ai dati del personale o alle impostazioni di amministrazione del server. Un igienista dentale ha bisogno della cronologia delle cure dei suoi pazienti, non delle fatture non pagate. Un contabile esterno ha bisogno dei dati finanziari, non delle radiografie.

In caso di compromissione di un account (phishing riuscito, password rubata), il principio del privilegio minimo limita i danni: l'aggressore può accedere solo ai dati autorizzati per quell'account. Se tutti condividono le stesse credenziali con accesso completo, una sola compromissione espone l'intero studio.

10.2 Regole di gestione degli account

Un account per persona, mai un account condiviso. Gli account generici come «studio», «admin», «ricezione» o «contabilità» impediscono qualsiasi tracciabilità. In caso di incidente, è impossibile stabilire chi ha compiuto quale azione e in quale momento. Ogni collaboratore deve disporre delle proprie credenziali, con una password personale che non condivide con nessuno.

Gli account di amministratore devono essere riservati alle operazioni tecniche (installazione di software, configurazione di rete, manutenzione) e non devono mai essere utilizzati per il lavoro quotidiano. Se il vostro fornitore IT utilizza un account di amministratore, tale account deve essere distinto da quelli del personale, protetto da un'autenticazione a due fattori e soggetto alla registrazione delle connessioni.

10.3 Gestione degli arrivi e delle partenze

L'arrivo di un nuovo collaboratore deve comportare la creazione di un account nominativo con diritti strettamente corrispondenti alla sua funzione. Il collaboratore deve ricevere una formazione sulle regole di utilizzo dei sistemi informatici dello studio, compresi la politica sulle password e i divieti (WhatsApp, chiavette USB personali, trasferimento di dati verso apparecchi non autorizzati).

La partenza di un collaboratore, volontaria o no, deve comportare la disattivazione immediata di tutti i suoi accessi: account utente, posta elettronica, software gestionale, accesso remoto, archiviazione cloud. Non rimandarla al giorno dopo, non posticiparla alla fine del mese. Un ex dipendente scontento che dispone ancora dei suoi accessi rappresenta un rischio reale, sia per la sicurezza dei dati sia per la responsabilità dello studio rispetto alla nLPD.

10.4 Verifica periodica dei diritti d'accesso

I diritti d'accesso non sono immutabili. Un collaboratore può cambiare funzione, uno stagista può terminare il suo stage, un fornitore esterno può smettere di intervenire. Senza verifiche regolari, gli accessi obsoleti si accumulano e creano falle invisibili.

Pianificate una verifica trimestrale: passate in rassegna l'elenco degli account attivi, verificate che ogni account corrisponda a una persona ancora in servizio, che i diritti attribuiti corrispondano alla funzione attuale e che tutti gli account inutilizzati siano disattivati.

Documentate questa verifica per iscritto: fa parte dei provvedimenti organizzativi che l'IFPDT può chiedere di consultare.

10.5 Strumenti che facilitano la gestione degli accessi

Alcune apparecchiature e tecnologie permettono di centralizzare e semplificare la gestione degli account e dei diritti d'accesso in uno studio. Un server NAS professionale (ad esempio di tipo Synology) offre una gestione degli utenti e delle cartelle condivise con autorizzazioni granulari: ogni collaboratore accede solo alle cartelle autorizzate per la sua funzione, con la registrazione delle connessioni e delle modifiche. È una soluzione adatta agli studi di piccole e medie dimensioni che non dispongono di un server dedicato.

Per gli studi che dispongono di un'infrastruttura Windows più avanzata, una directory centralizzata come Active Directory permette di gestire tutti gli account, le password, i gruppi di sicurezza e i criteri di accesso da un unico punto. Facilita la creazione e la soppressione degli account, l'applicazione automatica delle regole di sicurezza (complessità delle password, blocco dopo tentativi falliti, scadenza delle sessioni) e la limitazione degli accessi per gruppo funzionale (medici dentisti, assistenti, contabilità, amministrazione). Il vostro fornitore di servizi informatici deve essere in grado di consigliarvi la soluzione più adatta alle dimensioni e all'organizzazione del vostro studio.

Capitolo 11. Malware polimorfici e protezione EDR

Un malware polimorfico è un programma dannoso capace di modificare il proprio codice a ogni infezione per non essere riconosciuto dagli antivirus classici. Non è una minaccia nuova; queste tecniche esistono dagli anni '90, ma l'intelligenza artificiale ne ha notevolmente accelerato la sofisticazione. Ciò che richiedeva settimane di sviluppo a un aggressore si genera ormai in pochi minuti.

11.1 Perché l'antivirus classico non basta più

Un antivirus tradizionale funziona tramite firme: confronta ogni file con una banca dati di minacce conosciute. Se il malware cambia forma a ogni infezione, non viene mai riconosciuto. È come una guardia di sicurezza che riconosce solo i criminali schedati. Se il criminale cambia volto, passa inosservato.

Questo modello di rilevamento resta utile contro le minacce conosciute e ampiamente diffuse, ma è insufficiente contro gli attacchi mirati o i malware recenti che non sono mai stati catalogati. Ora, è proprio questo tipo di attacco a colpire gli studi medici: ransomware installati su misura, spesso dopo una fase di ricognizione della rete della vittima.

11.2 La soluzione: l'EDR (Endpoint Detection and Response)

Un EDR non cerca un volto conosciuto; osserva un comportamento. Se un programma comincia ad aprire in massa i file dei pazienti e a crittografarli uno per uno, l'EDR lo rileva, lo blocca e lo mette in quarantena in tempo reale, prima che abbia terminato. Poco importa l'aspetto del programma o se sia già stato catalogato.

Oltre al rilevamento comportamentale, un EDR offre funzionalità che l'antivirus classico non possiede: isolamento automatico del computer compromesso per evitare la propagazione al resto della rete, registrazione completa dell'incidente (quali file sono stati toccati, a che ora, da quale processo), possibilità di ripristinare i file modificati (rollback) e allarmi in tempo reale destinati al vostro fornitore di servizi informatici.

Tra le soluzioni EDR riconosciute sul mercato figurano SentinelOne, CrowdStrike, Sophos Intercept X, Microsoft Defender for Endpoint o ancora ESET Inspect. Ciascuna propone livelli di funzionalità e di prezzo diversi; la scelta va fatta d'intesa con il vostro fornitore di servizi informatici in funzione delle dimensioni del vostro studio e della vostra infrastruttura esistente.

11.3 EDR, EPP, antivirus: capire le differenze

Un antivirus classico rileva le minacce conosciute tramite firme. Un EPP (Endpoint Protection Platform) combina l'antivirus con livelli supplementari: firewall locale, controllo delle periferiche USB, filtraggio web. Un EDR va oltre aggiungendo l'analisi comportamentale, la risposta automatizzata e la visibilità completa su ciò che accade su ogni computer. Per uno studio dentistico che tratta dati degni di particolare protezione, un EDR gestito dal vostro fornitore di servizi informatici è il livello di protezione raccomandato.

