

REFERENCE GUIDE

Cybersecurity & FADP

Protect your patients' data.

Secure your IT infrastructure.

Understand your legal obligations.

DentalSystems Sàrl

Thomas Alvino, IT Technician

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

October 2026. Compliant with the FADP (SR 235.1)

TABLE OF CONTENTS

Introduction	7
Chapter 1. The legal framework: the FADP	8
1.1 What is the FADP?	8
1.2 Which data is concerned?	8
1.3 The three fundamental obligations	9
1.4 Notification of breaches (Art. 24 FADP)	9
1.5 Patients' rights (Art. 25 FADP)	11
Communication of health data (Art. 25 para. 3)	11
Responsibility when using a processor (Art. 25 para. 4)	11
Mandatory nature of the right of access (Art. 25 para. 5)	11
Free of charge and deadline (Art. 25 para. 6 and 7)	11
Patient's remedies in the event of non-compliance	11
1.6 Record of processing activities (Art. 12 FADP)	13
1.7 Penalties (Art. 60 to 66 FADP)	13
1.8 Major differences from the old law (DPA 1992)	15
1.9 Privacy by Design and Privacy by Default (Art. 7 FADP)	15
1.10 Data protection impact assessment (Art. 22 FADP)	16
Examples requiring a DPIA	16
Content of the impact assessment	16
1.11 Recent case law	16
Statthalteramt Bezirk Zürich, March 2025 (ST.2024.1046/ZM)	16
1.12 Good practice for handling access requests	16
Chapter 2. Secure e-mail	18
2.1 The problem	18
2.2 Compliant solutions	18
Chapter 3. Updates	20
3.1 Operating system	20

3.2 Applications and practice software	20
Chapter 4. Backups	21
4.1 The 3-2-1 rule	21
4.2 Why the immutable copy is essential	21
4.3 Testing the restore	22
Chapter 5. Passwords and two-factor authentication	23
5.1 The problem of weak passwords.....	23
5.2 Creating a strong password	23
5.3 Using a password manager.....	23
5.4 Two-factor authentication (2FA)	23
Chapter 6. Encryption of drives and archives	24
6.1 Encryption of workstations	24
6.2 Encrypted containers for sensitive archives	24
Chapter 7. WiFi network	25
7.1 The recommended configuration: three separate networks	25
Chapter 8. Secure remote access	26
8.1 The risk of free versions left permanently on standby	26
8.2 Recommended solutions	26
Chapter 9. Phishing	27
9.1 Recognising a phishing e-mail	27
9.2 Advanced protection: filtering by label.....	27
Chapter 10. User access management	28
10.1 Principle of least privilege.....	28
10.2 Account management rules.....	28
10.3 Managing arrivals and departures	28
10.4 Periodic review of access rights	30
10.5 Tools that make access management easier	30
Chapter 11. Polymorphic malware and EDR protection	31
11.1 Why conventional antivirus is no longer enough	31

11.2 The solution: EDR (Endpoint Detection and Response)	31
11.3 EDR, EPP, antivirus: understanding the differences	32
11.4 The role of the IT provider	32
Chapter 12. Modernising the IT equipment.....	33
12.1 Why an obsolete computer is dangerous	33
12.2 Recommended replacement cycle	33
12.3 Special case: iMacs running Boot Camp.....	34
12.4 Planning the migration.....	35
12.5 Secure destruction of old equipment.....	35
Chapter 13. The data processing agreement (Art. 9 FADP).....	36
13.1 Preconditions for using any processor	36
13.2 Who is concerned by the data processing agreement?	36
13.3 What the agreement must contain	37
13.4 Checking your provider's tools	39
13.5 Responsibility towards patients (Art. 25 para. 4).....	39
13.6 My current provider has no agreement: what should I do?	39
Chapter 14. Staff training	40
14.1 An implicit obligation under the FADP	40
14.2 Recommended content of a training session	40
14.3 Personal devices and BYOD	43
14.4 Temporary staff and third parties	43
14.5 The written internal security policy	44
14.6 Frequency, format and assessment	44
14.7 Shared responsibility	44
Chapter 15. Cyber insurance	46
15.1 What cyber insurance covers	46
15.2 Main insurers in Switzerland	46
15.3 Points to watch	46
Chapter 16. What to do in an incident.....	48

16.1 Scenario A: active attack (ransomware, intrusion)	48
16.2 Scenario B: accidental loss or leak	48
16.3 What the FDPIC actually does	48
Chapter 17. Real cases in French-speaking Switzerland	49
Groupe 3R, Réseau Radiologique Romand (April 2025 and April 2026)	49
Vidymed, Lausanne (December 2024).....	49
Switzerland in figures	49
Typical attack scenarios in the medical field	50
Ransomware via unsecured remote access	50
Phishing with a fake telecom operator invoice	50
Impersonation of the IT provider	50
Infected USB stick	50
What an attack costs	50
Compliance checklist	51
Communications	51
Infrastructure.....	51
Backups	51
Access and authentication	51
FADP compliance	51
Protection and follow-up	52
Checklist glossary	53
Useful contacts and resources.....	55
Emergency contacts	55
Legal texts	55
Further resources	55
Frequently asked questions	56
Is an accidental loss of data a breach within the meaning of the FADP?.....	56
My IT provider deleted data. Who is responsible?	56

I retired 3 years ago and a leak dating back 4 years has been discovered. Am I still concerned?.....	56
My iMacs run Windows 10 via Boot Camp: can we go back to macOS?	56
Which dental software should I choose?	56
A dental assistant sends an X-ray on WhatsApp. Who is responsible?	57
Does the FDPIC carry out inspections in practices?	57
Does the FADP impose a 72-hour deadline like the GDPR?	57
Glossary	58
Legal notice and terms of use	61
Intellectual property	61
Permitted use	61
Prohibited use	61
Limitation of liability	61

Introduction

This guide is intended for dentists, practice managers and their teams. It was written following the conference organised by the Swiss Dental Association, Neuchâtel Section (SSO-NE), on 12 March 2026, on cybersecurity and compliance with the new Federal Act on Data Protection (FADP).

The FADP, which came into force on 1 September 2023, imposes concrete obligations on dental practices regarding the protection of patient data. Health data (X-rays, diagnoses, treatment plans) is sensitive data within the meaning of the law, subject to stricter rules.

This document covers all the topics addressed at the conference, explored in more depth and supplemented by two additional subjects: staff training and cyber insurance. It is designed as a lasting reference work, to be kept and consulted every day.

About this guide

This document is provided for information and educational purposes. It does not constitute legal advice. For any question specific to your situation, consult a lawyer specialising in data protection. This English version is a translation; the French version prevails.

Chapter 1. The legal framework: the FADP

1.1 What is the FADP?

The new Federal Act on Data Protection (FADP, SR 235.1) came into force on 1 September 2023. It entirely replaces the old act dating from 1992, a time when patient files were still on paper and the internet did not exist in medical practices.

The FADP modernises the Swiss legal framework to adapt it to today's digital realities. It aligns with the European GDPR standards while retaining Swiss specificities, in particular regarding penalties and notification deadlines.

Key point: it is the head of the practice (the dentist) who is personally responsible for protecting their patients' data. Not the IT provider, not the management software, not the cloud hosting provider.

