

QUICK-REACTION SHEET: SECURITY INCIDENT

Dental practice | Emergency procedure | To be displayed near each workstation

Art. 24 FADP. Obligation to notify in the event of a data security breach

If you suspect an attack: follow these 6 steps in order. Do not panic.

1 ISOLATE

- Unplug the network cable (Ethernet) immediately
- Turn off the WiFi on the computer concerned
- DO NOT SWITCH OFF the computer; that destroys the evidence

2 CALL YOUR IT PROVIDER

- Contact your IT provider first
- If unavailable: FOCS via report.ncsc.admin.ch or incidents@ncsc.ch
- Explain the symptoms observed

3 DOCUMENT

- Photograph the error or ransom screens
- Note the exact time the incident was discovered
- List the computers and data that may be affected

4 DO NOT PAY A RANSOM

- Official recommendation of the Swiss Confederation
- Paying does not guarantee that the data will be recovered
- It finances criminal networks

5 ASSESS: high risk for patients?

- X-rays, files, diagnoses, AHV numbers, invoices affected?
- If YES, or it cannot be ruled out: reporting to the FDPIC is mandatory
- Do not wait for the end of the analysis to report

6 NOTIFY THE FDPIC

- Portal: databreach.edoeb.admin.ch
- FDPIC phone: +41 58 462 43 95
- Deadline: as soon as possible (Art. 24 FADP)

EMERGENCY CONTACTS AND REFERENCES

To be kept near each workstation in the practice

FOCS: Federal Office for Cyber Security

Active attack, ransomware, intrusion

incidents@ncsc.ch

Online form: report.ncsc.admin.ch

FDPIC: notification of a data breach

Legal obligation, Art. 24 FADP. Mon-Fri 10:00-12:00

+41 58 462 43 95

Portal: databreach.edoeb.admin.ch

Cantonal police
117

No More Ransom (decryption help)

www.nomoreransom.org

SCENARIO B: ACCIDENTAL LOSS OR LEAK OF DATA

- Loss of a storage medium (USB stick, hard drive, stolen laptop)
- Patient data sent to the wrong recipient by e-mail
- Accidental deletion of patient files with no backup
- Unauthorised access discovered (former employee, compromised account)

Procedure: document, assess the risk, notify the FDPIC if the risk is high, inform patients if necessary

LEGAL BASIS: FADP (SR 235.1)

Art. 5 let. h	Definition of a data security breach
Art. 8	Data security obligation (technical and organisational measures)
Art. 9	Processing by processors: an agreement with your IT provider is mandatory
Art. 24	Reporting breaches to the FDPIC as soon as possible
Art. 60-61	Criminal penalties: up to CHF 250,000 (personal liability)
Art. 66	Limitation period for prosecution: 5 years

PREVENTION: ESSENTIAL CHECKS

☐ Secure e-mail (HIN Mail / ProtonMail)	☐ All computers on an up-to-date Windows 11 / macOS
☐ 3-2-1 backups tested at least once a year	☐ Patient WiFi separate from the practice network
☐ Drive encryption (BitLocker / FileVault)	☐ Secure remote access (never free TeamViewer)
☐ Passwords of 12+ characters + password manager	☐ Data processing agreement signed (Art. 9 FADP)
☐ Two-factor authentication (2FA) on critical access	☐ Incident response plan documented and accessible

The FDPIC does not raid your practice.

It reads your report, checks that you reacted correctly, and may ask for further details.

The golden rule: notifying early is better than not notifying.

Legal notice and terms of use

This document was written by **DentalSystems Sàrl** for information and awareness purposes. It does not constitute legal advice. The information in this document is up to date as of October 2026 and may change as legislation and regulations evolve. This English version is a translation; the French version prevails.

For any legal question relating to the FADP, the GDPR or data protection in the medical context, consult a lawyer specialising in the field.

Intellectual property

This document is the exclusive property of DentalSystems Sàrl. All of its content (texts, structure, layout and graphic elements) is protected by copyright in accordance with the Federal Act on Copyright and Related Rights (CopA, SR 231.1).

Permitted use

This document is made available free of charge. It may be freely downloaded, printed and distributed within a dental practice or a medical organisation, without modification and with mention of its author (DentalSystems Sàrl).

Prohibited use

Unless DentalSystems Sàrl has given its prior written consent, the following are prohibited:

- Selling this document, even in modified form.
- Offering it for download to third parties (download sites, sharing platforms, resellers).
- Removing or altering its author's name or this notice.

The terms of use published on www.dentalsystems.ch apply; in the event of a discrepancy, they prevail over this notice.

Limitation of liability

This document is provided free of charge, for information. To the extent permitted by Swiss law, DentalSystems Sàrl is not liable for the consequences of its use; this limitation does not apply in the event of intent or gross negligence. Users remain responsible for adapting it to their situation. It replaces neither a professional audit nor legal advice.

DentalSystems Sàrl

Thomas Alvino, IT Technician

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

© 2026 DentalSystems Sàrl. All rights reserved.