A titolo di esempio, un antivirus classico come Windows Defender (incluso gratuitamente in Windows) offre una protezione di base tramite firme. Un EPP come Bitdefender GravityZone o ESET Protect aggiunge livelli di prevenzione supplementari. Un EDR come SentinelOne o CrowdStrike Falcon aggiunge il rilevamento comportamentale e la risposta automatizzata. Il costo aumenta con il livello di protezione, ma le conseguenze finanziarie di un attacco riuscito superano di gran lunga l'investimento in una soluzione adeguata.

11.4 Il ruolo del fornitore di servizi informatici

Un EDR non si configura da solo. Richiede una parametrizzazione adatta al vostro ambiente (esclusione dei software dentali legittimi, soglie di allarme, politica di risposta automatica) e una sorveglianza regolare degli allarmi generati.

Il vostro fornitore di servizi informatici deve essere in grado di installare, configurare e supervisionare questa soluzione. Chiedetegli se utilizza un EDR sui computer che gestisce, se riceve gli allarmi in tempo reale e qual è il suo tempo di reazione in caso di rilevamento di una minaccia attiva. Se il vostro fornitore si limita a installare un antivirus gratuito senza supervisione, il livello di protezione è insufficiente per dati medici soggetti alla nLPD.

Capitolo 12. Modernizzazione del parco informatico

Non lasciare mai una o due vecchie postazioni di lavoro in uno studio moderno. Un solo computer obsoleto o non aggiornato basta a compromettere tutta la rete. In uno studio dentistico, ciò significa un rischio reale di fuga di dati o di riscatto riguardante radiografie, diagnosi, dati amministrativi o contabili. Basta un solo anello debole per mettere in pericolo l'intero studio.

12.1 Perché un computer obsoleto è pericoloso

Un computer Windows superato o mai riavviato accumula falle di sicurezza note e documentate pubblicamente. Gli aggressori dispongono di banche dati che elencano queste falle e di strumenti automatizzati per sfruttarle. Se una di esse viene sfruttata, la catena di attacco è prevedibile: ottenere un accesso iniziale alla rete locale tramite il computer vulnerabile, aggirare le protezioni dei computer recenti spostandosi lateralmente nella rete, raggiungere il server di archiviazione, accedere al software gestionale o ai backup, quindi rubare o crittografare i dati sensibili. Tutto ciò può avvenire in poche ore, spesso di notte o nel fine settimana, quando nessuno sorveglia.

Il problema non riguarda soltanto le postazioni di lavoro visibili. Le apparecchiature spesso dimenticate sono altrettanto critiche: un vecchio server che funziona ancora «in attesa», una stampante di rete il cui firmware non è mai stato aggiornato, un router Wi-Fi di vecchia generazione, un NAS con un sistema operativo obsoleto. Ognuna di queste apparecchiature costituisce un potenziale punto d'ingresso.

12.2 Ciclo di rinnovo raccomandato

La regola pratica è rinnovare le postazioni di lavoro al massimo ogni 5 anni. Questo termine non è arbitrario: corrisponde alla durata media durante la quale un produttore garantisce la compatibilità con gli aggiornamenti di sicurezza del sistema operativo e dei componenti hardware (driver, firmware, modulo TPM).

Ciò che conta davvero non è l'età del computer in sé, ma la sua capacità di ricevere gli ultimi aggiornamenti di sicurezza. Un computer di 4 anni compatibile con Windows 11 e dotato di un modulo TPM 2.0 è in uno stato di sicurezza migliore di un computer di 2 anni bloccato su un sistema a fine supporto.

Per una postazione di lavoro, Windows 11 è oggi l'unica versione di Windows supportata dal produttore senza particolari accorgimenti. Un computer con Windows 7 o 8 non riceve più alcuna correzione di sicurezza; un computer con Windows 10 ne riceve solo se è iscritto al programma a pagamento ESU (tre anni al massimo per le imprese, fino all'ottobre 2028) o se

utilizza un'edizione specializzata LTSC (vedi capitolo 3). Queste soluzioni non fanno che rinviare la scadenza. Mantenere sulla rete dello studio un computer che non riceve più correzioni equivale a lasciare una porta sempre aperta, qualunque sia il livello di protezione delle altre apparecchiature.

12.3 Caso particolare: iMac con Boot Camp

Alcuni studi utilizzano ancora iMac Intel con Windows installato tramite Boot Camp. Questa configurazione pone un doppio problema: spesso questi iMac non possono più passare né a Windows 11 (per l'assenza del modulo TPM 2.0), né alle ultime versioni di macOS (poiché Apple ha cessato il supporto dei modelli Intel più vecchi). Queste macchine si trovano a fine vita su entrambi i fronti contemporaneamente.

La soluzione è sostituirli con PC dedicati con Windows 11. I software gestionali e di imaging dentale funzionano esclusivamente con Windows; un Mac non offre quindi alcun vantaggio funzionale in questo contesto e complica la manutenzione, gli aggiornamenti e la compatibilità hardware.

12.4 Pianificare la migrazione

La sostituzione del parco informatico non deve avvenire d'urgenza il giorno in cui un computer si guasta o diventa il bersaglio di un attacco. Deve essere pianificata in anticipo, d'intesa con il vostro fornitore di servizi informatici. Ecco le tappe raccomandate:

Iniziate con un inventario completo del parco: ogni postazione di lavoro, ogni server, ogni apparecchiatura di rete, con il sistema operativo installato, la data di acquisto o di messa in servizio e la compatibilità con gli aggiornamenti attuali. Individuate i computer a fine vita o a fine supporto. Stabilite un calendario di sostituzione realistico, ripartito se necessario su più mesi per distribuire l'investimento. Prevedete la migrazione dei dati e dei software gestionali, la riconfigurazione degli accessi di rete e la verifica del corretto funzionamento di ogni computer prima della messa in produzione.

Documentate questo inventario e questo calendario per iscritto. Fanno parte dei provvedimenti organizzativi che dimostrano la vostra conformità all'art. 8 LPD.

12.5 Distruzione sicura delle vecchie apparecchiature

La sostituzione di un computer non si conclude con l'installazione di quello nuovo. La vecchia apparecchiatura contiene potenzialmente dati dei pazienti sul suo disco rigido, anche se pensate di aver cancellato tutto. Una semplice formattazione non basta: esistono strumenti di recupero che permettono di ritrovare dati cancellati in modo convenzionale.