1.2 Which data is concerned?

A dental practice processes personal data every day, much of it sensitive data within the meaning of Art. 5 let. c FADP:

- Health data: panoramic X-rays, periapical radiographs, CBCT / 3D scans, intraoral and extraoral photos, diagnoses, treatment plans, prescriptions, medical history (allergies, chronic illnesses, current treatments), surgical reports, clinical notes, complete treatment history, medical correspondence with other practitioners, laboratories or specialists
- Digital impressions and models: digital dental impressions, optical impressions from intraoral scanners, digital 3D models (health data)
- Genetic data: results of genetic analyses, if the file contains any (Art. 5 let. c no. 3 FADP)
- Administrative data: AHV numbers, dates of birth, contact details, signed consents, insurance data (basic health insurance, supplementary insurance); medical history forms, for their part, are health data
- Financial data: invoices, insurance statements, payment methods, invoicing history
- Correspondence: exchanges with patients by e-mail or messaging, exchanges with insurers, dental laboratory order forms containing patient data

Sensitive data is subject to stricter rules and requires enhanced security measures; the practice and its staff are also bound by professional secrecy (Art. 321 of the Swiss Criminal Code).

1.3 The three fundamental obligations

1. Know where your data is and how it is protected. On the practice server, on a laptop that goes home in the evening, in cloud software whose servers you do not know the location of, in your unencrypted e-mail, on a USB stick in a drawer, on an old hard drive that has never been wiped, on a dental assistant's personal phone, in e-mails sent to a laboratory via Gmail, in backups that nobody has checked for months. Often, this data is protected by a Windows password "1234", an out-of-date free antivirus, or nothing at all.
2. Notify the FDPIC in the event of an incident. Art. 24 FADP requires the controller to report as soon as possible any data security breach that is likely to result in a high risk for the personality or fundamental rights of the persons concerned. The report must state at least the nature of the breach, its consequences and the measures taken or envisaged (Art. 24 para. 2). The processor (your IT provider, for example) must report any breach to you as soon as possible, whatever its severity (Art. 24 para. 3). If the protection of patients requires it, or if the FDPIC so requests, you must also inform the persons concerned directly (Art. 24 para. 4).
3. Be able to demonstrate your compliance. In the event of an investigation, the FDPIC may ask you to prove that you have taken the necessary technical and organisational measures (Art. 8 and 49 para. 3 FADP). In practice, this means having up-to-date documentation: record of processing activities, data processing agreement signed with your IT provider, internal security policy, proof of staff training, incident response procedure, log of backups and their restore tests. A lack of documentation does not necessarily mean a penalty, but it makes your position indefensible in the event of an incident.

1.4 Notification of breaches (Art. 24 FADP)

Swiss law requires notification "as soon as possible", a deliberately flexible wording, unlike the European GDPR, which sets a strict deadline of 72 hours. The FDPIC recommends acting as quickly as possible after the breach is discovered.

The official notification portal is available at databreach.edoeb.admin.ch. With the controller's consent, the FDPIC may forward the report to the Federal Office for Cyber Security (FOCS) for analysis of the incident.

Important

A report made under Art. 24 cannot be used against the person who made it in criminal proceedings, except with their consent (Art. 24 para. 6 FADP). Notifying does not expose you. Not notifying, on the other hand, does.

1.5 Patients' rights (Art. 25 FADP)

Any patient can ask the practice whether personal data concerning them is being processed. The practice must then provide, within 30 days and free of charge:

- The identity and contact details of the controller
- The personal data processed as such
- The purpose of the processing
- The retention period or the criteria for determining it
- The origin of the data if it was not collected from the patient
- The existence of any automated individual decision and its logic
- The recipients to whom data is disclosed, including abroad

Communication of health data (Art. 25 para. 3)

Health data may be communicated to the patient through a healthcare professional designated by the patient, with their consent. This provision protects the patient against medical information that is difficult to interpret without support.

Responsibility when using a processor (Art. 25 para. 4)

If the practice uses a processor (data hosting provider, IT provider), the practice remains responsible for providing the information to the patient. You cannot refer the patient to your IT provider.

Mandatory nature of the right of access (Art. 25 para. 5)

No patient can waive their right of access in advance. Any contractual clause to that effect is null and void.

Free of charge and deadline (Art. 25 para. 6 and 7)

The information is provided free of charge, within 30 days. If it is impossible to meet this deadline (complexity, volume of data), the controller must inform the patient and justify the extension.

Patient's remedies in the event of non-compliance

If the practice refuses to reply or does not meet the deadlines, the patient has several remedies:

- A reminder to the practice by registered letter

- A complaint to the FDPIC
- Civil action before the court (Art. 32 FADP)
- A criminal complaint if the information provided is intentionally false (Art. 60 FADP)

Beware of ambiguous wording

A company lawyer was fined CHF 600 in March 2025 (Statthalteramt Bezirk Zürich, decision ST.2024.1046/ZM) for replying that a company "had found no data" when it did hold some. The misleading wording was enough to constitute the offence. Even a partly accurate answer that gives a false impression of completeness can be penalised.

1.6 Record of processing activities (Art. 12 FADP)

In principle, every controller keeps a record of its processing activities (Art. 12 para. 1 FADP). Companies with fewer than 250 employees are exempt, but this exemption lapses if they process sensitive data on a large scale or carry out high-risk profiling (Art. 12 para. 5 FADP and Art. 24 DPO). A dental practice, by its nature, processes health data, which is sensitive data: depending on the number of patients and the volume of data, the exemption may therefore not apply. In all cases, keeping one is strongly recommended, even for small organisations.

The record must contain at least: the identity of the controller, the purpose of the processing, the categories of persons and data concerned, the recipients, the retention periods and a description of the security measures in place.

1.7 Penalties (Art. 60 to 66 FADP)

Intentional violations of the FADP are punishable by fines of up to CHF 250,000. These penalties target the responsible individuals, not the company. In a dental practice, it is the practice owner who is directly concerned.

Offence	Maximum fine	Condition
Intentionally inaccurate or incomplete information	CHF 250,000	On complaint
Intentional failure to inform the person concerned	CHF 250,000	On complaint
Use of a processor without an agreement or without checking data security (Art. 9)	CHF 250,000	On complaint
Disclosure of data abroad without safeguards	CHF 250,000	On complaint
Inaccurate information to the FDPIC during an investigation	CHF 250,000	Without complaint
Refusal to cooperate with the FDPIC	CHF 250,000	Without complaint

Limitation period: 5 years (Art. 66 FADP). Retirement or ceasing to practise does not remove liability for acts committed while practising.

Only intentional violations are punishable under criminal law

Negligence is not a criminal offence under the FADP, but it can lead to civil claims from patients who have suffered harm. Good faith and responsiveness are always mitigating factors.