Due opzioni conformi alla nLPD: la cancellazione sicura tramite software specializzato (sovrascrittura multipla dei dati che rende impossibile qualsiasi recupero) o la distruzione fisica del supporto di memoria (triturazione, smagnetizzazione). In entrambi i casi, chiedete un certificato di distruzione al vostro fornitore di servizi informatici e conservatelo nella vostra documentazione di conformità. Questo certificato costituisce la prova che i dati dei pazienti non sono stati abbandonati su un supporto non protetto.

Capitolo 13. Il contratto con il responsabile del trattamento (art. 9 LPD)

L'art. 9 LPD disciplina rigorosamente l'affidamento del trattamento di dati personali a un responsabile del trattamento. In pratica, ciò riguarda direttamente il rapporto tra uno studio dentistico e qualsiasi terzo che accede, memorizza, tratta o trasporta dati personali dei vostri pazienti per vostro conto.

Senza un contratto conforme con il responsabile del trattamento, potete comunque rivalervi sul fornitore secondo il Codice delle obbligazioni, ma è molto più difficile. E in caso di incidente siete voi, il titolare dello studio, a rispondere davanti all'IFPDT e davanti ai vostri pazienti. Chi affida intenzionalmente dati a un fornitore senza contratto, o senza verificare che garantisca la sicurezza dei dati, è punito, a querela di parte, con la multa fino a CHF 250'000 (art. 61 lett. b LPD).

13.1 Condizioni preliminari per affidare un trattamento

Prima ancora di redigere un contratto, l'art. 9 cpv. 1 pone due condizioni che il titolare del trattamento deve verificare. In primo luogo, il responsabile del trattamento può effettuare soltanto i trattamenti che lo studio stesso avrebbe il diritto di effettuare. Se un trattamento vi è vietato, non potete affidarlo a un terzo per aggirare il divieto. In secondo luogo, nessun obbligo legale o contrattuale di mantenere il segreto deve vietare l'affidamento del trattamento. Nel contesto medico, il segreto professionale (art. 321 del Codice penale) impone una particolare vigilanza sui dati a cui il responsabile del trattamento potrà realmente accedere.

L'art. 9 cpv. 2 aggiunge un obbligo attivo di verifica: il titolare del trattamento deve assicurarsi che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati. Non è una formalità. Dovete poter dimostrare di aver verificato le competenze, gli strumenti e le pratiche di sicurezza del vostro fornitore prima di concedergli l'accesso alla vostra infrastruttura.

13.2 Chi riguarda il contratto con il responsabile del trattamento?

Il contratto con il responsabile del trattamento non riguarda soltanto il vostro fornitore di servizi informatici. Ogni persona o impresa che accede a dati personali dei vostri pazienti per vostro conto è un responsabile del trattamento ai sensi della nLPD. Ecco i casi più frequenti in uno studio dentistico:

Il vostro fornitore di servizi informatici, che accede ai computer, ai server, ai backup e potenzialmente ai dati dei pazienti durante i suoi interventi di manutenzione. Il vostro fornitore di hosting cloud, se i vostri dati o backup sono memorizzati presso un fornitore esterno. Un laboratorio odontotecnico, se riceve file digitali contenenti dati identificabili dei pazienti

(impronte ottiche, radiografie con il nome del paziente). Un contabile o una fiduciaria esterni, se accedono ai dati di fatturazione contenenti informazioni sui pazienti. Un produttore di software dentale, se il software funziona in modalità cloud e i dati sono ospitati sui server del produttore.

Per ciascuno di questi responsabili del trattamento deve essere in vigore un contratto conforme all'art. 9 LPD.

13.3 Che cosa deve contenere il contratto

Il contratto deve definire chiaramente il quadro entro il quale il responsabile del trattamento è autorizzato a trattare i dati:

- La natura dei dati accessibili al responsabile del trattamento e le categorie di persone interessate (pazienti, personale, fornitori).
- Lo scopo del trattamento, limitato alle istruzioni dello studio. Il responsabile del trattamento non può utilizzare i dati per altri scopi, rivenderli o comunicarli a terzi senza previa istruzione del titolare del trattamento.
- L'elenco degli strumenti utilizzati e l'ubicazione dei server. Questo punto è direttamente legato all'art. 16 LPD: se gli strumenti del fornitore memorizzano o fanno transitare dati su server situati fuori dalla Svizzera, le garanzie di una protezione adeguata devono essere documentate nel contratto.
- Le misure di sicurezza tecniche e organizzative messe in atto dal responsabile del trattamento (crittografia, controllo degli accessi, registrazione dei log, antivirus o EDR).
- La procedura di notifica degli incidenti con un termine definito. L'art. 24 cpv. 3 LPD impone al responsabile del trattamento di informare quanto prima il titolare del trattamento in caso di violazione della sicurezza dei dati. Il contratto deve precisare un termine concreto, ad esempio 24 ore dopo il rilevamento.
- La procedura di fine contratto: soppressione di tutti gli accessi, restituzione o cancellazione dei dati detenuti, conferma scritta dell'esecuzione di queste misure.
- Il divieto di affidare il trattamento a terzi senza la previa autorizzazione dello studio (art. 9 cpv. 3 LPD), possibilmente data per scritto. Se il vostro fornitore di servizi informatici si avvale a sua volta di altri responsabili del trattamento (ad esempio un fornitore di hosting cloud per i vostri backup), ciò deve essere dichiarato e disciplinato per contratto.

- Una clausola di riservatezza senza limiti di durata, anche dopo la fine del contratto.

Non è un documento di 40 pagine. Un contratto ben redatto sta in 9 articoli, si legge in 5 minuti e si firma in 2.

13.4 Verificare gli strumenti del vostro fornitore

Il contratto deve includere una tabella o un allegato che elenchi gli strumenti utilizzati dal fornitore nell'ambito dei suoi interventi, indicando per ciascuno lo scopo e l'ubicazione dei dati. Ad esempio: lo strumento di teleassistenza utilizzato, la soluzione di monitoraggio, il gestore di password, la soluzione di backup, la posta elettronica professionale. Per ogni strumento i cui server si trovano fuori dalla Svizzera, verificate se lo Stato interessato è riconosciuto dal Consiglio federale come Stato che offre un livello di protezione adeguato (art. 16 cpv. 1 LPD) o se sono in atto garanzie contrattuali supplementari (art. 16 cpv. 2).

13.5 Responsabilità nei confronti dei pazienti (art. 25 cpv. 4)

Anche se un responsabile del trattamento tratta dati per vostro conto, restate l'unico interlocutore dei vostri pazienti. L'art. 25 cpv. 4 LPD è esplicito: il titolare del trattamento che fa trattare dati da un responsabile del trattamento resta tenuto a fornire le informazioni richieste dalla persona interessata. Non potete rinviare un paziente al vostro fornitore di servizi informatici quando chiede di accedere ai suoi dati. Spetta a voi rispondere, entro 30 giorni, anche se ciò richiede di sollecitare il vostro responsabile del trattamento per ottenere le informazioni.

13.6 Il mio fornitore attuale non ha un contratto: che fare?

Se attualmente non è in vigore alcun contratto con il vostro fornitore di servizi informatici o con gli altri responsabili del trattamento, la procedura è semplice. Contattate il vostro fornitore e chiedetegli se dispone di un contratto conforme all'art. 9 LPD. Se ne propone uno, leggetelo attentamente e verificate che copra i punti elencati sopra. Se non ne propone, è un segnale d'allarme sul suo livello di maturità in materia di protezione dei dati. Potete fornirgli un modello di contratto o farne redigere uno da un giurista specializzato.

L'assenza di un contratto non significa che la collaborazione debba cessare immediatamente, ma regolarizzare la situazione deve essere una priorità. In caso di incidente senza un contratto in vigore, la vostra posizione sarà notevolmente indebolita, sia nei confronti dell'IFPDT sia davanti ai vostri pazienti.

Delegate la parte tecnica. Mai la responsabilità.

Capitolo 14. Formazione del personale

La tecnologia non basta se le persone che la utilizzano non sono formate. Gli errori umani (un'e-mail di phishing aperta, uno schermo non bloccato, una cartella del paziente lasciata alla ricezione, una radiografia inviata tramite WhatsApp) rappresentano una parte significativa delle violazioni dei dati. La maggior parte di questi incidenti non deriva da un'intenzione malevola, ma da una mancanza di sensibilizzazione e di regole chiare.

14.1 Un obbligo implicito della nLPD

L'art. 8 LPD impone al titolare del trattamento di adottare provvedimenti organizzativi e tecnici adeguati per garantire la sicurezza dei dati. La formazione del personale fa parte di questi provvedimenti organizzativi. Nel suo rapporto esplicativo sulla nLPD, pubblicato dall'Ufficio federale di giustizia, il Consiglio federale sottolinea esplicitamente che l'attuazione efficace della sicurezza dei dati dipende dalla corretta formazione delle persone coinvolte. Una mancanza di formazione potrebbe comportare violazioni della sicurezza dei dati, ad esempio se un collaboratore apre un'e-mail contenente un software dannoso.

Nel diritto del lavoro svizzero, il datore di lavoro può impartire direttive, che i collaboratori devono rispettare (art. 321d CO). Formateli e consegnate loro le regole per scritto: altrimenti sarà difficile rimproverare loro un errore di sicurezza, e un licenziamento per questo motivo, soprattutto se immediato, potrebbe essere contestato.

14.2 Contenuto raccomandato di una formazione

La formazione deve coprire le situazioni reali con cui il personale si confronta quotidianamente.

Riconoscere i tentativi di frode. Il phishing via e-mail è il vettore più comune, ma non è l'unico rischio. La formazione deve includere le telefonate fraudolente (qualcuno si fa passare per il fornitore IT e chiede una password, un presunto collaboratore del produttore del software dentale chiede un accesso remoto, uno sconosciuto si presenta come paziente e chiede informazioni mediche per telefono), gli SMS e i messaggi fraudolenti, e le chiavette USB sconosciute trovate nello studio o nelle sue vicinanze. Esempi concreti ed esercizi pratici rafforzano la memorizzazione.

Regole di blocco dei computer. Bloccare lo schermo ogni volta che ci si allontana dalla postazione, anche per pochi secondi. La combinazione Windows+L su Windows o

Ctrl+Comando+Q su macOS deve diventare un riflesso. Uno schermo non bloccato in una sala accessibile ai pazienti costituisce una potenziale violazione della riservatezza.

Politica sulle password. Uso obbligatorio del gestore di password dello studio, attivazione dell'autenticazione a due fattori su tutti gli accessi critici, divieto di annotare le password su post-it o in file non crittografati.

Uso della posta elettronica sicura. Saper distinguere quando utilizzare la posta elettronica crittografata (qualsiasi contenuto con dati identificabili dei pazienti) e quando la posta elettronica standard è accettabile (scambi interni senza dati sensibili, ordini di materiale). Divieto assoluto di utilizzare servizi di messaggistica destinati al grande pubblico (Gmail, Hotmail, WhatsApp) per qualsiasi comunicazione contenente dati dei pazienti.

Procedura in caso di incidente

Ogni collaboratore deve sapere cosa fare in caso di sospetto attacco o fuga di dati: chi chiamare per primo (il medico dentista responsabile, poi il fornitore IT), cosa fare immediatamente (staccare il cavo di rete, non spegnere il computer), cosa non fare (non tentare di risolvere il problema da sé, non pagare un riscatto, non cancellare i messaggi sospetti prima di averli documentati).

Gestione dei dati dei pazienti. Non inviare mai dati dei pazienti tramite WhatsApp, SMS o posta elettronica personale. Non copiare dati su chiavette USB personali, dischi rigidi personali o servizi cloud non autorizzati. Non trasferire file dei pazienti su un computer personale, nemmeno per «lavorare da casa».

Sicurezza fisica e politica della scrivania pulita. Non lasciare mai cartelle dei pazienti, radiografie stampate o documenti amministrativi contenenti dati personali in vista su un bancone, su una scrivania o vicino alla ricezione.

I documenti cartacei contenenti dati dei pazienti devono essere distrutti con un distruggidocumenti, mai gettati nella spazzatura. Gli schermi visibili dalla sala d'attesa o dalle zone di passaggio devono essere orientati di conseguenza o dotati di filtri privacy.

Segreto professionale. Richiamo degli obblighi penali: l'art. 321 del Codice penale svizzero punisce la rivelazione di segreti confidati nell'esercizio della professione. Questo obbligo si applica a tutto il personale dello studio, non solo al medico dentista.

14.3 Apparecchi personali e BYOD

L'uso di apparecchi personali (telefoni, tablet, portatili, chiavette USB) per accedere ai dati dello studio deve essere vietato oppure rigorosamente disciplinato da una regola scritta. Se un collaboratore usa il suo telefono personale per consultare le e-mail professionali, i dati dei pazienti contenuti in queste e-mail si ritrovano su un apparecchio non controllato dallo studio, potenzialmente non crittografato e che può essere perso, rubato o compromesso. La politica dello studio deve definire chiaramente quali apparecchi sono autorizzati, quali applicazioni possono essere utilizzate e quali dati possono transitarvi.

14.4 Personale temporaneo e terzi

Gli stagisti, i sostituti, il personale delle pulizie, i tecnici esterni e qualsiasi altra persona che ha accesso fisico ai locali dello studio devono essere presi in considerazione nella politica di sicurezza. Uno stagista presente per due settimane può vedere gli stessi schermi di un dipendente fisso. Il personale delle pulizie che interviene al di fuori degli orari di apertura ha accesso agli uffici, alle stampanti e potenzialmente ai documenti lasciati in vista. I tecnici esterni (fornitori di apparecchiature mediche, installatori) possono aver bisogno di accedere temporaneamente alla rete.