1.8 Major differences from the old law (DPA 1992)

The 2023 FADP is a complete revision of the 1992 act. Here are the main differences:

Old DPA (1992)	New FADP (2023)
Protects natural persons and legal entities	Protects natural persons only
No obligation to notify	Mandatory report to the FDPIC in the event of a high-risk breach
Limited and rare fines	Fines of up to CHF 250,000 (individual liability)
No obligation to carry out an impact assessment	Impact assessment mandatory for high-risk processing
Record of processing optional	Record mandatory (except for limited exemptions)
No Privacy by Design	Privacy by Design and Privacy by Default mandatory (Art. 7)
Biometric data not specifically protected	Biometric and genetic data included in sensitive data

1.9 Privacy by Design and Privacy by Default (Art. 7 FADP)

Art. 7 lays down two fundamental principles that must guide every IT decision in the practice:

Privacy by Design (data protection by design): data protection measures must be built in from the moment a software, an item of equipment or a process is chosen. It is not about fixing things afterwards, but about planning security from the outset.

Privacy by Default (data protection by default): the default settings of any system must limit the processing of data to the strict minimum necessary. By default, dental software should not share patient data with third parties or store more information than necessary.

In practice, these principles apply when choosing management software, configuring a network, setting up a new workstation or adopting a cloud tool. Every decision must include the question: "does this solution protect patient data by default?"

1.10 Data protection impact assessment (Art. 22 FADP)

An impact assessment (DPIA) is mandatory when planned processing is likely to result in a high risk for the rights of the persons concerned. Whether there is a high risk depends on the nature, scope, circumstances and purpose of the processing.

Examples requiring a DPIA

- Introducing a facial recognition system in the practice
- Large-scale profiling of patients
- Mass processing of health data with artificial intelligence
- Extensive video surveillance of the practice

Content of the impact assessment

The DPIA must contain a description of the planned processing, an assessment of the risks for the rights of the persons concerned, and the measures planned to protect those rights. If, despite the planned measures, the risk remains high, the controller must consult the FDPIC before the processing (Art. 23 FADP).

In practice for a dental practice

Most dental practices will not need to carry out a DPIA in their day-to-day work. On the other hand, introducing new software that processes patient data on a large scale, an AI tool for analysing X-rays, or a biometric access system could trigger this obligation.

1.11 Recent case law

Although the FADP is still recent, the first decisions are starting to shape how it is applied in practice.

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

A company lawyer was fined CHF 600 for replying to an access request by stating that a company "had found no data" when it did hold some. The misleading wording was enough to constitute the offence within the meaning of Art. 60 para. 1 let. a FADP.

This case shows that even a partly accurate answer that gives a false impression of completeness can be penalised. For a dental practice, this means that a patient's access request must receive a complete, precise and verifiable answer within 30 days.

1.12 Good practice for handling access requests

- Always reply within 30 days

- Provide a complete answer the first time
- Avoid ambiguous wording (never answer "we found nothing" if data exists)
- Document every request and every answer in an internal register
- Train staff to handle these requests correctly
- Designate a person responsible for handling access requests
- Verify the requester's identity before disclosing any data

Chapter 2. Secure e-mail

Sending patient data by e-mail is one of the most common practices in dental practices, and one of the riskiest. An X-ray sent via Gmail, Bluewin or Hotmail travels without end-to-end encryption, on servers that are often located outside Switzerland.

2.1 The problem

Consumer e-mail services are not designed for medical data:

- **Gmail / Hotmail / Yahoo:** servers outside Switzerland, no end-to-end encryption.
Doubly non-compliant.
- **Bluewin:** servers in Switzerland, but no end-to-end encryption. Swisscom can technically access the content. Insufficient for medical data.
- **Infomaniak Mail:** better protected than Gmail, but no native end-to-end encryption.
Suitable for non-sensitive internal exchanges, not for patient data.

2.2 Compliant solutions

- **HIN Mail:** the reference in the Swiss medical field. Secure communication between healthcare professionals, compatible with the national HIN network. The ideal solution for exchanges with doctors, laboratories and specialists.
- **Proton:** founded in 2014 at CERN in Geneva by scientists and engineers concerned about the mass surveillance revealed by Edward Snowden. The founding goal was to create communication tools that nobody, not even Proton, can read. The company is based in Geneva and subject to Swiss law, one of the strictest privacy laws in the world. According to its privacy policy, data is hosted on servers located exclusively in Switzerland, Germany or Norway; Germany and Norway are recognised by the Federal Council as offering an adequate level of protection (Annex 1 DPO).

Proton is not limited to e-mail. The complete ecosystem includes **ProtonMail** (encrypted e-mail, end to end between Proton users), **Proton Drive** (encrypted cloud storage, a compliant alternative to Google Drive or Dropbox), **Proton Pass** (encrypted password manager), **Proton VPN** (virtual private network for securing

remote connections) and **Proton Calendar** (encrypted calendar). For a dental practice, this ecosystem covers several needs with a single solution: secure e-mail for exchanges with patients and suppliers outside the HIN network, cloud storage for sensitive administrative documents, a password manager for the team, and a VPN. End-to-end encryption is only automatic between Proton users: to an address that is not with Proton (a laboratory, a patient), the message is only end-to-end encrypted if you choose a password-protected e-mail, which the recipient must enter to open it (the message expires after 28 days at the latest). Proton applies a zero-access policy: it cannot decrypt end-to-end encrypted content, even at the request of an authority. It can, however, be compelled by the competent Swiss authorities to hand over the data it holds, in particular metadata: sender and recipient addresses, message subjects, dates and times of sending and receipt.

Practical rule

If the content of the e-mail contains an X-ray, a diagnosis, an AHV number or any other identifiable patient data, it must go through end-to-end encrypted e-mail. No exceptions.

Chapter 3. Updates

Updates fix security vulnerabilities and prevent most of the most common attacks. A system that is not updated is a vulnerable system. Every day without a security update is one more open door for attackers.

3.1 Operating system

Windows and macOS must be kept up to date. Support for Windows 10 ended in October 2025: vulnerabilities discovered after that date are no longer fixed by Microsoft, except on computers enrolled in the paid Extended Security Updates (ESU) programme.

For a workstation, Windows 11 is today the only version of Windows that still receives security updates without any special arrangement. The exceptions are limited: the ESU programme extends Windows 10 by three years at most for businesses (until October 2028), at a price that doubles each year; some specialised Windows 10 LTSC editions, reserved for businesses and dedicated devices, remain supported until 2027, 2029 or 2032 depending on the edition; servers follow their own calendar (Windows Server). These are transitional solutions, not a lasting alternative: any computer running Windows 7, 8 or 10 must be replaced or migrated.

3.2 Applications and practice software

Dental software, whatever solution is used in your practice, must be updated regularly. An old version may contain exploitable vulnerabilities or cause data corruption. This concerns practice management software as well as imaging and radiology software.

Web browsers, PDF readers and office suites must also be kept up to date. They are frequent and often neglected attack vectors.

Check with your vendor that the installed version is still supported and receives security updates. If this is no longer the case, plan the migration to a recent version or an alternative solution.

Good practice

Enable automatic updates on all computers. Schedule a weekly restart so that pending security updates can be installed. A computer that is never restarted accumulates unpatched security vulnerabilities.

Chapter 4. Backups

Your backup is your last line of defence. In the event of ransomware, human error or hardware failure, it determines whether you lose everything or resume work within a few hours.