Ogni persona che ha un accesso fisico o digitale, anche temporaneo, deve ricevere un minimo di informazioni sulle regole di riservatezza dello studio. Per il personale temporaneo è sufficiente un documento riassuntivo di una pagina che richiami le regole essenziali, firmato all'arrivo.

14.5 La politica interna di sicurezza scritta

La formazione orale non basta. Lo studio deve disporre di una politica interna di sicurezza informatica formalizzata per iscritto, consegnata a ogni collaboratore al suo arrivo e aggiornata almeno una volta all'anno. Questo documento costituisce il riferimento in caso di controversia e tutela il medico dentista in caso di incidente: dimostra che le regole esistevano, che sono state comunicate e che il collaboratore ne ha preso conoscenza. La politica deve coprire almeno le regole di utilizzo delle postazioni di lavoro, la politica sulle password, le regole relative alla posta elettronica e alle comunicazioni, il divieto o la disciplina degli apparecchi personali, la procedura in caso di incidente e le sanzioni interne in caso di inosservanza. Ogni collaboratore firma una copia con cui attesta di aver letto, compreso e accettato le regole. Questa firma viene conservata nel fascicolo del personale.

14.6 Frequenza, formato e valutazione

La formazione deve aver luogo almeno una volta all'anno per tutto il personale, con una sessione dedicata all'arrivo di ogni nuovo collaboratore, compresi gli stagisti e i sostituti. Il formato può essere una presentazione interna da 30 a 60 minuti, completata dalla consegna del documento di politica interna.

Per valutare l'efficacia della formazione si raccomandano esercizi pratici: simulazioni di phishing (invio di una falsa e-mail fraudolenta per verificare la reazione del personale), brevi quiz sulle buone pratiche, simulazioni di situazioni concrete (un collaboratore riceve una telefonata in cui gli si chiede una password). Questi esercizi non mirano a cogliere in fallo il personale, ma a individuare i punti deboli e ad adattare di conseguenza la successiva sessione di formazione.

Documentate ogni sessione: data, partecipanti, temi trattati, risultati degli esercizi se del caso. Questa documentazione fa parte dei provvedimenti organizzativi che l'IFPDT può chiedere di vedere in caso di controllo.

14.7 Responsabilità condivisa

Se un'assistente invia una radiografia tramite WhatsApp, può incorrere in una responsabilità penale personale se tale invio costituisce una rivelazione intenzionale di dati coperti dal segreto (art. 62 LPD sull'obbligo del segreto e art. 321 CP sul segreto professionale, che riguarda anche gli ausiliari dei dentisti; reati perseguibili a querela di parte). Una semplice negligenza non è punibile in virtù di questi due articoli. Ma è il medico dentista a notificare la

violazione all'IFPDT e a rispondere davanti ai pazienti. La sua esposizione dipende dalle misure che aveva messo in atto: politica interna scritta e firmata, formazione impartita e documentata, gestione adeguata degli accessi. Se non era in atto nulla, è anch'egli esposto per non aver prevenuto il rischio. Se tutto era in atto e documentato, la sua posizione è notevolmente rafforzata.

Capitolo 15. Assicurazioni cyber

Anche con un livello di sicurezza informatica eccellente, il rischio zero non esiste. Un'assicurazione cyber permette di trasferire una parte del rischio finanziario a un assicuratore e di beneficiare di un aiuto professionale in caso di crisi.

15.1 Che cosa copre un'assicurazione cyber

Le assicurazioni cyber proposte in Svizzera coprono generalmente:

- Le spese di intervento informatico d'urgenza (analisi forense, ripristino)
- La perdita di fatturato dovuta all'interruzione dell'attività
- Le spese di notifica obbligatoria (IFPDT, pazienti interessati)
- La responsabilità civile in caso di danni ai dati di terzi
- Le spese di gestione della crisi e di comunicazione
- Le spese legali legate all'incidente

15.2 Principali assicuratori in Svizzera

Diversi assicuratori svizzeri propongono formule appositamente concepite per le PMI:

- **Zurich:** formula modulare in 4 varianti, che include una formazione gratuita in cibersicurezza per gli assicurati.
- **Helvetia:** assicurazione cyber con hotline 24 ore su 24 e rete di partner specializzati, label cyber-safe per uno sconto del 20%.
- **AXA:** protezione su tre livelli: prevenzione, aiuto d'urgenza, riparazione.
- **Baloise:** tre formule (ECO, SMART, TOP) con copertura del riscatto a determinate condizioni.
- **Allianz:** Cyber Risk con copertura dell'interruzione d'esercizio per 24 mesi.

15.3 Punti a cui prestare attenzione

Prima di sottoscrivere, verificate attentamente:

- Le esclusioni (alcune polizze escludono gli attacchi se gli aggiornamenti non erano stati installati)

- L'importo delle franchigie, talvolta elevate per le PMI
- Le condizioni preliminari di sicurezza richieste dall'assicuratore
- Il massimale di copertura e la sua coerenza con la vostra esposizione reale
- La copertura o meno del pagamento del riscatto (politica variabile a seconda degli assicuratori)

Consiglio

L'assicurazione cyber non sostituisce le misure di sicurezza; le completa. Un assicuratore esigerà un livello minimo di protezione (antivirus, backup, password) per accettare di coprirvi. È un circolo virtuoso: più siete protetti, più basso è il premio.

Capitolo 16. Cosa fare in caso di incidente

Se succede (e statisticamente, per alcuni studi, succederà), i primi minuti sono determinanti.

16.1 Scenario A: attacco in corso (ransomware, intrusione)

Fase 1. ISOLARE: staccare il cavo di rete, disattivare il Wi-Fi. Non spegnere il computer: si distruggerebbero prove utili per l'analisi.

Fase 2. CHIAMARE IL SUPPORTO IT: per primo il vostro fornitore di servizi informatici. Se non è raggiungibile, l'UFCS tramite incidents@ncsc.ch o il modulo su report.ncsc.admin.ch.

Fase 3. NON PAGARE: raccomandazione ufficiale della Confederazione Svizzera. Pagare non garantisce il recupero dei dati e finanzia le reti criminali.

Fase 4. DOCUMENTARE: fotografare le schermate di errore, annotare l'ora esatta della scoperta, conservare tutto. Queste informazioni saranno necessarie per l'assicurazione, la polizia e la notifica prevista dalla legge.

Fase 5. VALUTARE: la violazione comporta verosimilmente un rischio elevato per i pazienti (ad es. dati sulla salute rubati, esposti o crittografati da un ransomware)? In caso affermativo, o se non potete escluderlo rapidamente, la notifica all'IFPDT è obbligatoria (art. 24 cpv. 1 LPD).