4.1 The 3-2-1 rule

3 copies of your data (the original and two backups), on 2 different media, 1 of them kept outside the practice, in another location, so that a fire, water damage or theft cannot destroy all the copies at once. This is the rule recommended by the Federal Office for Cyber Security (FOCS). It is also recommended that one of the copies be disconnected or immutable: a version that nobody can modify or delete, not even ransomware (the 3-2-1-1-0 variant, see below).

An immutable copy does not necessarily mean a hard drive to unplug every evening. Technologies such as automatic snapshots, cloud storage with immutable retention or versioned backups make it possible to protect data without daily human intervention. Your IT provider must be able to propose and set up a backup system suited to your practice, compliant with the 3-2-1 rule and documented in writing. It is not up to the practitioner to design the backup architecture; it is, however, up to them to make sure that it exists, that it works and that it is tested.

A concrete example of implementation: the practice server holds the working data (copy 1), an automatic backup is replicated to a NAS or a dedicated drive in the practice (copy 2), and a third copy is sent every night to secure cloud storage in Switzerland with immutable retention (copy 3). If ransomware encrypts the first two copies, the third remains intact and allows a complete restore.

The solution can be tailored to the size of the practice and the volume of data. Some providers apply the 3-2-1-1-0 rule, which adds to the basic rule an offline or immutable copy (the second "1") and aims for zero errors in restore tests (the "0"). What matters is not the complexity of the system, but the guarantee that your patient data can be recovered in the event of a disaster, within a timeframe compatible with the continuity of your work.

If your current IT provider cannot clearly explain your backup strategy to you, where your copies are, whether one of them is kept outside the practice, whether a copy is disconnected or immutable and when they were last tested, that is a warning sign.

4.2 Why the immutable copy is essential

Modern ransomware detects and encrypts all backups connected to the network. An external hard drive that is permanently plugged in will also be encrypted during the attack. Only a copy that is physically disconnected or logically isolated (immutable versioning) will remain intact.

4.3 Testing the restore

An untested backup is an illusion of security

Regularly test the actual restore of a sample of data, for example a few patient files or a few X-rays. The SSO and FMH recommendations require a test at least once a year; a test every month is good practice, which makes it possible to discover a problem sooner. Check that the files open correctly and that the data can be used. Without regular testing, you will discover too late that your backups are corrupted or incomplete.

Chapter 5. Passwords and two-factor authentication

5.1 The problem of weak passwords

A password like "1234", the name of the practice or a date of birth can be guessed in seconds. An account shared by the whole team makes any traceability impossible in the event of an incident. Without two-factor authentication, a single password is the only barrier between an attacker and your patient data.

5.2 Creating a strong password

At least 12 characters, combining upper-case and lower-case letters, numbers and symbols. A concrete method: choose two words with no logical connection, add a memorable number and special characters that are next to each other on the keyboard.

Example

CarmolTroppen91()=. Easy to remember, no connection with your practice or yourself.

5.3 Using a password manager

A password manager stores all your credentials in encrypted form. You only have one master password to remember.

- Proton Pass: end-to-end encrypted, servers in Switzerland, Germany or Norway
- Bitwarden: open source, can be self-hosted
- KeePass: local storage, no cloud

5.4 Two-factor authentication (2FA)

2FA adds a second check after the password: a temporary code on your phone, a push notification, or a physical key. Even if your password is compromised, the attacker cannot access the account without this second factor.

Enable it on: work e-mail, dental software (if available), cloud backups, remote access, bank accounts.

Chapter 6. Encryption of drives and archives

6.1 Encryption of workstations

A laptop stolen from a car or a server taken in a burglary gives immediate access to all the data if the drive is not encrypted. Encryption makes the data completely unreadable without the decryption key.

- **Windows:** BitLocker, built into Windows Pro and Enterprise, free. To be enabled on all computers.
- **macOS:** FileVault, built in, free. To be enabled in the system settings.
- **Servers:** hardware encryption (TPM), BitLocker or software encryption depending on the infrastructure.

6.2 Encrypted containers for sensitive archives

For external drives containing patient archives, accounts or old backups, an encrypted container works like a digital safe: accessible only with a strong password.

- **Windows:** BitLocker To Go (external drives), VeraCrypt (encrypted containers)
- **macOS:** FileVault for external drives
- **Cross-platform:** VeraCrypt: open source, robust, free

Chapter 7. WiFi network

A single WiFi network shared by staff, medical devices and patients is a major security flaw. Without separation, an infected phone connected to the guest network can reach the practice server.

7.1 The recommended configuration: three separate networks

- **Main network:** workstations, server, printers, isolated and protected.
- **Medical network:** radiology devices, sensors, connected equipment, if needed depending on the infrastructure.
- **Guest network:** patients. Internet access only, no visibility of the practice's internal network.

Separating the networks is the digital equivalent of the partition between the waiting room and the treatment room. The WPA3 protocol is recommended if the hardware supports it, WPA2 being the acceptable minimum.

WiFi password

Never display the main network password in the waiting room. The guest network can use a captive portal with a daily code or a one-off code given on request.

Chapter 8. Secure remote access

Remote access tools are essential for remote IT maintenance, but if poorly configured, they are a major way in for attackers.

8.1 The risk of free versions left permanently on standby

Typical scenario: a remote control tool, left permanently on standby with a weak password, allows an attacker to get into the practice during the night and deploy ransomware there. The practice loses several days of work, and only the data backed up out of reach can be recovered.

Leaving TeamViewer, AnyDesk or another remote access tool active 24/7 without enhanced security is like leaving a door to your practice permanently open.

8.2 Recommended solutions

Solution	Use	Security	Recommendation
Free TeamViewer / AnyDesk	Occasional	Low	To be avoided for medical data
TeamViewer Pro + 2FA	One-off	Adequate	Acceptable if properly configured
Professional VPN	Permanent	High	WireGuard or OpenVPN recommended
Business RMM	Remote maintenance	Very high	NinjaOne, Datto, Atera

Golden rule

No remote access may be configured with permanent open access. Every connection must be logged, authenticated and limited in time. The higher the level of privilege (server access, patient data), the more secure the solution must be.

Chapter 9. Phishing

Phishing remains the most common attack vector against medical practices. The attacker poses as a trusted contact (Swisscom, your bank, your IT provider) to obtain credentials or get someone to open an infected file.

9.1 Recognising a phishing e-mail

- Suspicious sender address (unusual domain, spelling mistakes)
- Artificial urgency: "Your account will be blocked in 24 hours"
- Request to click on a link or open an unexpected attachment
- Spelling mistakes or unusual wording
- Request for credentials, passwords or bank details

9.2 Advanced protection: filtering by label

E-mails from regular, trusted senders can be automatically filtered and labelled. Any e-mail claiming to come from one of these contacts but not recognised by the filter should immediately arouse suspicion.

This configuration is possible through filtering rules built into your e-mail service or through professional anti-phishing solutions. If you opt for a third-party e-mail filtering tool, be sure to check where the servers that analyse the content of your messages are located.

A solution that routes your e-mails through servers located outside Switzerland may be problematic under Art. 16 FADP, particularly if these e-mails contain patient data. Prefer solutions whose data processing takes place in Switzerland or, failing that, in a country recognised by the Federal Council as offering an adequate level of protection. Your IT provider must be able to confirm the location of the servers and the applicable protection safeguards.