Fase 6. NOTIFICARE: databreach.edoeb.admin.ch, quanto prima.

16.2 Scenario B: perdita o fuga accidentale

Perdita di un supporto di dati, invio al destinatario sbagliato, cancellazione accidentale, scoperta di un accesso non autorizzato: la procedura è simile: documentare, valutare il rischio per i pazienti, notificare la violazione all'IFPDT se il rischio è elevato, informare i pazienti se necessario.

16.3 Cosa fa concretamente l'IFPDT

Non è un'irruzione nel vostro studio. L'IFPDT legge la vostra notifica, verifica che abbiate reagito correttamente, può chiedere precisazioni o fornire consigli.

L'IFPDT non può infliggere direttamente multe. Le sanzioni penali passano per le autorità cantonali e riguardano le violazioni intenzionali, non gli studi che hanno notificato in buona fede.

La regola d'oro: notificare presto è meglio che non notificare.

Capitolo 17. Casi reali nella Svizzera romanda

Questi attacchi non sono teorici. Hanno colpito strutture mediche nella Svizzera romanda, in ambienti paragonabili a uno studio dentistico.

Groupe 3R, Réseau Radiologique Romand (aprile 2025 e aprile 2026)

Venti centri di diagnostica per immagini distribuiti su sette Cantoni. Ransomware, furto di dati medici e amministrativi, tentativo di estorsione. Il riscatto è stato rifiutato. L'incidente è stato segnalato all'UFCS. Il gruppo ha subito un secondo attacco ransomware nell'aprile 2026; ha di nuovo rifiutato di pagare, e dati rubati sono stati pubblicati su Internet.

Vidymed, Losanna (dicembre 2024)

Intrusione informatica rilevata il 7 dicembre 2024 in quattro centri medici di Losanna e di Épalinges: tutta l'informatica è stata sospesa e il personale è tornato alla carta. La maggior parte dei dati è stata ripristinata solo cinque settimane dopo. Una situazione che paralizzerebbe qualsiasi studio dentistico.

La Svizzera in cifre

Nel 2025, l'Ufficio federale della cibersicurezza (UFCS) ha ricevuto 64'733 segnalazioni volontarie di ciberincidenti (rapporto annuale 2025 dell'UFCS).

Scenari tipici di attacco nel settore medico

Oltre ai casi reali descritti sopra, ecco quattro scenari tipici, costruiti a partire dagli attacchi più comuni contro gli studi. Mostrano come inizia più spesso un attacco:

Ransomware tramite accesso remoto non protetto

Uno strumento di controllo remoto resta sempre aperto, protetto da una password corta, per facilitare gli interventi del fornitore. Un aggressore la indovina con tentativi automatici e prende il controllo del server durante la notte. Il ransomware si propaga a tutta la rete: lo studio resta chiuso per diversi giorni, e solo i dati salvati in un luogo fuori portata possono essere recuperati.

Phishing con una falsa fattura di un operatore di telecomunicazioni

Un'e-mail imita la fattura di un operatore di telecomunicazioni, con l'oggetto «La vostra fattura non pagata». Una volta aperto l'allegato, un ransomware crittografa la rete, compresi i backup collegati in permanenza. Senza una copia fuori portata, lo studio non dispone più di alcuna copia utilizzabile dei suoi dati.

Usurpazione d'identità del fornitore IT

Un aggressore si fa passare per il fornitore di servizi informatici dello studio e chiede le credenziali «per un aggiornamento urgente». Un'assistente le trasmette in buona fede. L'aggressore accede al server e copia cartelle di pazienti prima di essere scoperto.

Chiavetta USB infetta

Una chiavetta USB «dimenticata» nel parcheggio dello studio porta l'etichetta «Salari». Una volta inserita in un computer, installa uno spyware che registra le password digitate sulla tastiera: quelle del software dentale, della posta elettronica e dell'e-banking sono compromesse.

Quanto costa un attacco

Giorni, a volte settimane, di lavoro a ritmo ridotto: da Vidymed sono servite cinque settimane per recuperare la maggior parte dei dati. A ciò si aggiungono il ripristino, l'intervento degli specialisti, l'informazione dei pazienti e la perdita della loro fiducia.

Checklist di conformità

Utilizzate questa lista per valutare il vostro livello di conformità attuale e migliorare ciò che manca nella vostra infrastruttura. Ogni punto non spuntato rappresenta un rischio da trattare. Un lessico dei termini tecnici è disponibile alla fine della lista.

Comunicazioni

- Posta elettronica crittografata utilizzata per tutti i dati dei pazienti (HIN Mail, ProtonMail o equivalente)
- Nessun dato dei pazienti inviato tramite Gmail, Hotmail, Bluewin, WhatsApp o SMS
- Documenti cartacei contenenti dati dei pazienti distrutti con un distruggidocumenti

Infrastruttura

- Tutti i computer con Windows 11 o macOS aggiornato
- Nessun computer con Windows 7, 8 o 10 sulla rete
- Aggiornamenti automatici attivati su tutti i computer, server e applicazioni
- Crittografia dei dischi attivata su tutti i computer e server (BitLocker / FileVault)
- Wi-Fi per i pazienti separato dalla rete dello studio

Backup

- Strategia 3-2-1 in atto (3 copie, 2 supporti, 1 fuori dallo studio), con una copia scollegata o immutabile
- Ripristino testato regolarmente (almeno una volta all'anno, idealmente ogni mese)

Accessi e autenticazione

- Un account nominativo per ogni collaboratore, nessun account condiviso
- Password di almeno 12 caratteri, conservate in un gestore sicuro
- 2FA attivata su posta elettronica, software gestionale e accesso remoto
- Account degli ex collaboratori disattivati
- Accesso remoto solo tramite VPN o RMM professionale

Conformità nLPD

- Contratto con il responsabile del trattamento (art. 9) firmato dal fornitore IT
- Contratto con il responsabile del trattamento in vigore con ogni terzo che accede ai dati dei pazienti
- Politica interna di sicurezza redatta e firmata da ogni collaboratore
- Formazione del personale svolta negli ultimi 12 mesi
- Piano di risposta agli incidenti documentato e accessibile
- Contatti d'emergenza affissi (fornitore IT, UFCS, IFPDT)

Protezione e monitoraggio

- Soluzione EDR installata e supervisionata
- Audit di sicurezza annuale effettuato
- Assicurazione cyber sottoscritta e condizioni verificate

Lessico della checklist

Posta elettronica crittografata: servizio di e-mail il cui contenuto viene bloccato all'invio e può essere letto solo dal destinatario. Né il fornitore né un pirata informatico che intercetta il messaggio possono accedervi. Esempi: HIN Mail, ProtonMail.

Backup 3-2-1: 3 copie dei vostri dati, su 2 supporti diversi, di cui 1 conservata fuori dallo studio. Si raccomanda inoltre che una delle copie sia scollegata o immutabile (protetta da qualsiasi modifica o cancellazione, anche da parte di un virus): è la variante 3-2-1-1-0.

BitLocker / FileVault: strumenti di crittografia integrati gratuitamente in Windows (BitLocker) e in macOS (FileVault). Rendono il contenuto del disco rigido totalmente illeggibile in caso di furto del computer.

2FA (autenticazione a due fattori): seconda verifica dopo la password, generalmente un codice temporaneo visualizzato sul telefono. Stesso principio della carta bancaria: il numero da solo non basta, serve anche il codice.

VPN: connessione crittografata tra un apparecchio remoto e la rete dello studio. Protegge i dati in transito come un tunnel privato.

RMM: software professionale di teleassistenza che registra ogni connessione, applica gli aggiornamenti e sorveglia i computer in continuo. Alternativa sicura agli strumenti gratuiti come TeamViewer.

EDR: protezione avanzata che analizza il comportamento dei programmi in tempo reale e blocca le azioni sospette, anche sconosciute. Va oltre l'antivirus classico, che rileva solo le minacce già catalogate.

Art. 9 LPD: articolo di legge che disciplina il ricorso a un responsabile del trattamento. Un terzo può trattare dati dei pazienti per lo studio (fornitore IT, fornitore di hosting cloud, laboratorio, contabile) solo se un contratto o la legge lo prevede, e lo studio deve assicurarsi che sia in grado di garantire la sicurezza dei dati. La forma scritta non è richiesta, ma è il modo più sicuro di provare il contratto. Chi affida intenzionalmente dati senza rispettare

queste condizioni è punito, a querela di parte, con la multa fino a CHF 250'000 (art. 61 lett. b).

UFCS: Ufficio federale della cibersicurezza. Organismo da contattare in caso di ciberattacco. Contatto: incidents@ncsc.ch o report.ncsc.admin.ch.

IFPDT: Incaricato federale della protezione dei dati e della trasparenza. Autorità a cui notificare una violazione della sicurezza dei dati a rischio elevato (art. 24 LPD). Contatto: +41 58 462 43 95 o databreach.edoeb.admin.ch.

Contatti e risorse utili

Contatti d'emergenza

- **UFCS:** Ufficio federale della cibersicurezza: incidents@ncsc.ch / report.ncsc.admin.ch
- **IFPDT:** Incaricato federale della protezione dei dati e della trasparenza: +41 58 462 43 95 (lun–ven 10:00–12:00) / databreach.edoeb.admin.ch
- **Polizia cantonale:** 117

Testi legali

- **nLPD (RS 235.1):** www.fedlex.admin.ch
- **Ordinanza sulla protezione dei dati (OPDa):** www.fedlex.admin.ch
- **Guida dell'IFPDT sulle violazioni della sicurezza dei dati:** www.edoeb.admin.ch
- **Guida PMI sulla protezione dei dati:** www.kmu.admin.ch

Risorse complementari

- **FMH:** strumenti e modelli per studi medici: www.fmh.ch
- **HIN:** sicurezza dell'informazione per il settore medico: www.hin.ch
- **No More Ransom (aiuto alla decrittografia):** www.nomoreransom.org

Domande frequenti

Le domande seguenti sono quelle che i medici dentisti pongono più spesso. Derivano da situazioni reali riscontrate in studi dentistici della Svizzera romanda.

Una perdita accidentale di dati è una violazione ai sensi della nLPD?

Sì. L'art. 5 lett. h LPD definisce la violazione della sicurezza dei dati come qualsiasi perdita, modifica, cancellazione o distruzione di dati personali, accidentale o illecita. Cancellare per errore cartelle dei pazienti, perdere un disco rigido o subire un guasto del server senza backup: tutto ciò rientra in questa definizione. Se il rischio per i pazienti è elevato, la notifica all'IFPDT è obbligatoria.

Il mio fornitore IT ha cancellato dei dati. Chi è responsabile?

Voi, il medico dentista, in quanto titolare del trattamento (art. 9 e art. 25 cpv. 4 LPD). Non potete rinviare il paziente al vostro informatico. La vostra possibilità di rivalervi sul fornitore è molto più solida con un contratto conforme con il responsabile del trattamento; senza contratto resta possibile secondo il Codice delle obbligazioni, ma è più difficile. Delegate la parte tecnica, mai la responsabilità.

Sono in pensione da 3 anni e viene scoperta una fuga di dati risalente a 4 anni fa. Sono ancora coinvolto?

Sì. L'art. 66 LPD fissa a 5 anni il termine di prescrizione dell'azione penale. Il pensionamento o la cessazione dell'attività non elimina la responsabilità per fatti commessi durante l'esercizio della professione. Il punto di partenza esatto (data della fuga o data della scoperta) richiede il parere di un giurista, ma il termine di 5 anni è confermato dalla legge.

I miei iMac con Windows 10 tramite Boot Camp: si può tornare a macOS?

No, e non risolverebbe nulla. I software dentali (Sidexis, Romexis, DBSWin, Cliniview, DTX Studio) funzionano esclusivamente con Windows. Inoltre, spesso questi iMac Intel non possono più passare né a Windows 11, né alle ultime versioni di macOS. Sono a fine vita su entrambi i fronti. La soluzione: sostituirli con PC dedicati con Windows 11.

Quale software dentale scegliere?

Questa guida non raccomanda né sconsiglia pubblicamente alcun software specifico. Ecco però i criteri di sicurezza da verificare: il software offre nativamente l'autenticazione a due

fattori (2FA)? Il produttore pubblica aggiornamenti di sicurezza regolari? Dove sono ospitati i dati? Il team di sviluppo dispone di competenze documentate in materia di sicurezza? Un software medico critico è un prodotto IT: chiedetevi se il produttore ha i mezzi per farlo evolvere nel tempo.

Un'assistente invia una radiografia tramite WhatsApp. Chi è responsabile?

Entrambi, ma non per le stesse ragioni. L'assistente può incorrere in una responsabilità penale personale se l'invio costituisce una rivelazione intenzionale di dati coperti dal segreto: art. 62 LPD (violazione dell'obbligo del segreto) e art. 321 del Codice penale (segreto professionale, che riguarda anche gli ausiliari dei dentisti), a querela di parte. Un errore dovuto a semplice negligenza non è punibile in virtù di questi articoli. Il medico dentista, dal canto suo, è colui che notifica la violazione all'IFPDT e che risponde davanti ai pazienti. La sua esposizione dipende dalle misure che aveva messo in atto: politica interna scritta, formazione impartita, gestione degli accessi. Se non esisteva nulla di tutto ciò, è anch'egli esposto per non aver prevenuto il rischio.

L'IFPDT effettua controlli negli studi?