Chapter 10. User access management

Defining who can access what greatly reduces internal risks and limits the damage if an account is compromised.

10.1 Principle of least privilege

Each user should only have access to the data strictly necessary for their role. This principle, widely recognised in IT security, is directly linked to Art. 8 FADP, which requires appropriate organisational measures to ensure data security.

In a dental practice, the roles are clearly distinct and access must reflect this reality. A dental assistant must be able to consult patient files and make appointments, but does not need access to the practice's accounts, HR data or server administration settings. A hygienist needs their patients' treatment history, not the unpaid invoices. An external accountant needs the financial data, not the X-rays.

If an account is compromised (successful phishing, stolen password), the principle of least privilege limits the damage: the attacker can only access the data authorised for that account. If everyone shares the same login with full access, a single compromise exposes the entire practice.

10.2 Account management rules

One account per person, never a shared account. Generic accounts such as "practice", "admin", "reception" or "accounts" make any traceability impossible. In the event of an incident, it is impossible to determine who did what and when. Each member of staff must have their own login, with a personal password that they share with no one.

Administrator accounts must be reserved for technical operations (installing software, network configuration, maintenance) and never used for day-to-day work. If your IT provider uses an administrator account, this account must be separate from those of the staff, protected by two-factor authentication and subject to connection logging.

10.3 Managing arrivals and departures

The arrival of a new member of staff must trigger the creation of a named account with rights strictly matching their role. The new member of staff must receive training on the rules for using the practice's IT systems, including the password policy and the prohibitions (WhatsApp, personal USB sticks, transferring data to unauthorised equipment).

The departure of a member of staff, whether voluntary or not, must lead to the immediate deactivation of all their access: user account, e-mail, management software, remote access, cloud storage. Do not put it off until the next day, do not postpone it to the end of the month. A disgruntled former employee who still has their access is a real risk, both for data security and for the practice's liability under the FADP.

10.4 Periodic review of access rights

Access rights are not set in stone. A member of staff may change role, a trainee may finish their placement, an external provider may stop working for the practice. Without regular checks, obsolete access builds up and creates invisible vulnerabilities.

Schedule a quarterly review: go through the list of active accounts, check that each account corresponds to a person who is still in post, that the rights granted correspond to their current role, and that all unused accounts are deactivated. Document this review in writing: it is one of the organisational measures that the FDPIC may ask to see.

10.5 Tools that make access management easier

Some equipment and technologies make it possible to centralise and simplify the management of accounts and access rights in a practice. A professional NAS server (for example of the Synology type) offers management of users and shared folders with granular permissions: each member of staff only accesses the folders authorised for their role, with logging of connections and changes. It is a suitable solution for small and medium-sized practices that do not have a dedicated server.

For practices with a more advanced Windows infrastructure, a centralised directory such as Active Directory makes it possible to manage all accounts, passwords, security groups and access policies from a single point. It makes it easier to create and delete accounts, to apply security rules automatically (password complexity, lockout after failed attempts, session expiry) and to restrict access by functional group (practitioners, dental assistants, accounts, administration). Your IT provider must be able to advise you on the solution best suited to the size and organisation of your practice.

Chapter 11. Polymorphic malware and EDR protection

Polymorphic malware is a malicious program capable of changing its own code with each infection so as not to be recognised by conventional antivirus software. It is not a new threat; these techniques have existed since the 1990s, but artificial intelligence has considerably accelerated their sophistication. What used to take an attacker weeks of development can now be generated in a few minutes.

11.1 Why conventional antivirus is no longer enough

A traditional antivirus works by signature: it compares each file with a database of known threats. If the malware changes its form with each infection, it is never recognised. It is like a security guard who only recognises criminals on file. If the criminal changes their face, they go unnoticed.

This detection model remains useful against known and widespread threats, but it is insufficient against targeted attacks or recent malware that has never been catalogued. Yet it is precisely this type of attack that hits medical practices: custom-deployed ransomware, often after a phase of reconnaissance of the victim's network.

11.2 The solution: EDR (Endpoint Detection and Response)

An EDR does not look for a known face; it observes behaviour. If a program starts opening patient files en masse and encrypting them one by one, the EDR detects it, stops it and quarantines it in real time, before it has finished. It does not matter what the program looks like or whether it has already been listed.

Beyond behavioural detection, an EDR offers capabilities that conventional antivirus does not have: automatic isolation of the compromised computer to prevent spread to the rest of the network, complete logging of the incident (which files were affected, at what time, by which process), the ability to restore modified files (rollback), and real-time alerts for your IT provider.

Recognised EDR solutions on the market include SentinelOne, CrowdStrike, Sophos Intercept X, Microsoft Defender for Endpoint and ESET Inspect. Each offers different levels of functionality and pricing; the choice should be made together with your IT provider according to the size of your practice and your existing infrastructure.

11.3 EDR, EPP, antivirus: understanding the differences

A conventional antivirus detects known threats by signature. An EPP (Endpoint Protection Platform) combines antivirus with additional layers: local firewall, USB device control, web filtering. An EDR goes further by adding behavioural analysis, automated response and complete visibility of what is happening on each computer. For a dental practice processing sensitive data, an EDR managed by your IT provider is the recommended level of protection.

For example, a conventional antivirus such as Windows Defender (included free of charge in Windows) offers basic signature-based protection. An EPP such as Bitdefender GravityZone or ESET Protect adds further layers of prevention. An EDR such as SentinelOne or CrowdStrike Falcon adds behavioural detection and automated response. The cost increases with the level of protection, but the financial consequences of a successful attack far exceed the investment in a suitable solution.

11.4 The role of the IT provider

An EDR does not configure itself. It requires settings adapted to your environment (exclusion of legitimate dental software, alert thresholds, automatic response policy) and regular monitoring of the alerts it generates.

Your IT provider must be able to deploy, configure and monitor this solution. Ask them whether they use an EDR on the computers they manage, whether they receive alerts in real time and how quickly they react when an active threat is detected. If your provider merely installs a free antivirus without monitoring, the level of protection is insufficient for medical data subject to the FADP.

Chapter 12. Modernising the IT equipment

Never leave one or two old workstations in a modern practice. A single obsolete or unpatched computer is enough to compromise the whole network. In a dental practice, this means a real risk of a leak or a ransom demand involving X-rays, diagnoses, administrative or accounting data. A single weak link is enough to endanger the whole practice.

12.1 Why an obsolete computer is dangerous

An outdated Windows computer, or one that is never restarted, accumulates known and publicly documented security vulnerabilities. Attackers have databases listing these vulnerabilities and automated tools to exploit them. If one of them is exploited, the attack chain is predictable: gain initial access to the local network through the vulnerable computer, get around the protections of the recent computers by moving laterally across the network, reach the storage server, access the practice software or the backups, then steal or encrypt the sensitive data. All of this can happen within a few hours, often at night or at the weekend when nobody is watching.

The problem does not only concern the visible workstations. Often-forgotten equipment is just as critical: an old server still running "for the time being", a network printer whose firmware has never been updated, an old-generation WiFi router, a NAS whose operating system is obsolete. Each of these devices is a potential point of entry.

12.2 Recommended replacement cycle

The practical rule is to replace workstations every 5 years at most. This period is not arbitrary: it corresponds to the average length of time during which a manufacturer guarantees compatibility with security updates for the operating system and hardware components (drivers, firmware, TPM module).

What really matters is not the age of the computer as such, but its ability to receive the latest security updates. A 4-year-old computer compatible with Windows 11 with a TPM 2.0 module is in a better security state than a 2-year-old computer stuck on a system at the end of support.

For a workstation, Windows 11 is today the only version of Windows supported by the vendor without any special arrangement. A computer running Windows 7 or 8 no longer receives any security updates; a computer running Windows 10 only receives them if it is enrolled in the paid ESU programme (three years at most for businesses, until October 2028) or if it uses a specialised LTSC edition (see chapter 3). These solutions merely postpone the deadline. Keeping a computer that no longer receives security updates on the practice network is like leaving a door permanently open, whatever the level of protection of the other equipment.

12.3 Special case: iMacs running Boot Camp

Some practices still use Intel iMacs with Windows installed via Boot Camp. This configuration poses a twofold problem: these iMacs often can no longer be upgraded either to Windows 11 (because they lack a TPM 2.0 module) or to the latest versions of macOS (Apple having stopped supporting the oldest Intel models). These machines are reaching the end of their life on both sides at the same time.

The solution is to replace them with dedicated Windows 11 PCs. Dental management and imaging software runs exclusively on Windows; a Mac therefore brings no functional advantage in this context and complicates maintenance, updates and hardware compatibility.

12.4 Planning the migration

Replacing the IT equipment must not be done in a hurry on the day a computer breaks down or becomes the target of an attack. It must be planned in advance, together with your IT provider. Here are the recommended steps:

Start with a complete inventory of the equipment: each workstation, each server, each network device, with the operating system installed, the date of purchase or commissioning, and compatibility with current updates. Identify the computers at the end of their life or end of support. Draw up a realistic replacement schedule, spread over several months if necessary to spread the investment. Plan the migration of data and practice software, the reconfiguration of network access and the check that each computer works properly before it goes into production.

Document this inventory and schedule in writing. It is one of the organisational measures demonstrating your compliance with Art. 8 FADP.

12.5 Secure destruction of old equipment

Replacing a computer does not end with installing the new one. The old equipment potentially contains patient data on its hard drive, even if you think you have erased everything. A simple format is not enough: recovery tools can retrieve data that has been deleted in the conventional way.

Two options comply with the FADP: secure erasure using specialised software (multiple overwriting of the data, making any recovery impossible) or physical destruction of the storage medium (shredding, degaussing). In both cases, ask your IT provider for a certificate of destruction and keep it in your compliance documentation. This certificate is proof that patient data has not been abandoned on an unsecured medium.

Chapter 13. The data processing agreement (Art. 9 FADP)

Art. 9 of the FADP strictly governs the processing of personal data by processors. In practice, this directly concerns the relationship between a dental practice and any third party that accesses, stores, processes or transports your patients' personal data on your behalf.

Without a compliant data processing agreement, you still have recourse against the provider under the Code of Obligations, but it is much harder to enforce. And in the event of an incident, it is you, the head of the practice, who answers to the FDPIC and to your patients. Intentionally entrusting data to a provider without an agreement, or without checking that it guarantees data security, is punishable, on complaint, by a fine of up to CHF 250,000 (Art. 61 let. b FADP).

13.1 Preconditions for using any processor

Even before drafting an agreement, Art. 9 para. 1 lays down two conditions that the controller must check. First, the processor may only carry out processing that the practice itself would be entitled to carry out. If a processing operation is prohibited for you, you cannot entrust it to a third party to get around the prohibition. Second, no legal or contractual duty of secrecy may prohibit this delegation. In the medical context, professional secrecy (Art. 321 of the Swiss Criminal Code) calls for particular vigilance regarding the data that the processor will actually be able to access.

Art. 9 para. 2 adds an active obligation to check: the controller must make sure that the processor is able to guarantee data security. This is not a formality. You must be able to show that you checked your provider's skills, tools and security practices before giving them access to your infrastructure.

13.2 Who is concerned by the data processing agreement?

The data processing agreement does not only concern your IT provider. Any person or company that accesses your patients' personal data on your behalf is a processor within the meaning of the FADP. Here are the most common cases in a dental practice:

Your IT provider, who accesses the computers, servers, backups and potentially patient data during maintenance work. Your cloud hosting provider, if your data or backups are stored with an external supplier. A dental laboratory, if it receives digital files containing identifiable patient data (optical impressions, X-rays with the patient's name). An external accountant or fiduciary, if they access invoicing data containing patient information. A dental software vendor, if the software runs in the cloud and the data is hosted on the vendor's servers.

For each of these processors, an agreement compliant with Art. 9 FADP must be in place.

13.3 What the agreement must contain

The agreement must clearly define the framework within which the processor is authorised to process data:

- The nature of the data accessible to the processor and the categories of persons concerned (patients, staff, suppliers).
- The purpose of the processing, limited to the practice's instructions. The processor may not use the data for other purposes, sell it or disclose it to third parties without the controller's prior instructions.
- The list of tools used and the location of the servers. This point is directly linked to Art. 16 FADP: if the provider's tools store data on, or route it through, servers located outside Switzerland, the safeguards ensuring adequate protection must be documented in the agreement.
- The technical and organisational security measures put in place by the processor (encryption, access control, logging, antivirus or EDR).
- The incident notification procedure with a defined deadline. Art. 24 para. 3 FADP requires the processor to inform the controller as soon as possible in the event of a data security breach. The agreement must specify a concrete deadline, for example 24 hours after detection.
- The end-of-contract procedure: removal of all access, return or deletion of the data held, written confirmation that these measures have been carried out.
- The prohibition on delegating processing to third parties without the practice's prior authorisation (Art. 9 para. 3 FADP), ideally given in writing. If your IT provider itself uses sub-processors (for example a cloud hosting provider for your backups), this must be declared and governed by contract.
- A confidentiality clause with no time limit, including after the end of the agreement.

It is not a 40-page document. A well-drafted agreement fits into 9 articles, can be read in 5 minutes and signed in 2.

13.4 Checking your provider's tools

The agreement must include a table or an annex listing the tools used by the provider in the course of its work, with the purpose and the location of the data for each one. For example: the remote maintenance tool used, the monitoring solution, the password manager, the backup solution, the business e-mail. For each tool whose servers are located outside Switzerland, check whether the country concerned is recognised by the Federal Council as offering an adequate level of protection (Art. 16 para. 1 FADP), or whether additional contractual safeguards are in place (Art. 16 para. 2).

13.5 Responsibility towards patients (Art. 25 para. 4)

Even if a processor processes data on your behalf, you remain your patients' sole point of contact. Art. 25 para. 4 FADP is explicit: a controller who has data processed by a processor remains obliged to provide the information requested by the person concerned. You cannot refer a patient to your IT provider when they ask for access to their data. It is up to you to reply, within 30 days, even if this requires you to call on your processor to obtain the information.