L'IFPDT può aprire un'inchiesta d'ufficio o su denuncia, se vi sono indizi sufficienti che un trattamento possa violare le disposizioni sulla protezione dei dati (art. 49 LPD). Le fonti di rischio reali per un medico dentista sono un paziente scontento, un incidente che diventa pubblico o una denuncia di un ex dipendente.

La nLPD impone un termine di 72 ore come il RGPD?

No. La legge svizzera impone una notifica «quanto prima», una formulazione volutamente più flessibile rispetto al RGPD europeo, che fissa un termine rigido di 72 ore. L'IFPDT raccomanda di agire «il più rapidamente possibile». In pratica: agire non appena si viene a conoscenza della violazione e completare poi la documentazione se necessario. Non esiste una sanzione specifica in caso di ritardo, ma la reattività è un fattore preso in considerazione nella valutazione della buona fede.

Glossario

I termini seguenti sono utilizzati in questa guida e nella nLPD. Questo glossario li definisce in un linguaggio accessibile ai non specialisti.

Termine	Definizione
nLPD	Nuova legge federale sulla protezione dei dati (RS 235.1), entrata in vigore il 1° settembre 2023.
IFPDT	Incaricato federale della protezione dei dati e della trasparenza. Autorità di vigilanza indipendente, incaricata di vigilare sul rispetto della legge.
UFCS	Ufficio federale della cibersecurity (in precedenza NCSC/MELANI). Centro di competenza della Confederazione per le cyberminacce.
Dati personali	Tutte le informazioni concernenti una persona fisica identificata o identificabile (art. 5 lett. a).
Dati personali degni di particolare protezione	Categoria con protezione rafforzata: dati sulla salute, opinioni religiose/politiche, dati genetici e biometrici, perseguimenti penali, assistenza sociale (art. 5 lett. c).
Titolare del trattamento	La persona che determina lo scopo e i mezzi del trattamento. In uno studio dentistico: il titolare dello studio (art. 5 lett. j).
Responsabile del trattamento	La persona che tratta dati per conto del titolare del trattamento. Esempio: il fornitore di servizi informatici dello studio (art. 5 lett. k).
Violazione della sicurezza	Qualsiasi perdita, modifica, cancellazione, distruzione, divulgazione o accesso non autorizzato a dati personali, in modo accidentale o illecito (art. 5 lett. h).
Privacy by Design	Obbligo di integrare la protezione dei dati sin dalla progettazione di un sistema o di un processo (art. 7 cpv. 1).

Privacy by Default	Obbligo di limitare per impostazione predefinita il trattamento allo stretto necessario (art. 7 cpv. 3).
VIPD	Valutazione d'impatto sulla protezione dei dati. Obbligatoria quando un trattamento presenta un rischio elevato (art. 22).
2FA / MFA	Autenticazione a due fattori / autenticazione a più fattori. Seconda verifica dopo la password (codice SMS, applicazione, chiave fisica).
EDR	Endpoint Detection and Response. Soluzione di sicurezza che rileva le minacce tramite l'analisi comportamentale in tempo reale, e non tramite firme.
Ransomware	Software dannoso che crittografa i dati ed esige un riscatto per sbloccarli.
Phishing	Tecnica di frode via e-mail, SMS o telefono volta a ottenere credenziali o a far aprire un file infetto.
BitLocker	Strumento di crittografia integrato in Windows Pro/Enterprise. Rende i dati illeggibili senza la chiave di decrittografia.
FileVault	Equivalente di BitLocker per macOS. Crittografia integrata del disco di sistema.
VPN	Virtual Private Network. Tunnel crittografato che consente un accesso remoto sicuro alla rete dello studio.
RMM	Remote Monitoring and Management. Soluzione professionale di teleassistenza con tracciabilità (NinjaOne, Datto, Atera).
Regola 3-2-1	Strategia di backup raccomandata dall'UFCS: 3 copie dei dati, su 2 supporti diversi, di cui 1 fuori dallo studio. La variante 3-2-1-1-0 aggiunge una copia offline o immutabile (protetta da modifiche) e mira a zero errori nei test di ripristino.
WPA3 / WPA2	Protocolli di sicurezza Wi-Fi. WPA3 è la versione più recente e più sicura; WPA2 è il minimo accettabile.

HIN	Health Info Net. Rete sicura svizzera per gli scambi tra professionisti della salute.
OPDa	Ordinanza sulla protezione dei dati. Testo d'esecuzione della nLPD, che ne precisa le modalità tecniche e organizzative.

Note legali e condizioni di utilizzo

Il presente documento è stato redatto da **DentalSystems Sàrl** a scopo informativo e di sensibilizzazione. Non costituisce una consulenza legale. Le informazioni contenute nel presente documento sono aggiornate a ottobre 2026 e possono evolvere in funzione delle 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 nel contesto medico, rivolgetevi a un giurista specializzato.

Proprietà intellettuale

Il presente documento è di proprietà esclusiva di DentalSystems Sàrl. L'insieme del suo 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 autorizzato

Questa guida (DS1) e la scheda riflessi (DS2) sono messe a disposizione gratuitamente. Possono essere liberamente scaricate, stampate e diffuse all'interno di uno studio dentistico o di una struttura medica, senza modifiche e con l'indicazione del loro autore (DentalSystems Sàrl). I modelli del kit (da DS3 a DS11) possono essere modificati e utilizzati a nome dello studio, anche nei confronti dei suoi pazienti, dei suoi collaboratori e dei suoi fornitori, senza mantenere le menzioni di DentalSystems Sàrl.

Utilizzi vietati

Salvo previo accordo scritto di DentalSystems Sàrl, sono severamente vietate:

- La vendita o la commercializzazione di questi documenti, in qualsiasi forma, anche in versione modificata.
- La diffusione di una versione modificata della guida o della scheda riflessi, o la loro presentazione come opera di un altro autore.
- La soppressione, l'alterazione o l'occultamento, nella guida e nella scheda riflessi, delle indicazioni dell'autore, del logo o dei recapiti di DentalSystems Sàrl.
- La messa a disposizione di questi documenti per il download da parte di terzi (siti di download, piattaforme di condivisione, rivenditori).

Qualsiasi utilizzo commerciale non autorizzato costituisce una violazione del diritto d'autore e potrà essere oggetto di azioni legali. In caso di divergenza, prevalgono le condizioni di utilizzo pubblicate su www.dentalsystems.ch.

Limitazione di responsabilità

Il presente documento è fornito gratuitamente, a scopo informativo. Nei limiti consentiti dal diritto svizzero, DentalSystems Sàrl non risponde delle conseguenze dirette o indirette del suo utilizzo; questa limitazione non si applica in caso di dolo o colpa grave (art. 100 CO). L'utilizzatore resta l'unico responsabile dell'adattamento di queste informazioni alla propria situazione specifica. Il presente 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.