13.6 My current provider has no agreement: what should I do?

If no data processing agreement is currently in place with your IT provider or your other processors, the process is simple. Contact your provider and ask whether they have an agreement compliant with Art. 9 FADP. If they offer one, read it carefully and check that it covers the points listed above. If they do not, that is a warning sign about their level of maturity in data protection. You can provide them with a template agreement or have one drafted by a lawyer specialising in the field.

The absence of an agreement does not mean that the collaboration must stop immediately, but regularising the situation must be a priority. If an incident occurs with no agreement in place, your position will be considerably weakened, both towards the FDPIC and towards your patients.

You delegate the technical side. Never the responsibility.

Chapter 14. Staff training

Technology is not enough if the people who use it are not trained. Human errors (a phishing e-mail opened, an unlocked screen, a patient file left at reception, an X-ray sent by WhatsApp) account for a significant share of data breaches. Most of these incidents are not the result of malicious intent, but of a lack of awareness and clear rules.

14.1 An implicit obligation under the FADP

Art. 8 FADP requires the controller to take appropriate organisational and technical measures to ensure data security. Staff training is one of these organisational measures. In its explanatory report on the FADP published by the Federal Office of Justice, the Federal Council explicitly stresses that the effective implementation of data security depends on the people involved being properly trained. A lack of training could lead to data security breaches, for example if a member of staff opens an e-mail containing malicious software.

Under Swiss employment law, the employer may issue instructions, which employees must follow (Art. 321d CO). Train your staff and give them the rules in writing: without this, a security failing will be hard to hold against them, and a dismissal on that ground, especially a summary dismissal, could be challenged.

14.2 Recommended content of a training session

The training must cover the real situations that staff face every day.

Recognising fraud attempts. E-mail phishing is the most common vector, but it is not the only risk. The training must include fraudulent phone calls (someone poses as the IT provider and asks for a password, a supposed employee of the dental software vendor asks for remote access, a stranger introduces themselves as a patient and asks for medical information over the phone), fraudulent text messages and messages, and unknown USB sticks found in or near the practice. Concrete examples and practical exercises help people remember.

Rules for locking computers. Lock the screen every time you leave your workstation, even for a few seconds. The Windows+L combination on Windows or Ctrl+Command+Q on macOS must become a reflex. An unlocked screen in a room accessible to patients is a potential breach of confidentiality.

Password policy. Mandatory use of the practice's password manager, two-factor authentication enabled on all critical access, a ban on writing passwords on sticky notes or in unencrypted files.

Using secure e-mail. Knowing when to use encrypted e-mail (any content containing identifiable patient data) and when standard e-mail is acceptable (internal exchanges without sensitive data, orders for supplies). A strict ban on using consumer messaging services (Gmail, Hotmail, WhatsApp) for any communication containing patient data.

Incident procedure

Every member of staff must know what to do if an attack or a leak is suspected: whom to call first (the responsible practitioner, then the IT provider), what to do immediately (unplug the network cable, do not switch the computer off), what not to do (do not try to solve the problem yourself, do not pay a ransom, do not delete suspicious messages before they have been documented).

Handling patient data. Never send patient data via WhatsApp, text message or personal e-mail. Do not copy data to personal USB sticks, personal hard drives or unauthorised cloud services. Do not transfer patient files to a personal computer, including to "work from home".

Physical security and clean desk policy. Never leave patient files, printed X-rays or administrative documents containing personal data visible on a counter, a desk or near reception.

Paper documents containing patient data must be destroyed with a shredder, never thrown in the bin. Screens visible from the waiting room or passageways must be positioned accordingly or fitted with privacy filters.

Professional secrecy. A reminder of the criminal-law obligations: Art. 321 of the Swiss Criminal Code punishes the disclosure of secrets confided in the course of professional practice. This obligation applies to all practice staff, not just the practitioner.

14.3 Personal devices and BYOD

The use of personal devices (phones, tablets, laptops, USB sticks) to access the practice's data must either be prohibited or strictly governed by a written rule. If a member of staff uses their personal phone to read work e-mails, the patient data in those e-mails ends up on a device not controlled by the practice, potentially unencrypted, and liable to be lost, stolen or compromised. The practice's policy must clearly define which devices are authorised, which applications may be used, and which data may pass through them.

14.4 Temporary staff and third parties

Trainees, locums, cleaning staff, external technicians and anyone else with physical access to the practice's premises must be taken into account in the security policy. A trainee present for two weeks can see the same screens as a permanent employee. Cleaning staff working outside opening hours have access to offices, printers and potentially to documents left visible. External technicians (medical equipment suppliers, installers) may need temporary access to the network.

Everyone with physical or digital access, even temporary, must receive a minimum of information about the practice's confidentiality rules. For temporary staff, a one-page summary document setting out the essential rules, signed on arrival, is sufficient.

14.5 The written internal security policy

Oral training is not enough. The practice must have an internal IT security policy set down in writing, given to each member of staff on arrival and updated at least once a year. This document is the reference in the event of a dispute and protects the practitioner in the event of an incident: it shows that rules existed, that they were communicated and that the member of staff took note of them.

The policy must cover at least the rules for using workstations, the password policy, the rules on e-mail and communications, the prohibition or regulation of personal devices, the incident procedure, and the internal penalties for non-compliance. Each member of staff signs a copy confirming that they have read, understood and accepted the rules. This signature is kept in the staff file.

14.6 Frequency, format and assessment

Training must take place at least once a year for all staff, with a dedicated session whenever a new member of staff arrives, including trainees and locums. The format can be an internal presentation of 30 to 60 minutes, supplemented by handing over the internal policy document.

To assess the effectiveness of the training, practical exercises are recommended: phishing simulations (sending a fake fraudulent e-mail to check how staff react), quick quizzes on good practice, role plays (a member of staff receives a call asking for a password). These exercises are not meant to catch staff out but to identify weak points and adapt the next training session accordingly.

Document each session: date, participants, topics covered, results of the exercises where applicable. This documentation is one of the organisational measures that the FDPIC may ask to see during an inspection.

14.7 Shared responsibility

If a dental assistant sends an X-ray on WhatsApp, they may incur personal criminal liability if this amounts to intentional disclosure of data covered by secrecy (Art. 62 FADP on the duty of confidentiality and Art. 321 SCC on professional secrecy, which also covers dentists' assistants; offences prosecuted on complaint). Mere negligence is not punishable under these two articles. But the dentist is the one who notifies the FDPIC and answers to the patients. Their own exposure depends on the measures they had put in place: a written and

signed internal policy, training given and documented, appropriate access management. If nothing was in place, they share the exposure for failing to prevent the risk. If everything was in place and documented, their position is considerably stronger.

Chapter 15. Cyber insurance

Even with an excellent level of IT security, there is no such thing as zero risk. Cyber insurance makes it possible to transfer part of the financial risk to an insurer and to receive professional help in a crisis.

15.1 What cyber insurance covers

The cyber insurance policies offered in Switzerland generally cover:

- The costs of emergency IT response (forensics, restoration)
- Loss of revenue due to business interruption
- The costs of mandatory notification (FDPIC, patients concerned)
- Civil liability for damage to third parties' data
- Crisis management and communication costs
- Legal costs related to the incident

15.2 Main insurers in Switzerland

Several Swiss insurers offer policies specially designed for SMEs:

- **Zurich:** a modular policy in 4 variants, including free cybersecurity training for policyholders.
- **Helvetia:** cyber insurance with a 24/7 hotline and a network of specialist partners, cyber-safe label for a 20% discount.
- **AXA:** protection on three levels: prevention, emergency assistance, repair.
- **Baloise:** three policies (ECO, SMART, TOP) with ransom cover under certain conditions.
- **Allianz:** Cyber Risk with business interruption cover for 24 months.

15.3 Points to watch

Before taking out a policy, check carefully:

- The exclusions (some policies exclude attacks if updates had not been installed)

- The amount of the excess, sometimes high for SMEs
- The security preconditions required by the insurer
- The coverage limit and whether it matches your actual exposure
- Whether or not ransom payments are covered (policy varies between insurers)

Advice

Cyber insurance does not replace security measures; it complements them. An insurer will require a minimum level of protection (antivirus, backups, passwords) before agreeing to cover you. It is a virtuous circle: the better protected you are, the lower the premium.

Chapter 16. What to do in an incident

If it happens (and statistically, for some practices, it will), the first minutes are decisive.

16.1 Scenario A: active attack (ransomware, intrusion)

Step 1. ISOLATE: unplug the network cable, turn off the WiFi. Do not switch the computer off; that destroys evidence useful for the analysis.

Step 2. CALL IT: your IT provider first. If unavailable, the FOCS via incidents@ncsc.ch or the form at report.ncsc.admin.ch.

Step 3. DO NOT PAY: the official recommendation of the Swiss Confederation. Paying does not guarantee that the data will be recovered and finances criminal networks.

Step 4. DOCUMENT: photograph the error screens, note the exact time of discovery, keep everything. This information will be needed for the insurer, the police and the legal notification.

Step 5. ASSESS: is the breach likely to result in a high risk for patients (e.g. health data stolen, exposed or encrypted by ransomware)? If so, or if you cannot rule it out quickly, reporting to the FDPIC is mandatory (Art. 24 para. 1 FADP).

Step 6. NOTIFY: databreach.edoeb.admin.ch, as soon as possible.

16.2 Scenario B: accidental loss or leak

Loss of a data medium, sending to the wrong recipient, accidental deletion, unauthorised access discovered: the procedure is similar: document, assess the risk for patients, notify the FDPIC if the risk is high, inform patients if necessary.

16.3 What the FDPIC actually does

It is not a raid on your practice. The FDPIC reads your report, checks that you reacted correctly, and may ask for further details or give advice.

The FDPIC cannot impose a fine directly. Criminal penalties go through the cantonal authorities and target intentional violations, not practices that have notified in good faith.

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

Chapter 17. Real cases in French-speaking Switzerland

These attacks are not theoretical. They have hit medical organisations in French-speaking Switzerland, in environments comparable to a dental practice.

Groupe 3R, Réseau Radiologique Romand (April 2025 and April 2026)

Twenty medical imaging centres spread over seven cantons. Ransomware, theft of medical and administrative data, attempted extortion. The ransom was refused. The incident was reported to the FOCS. The group suffered a second ransomware attack in April 2026; it again refused to pay, and stolen data was published on the internet.

Vidymed, Lausanne (December 2024)

An IT intrusion detected on 7 December 2024 in four medical centres in Lausanne and Épalinges: all IT systems were suspended and staff went back to paper. Most of the data was only restored five weeks later. A situation that would paralyse any dental practice.

Switzerland in figures

In 2025, the Federal Office for Cyber Security (FOCS) received 64,733 voluntary reports of cyber incidents (FOCS annual report 2025).

Typical attack scenarios in the medical field

Beyond the real cases above, here are four typical scenarios, built from the most common attacks against practices. They show how an attack most often begins:

Ransomware via unsecured remote access

A remote control tool is left permanently open, protected by a short password, to make the provider's work easier. An attacker guesses it through automated attempts and takes control of the server during the night. The ransomware spreads to the whole network: the practice stays closed for several days, and only the data backed up out of reach can be recovered.

Phishing with a fake telecom operator invoice

An e-mail imitates a telecom operator's invoice, with the subject "Your unpaid invoice". Once the attachment is opened, ransomware encrypts the network, including the permanently connected backups. Without a copy out of reach, the practice no longer has any usable copy of its data.

Impersonation of the IT provider

An attacker poses as the practice's IT provider and asks for the login details "for an urgent update". A dental assistant passes them on in good faith. The attacker accesses the server and copies patient files before being detected.

Infected USB stick

A USB stick "forgotten" in the practice car park is labelled "Salaries". Once plugged into a computer, it installs spyware that records the passwords typed on the keyboard: those for the dental software, the e-mail and online banking are compromised.

What an attack costs

Days, sometimes weeks, of working at reduced capacity: at Vidymed, it took five weeks to recover most of the data. Add to that the recovery work, the specialists' intervention, informing patients and the loss of their trust.

Compliance checklist

Use this list to assess your current level of compliance and improve what is missing from your current infrastructure. Each unticked point is a risk to be dealt with. A glossary of technical terms is available at the end of the list.

Communications

- Encrypted e-mail used for all patient data (HIN Mail, ProtonMail or equivalent)
- No patient data sent via Gmail, Hotmail, Bluewin, WhatsApp or text message
- Paper documents containing patient data destroyed with a shredder

Infrastructure

- All computers running Windows 11 or an up-to-date macOS
- No computer running Windows 7, 8 or 10 on the network
- Automatic updates enabled on all computers, servers and applications
- Drive encryption enabled on all computers and servers (BitLocker / FileVault)
- Patient WiFi separate from the practice network

Backups

- 3-2-1 strategy in place (3 copies, 2 media, 1 outside the practice), with a disconnected or immutable copy
- Restore tested regularly (at least once a year, ideally every month)

Access and authentication

- One named account per member of staff, no shared accounts
- Passwords of 12+ characters, stored in a secure password manager
- 2FA enabled on e-mail, management software and remote access
- Former staff accounts deactivated
- Remote access via VPN or professional RMM only

FADP compliance

- Art. 9 data processing agreement signed with the IT provider

- Data processing agreement in place with every third party accessing patient data
- Internal security policy drawn up and signed by each member of staff
- Staff training carried out in the last 12 months
- Incident response plan documented and accessible
- Emergency contacts displayed (IT provider, FOCS, FDPIC)

Protection and follow-up

- EDR solution deployed and monitored
- Annual security audit carried out
- Cyber insurance taken out and conditions checked

Checklist glossary

Encrypted e-mail: an e-mail service whose content is locked when it is sent and can only be read by the recipient. Neither the provider nor a hacker intercepting the message can access it. Examples: HIN Mail, ProtonMail.

3-2-1 backup: 3 copies of your data, on 2 different media, 1 of them kept outside the practice. It is recommended that one of the copies also be disconnected or immutable (protected against any modification or deletion, even by a virus): this is the 3-2-1-1-0 variant.

BitLocker / FileVault: encryption tools built into Windows (BitLocker) and macOS (FileVault) at no extra cost. They make the content of the hard drive completely unreadable if the computer is stolen.

2FA (two-factor authentication): a second check after the password, usually a temporary code displayed on the phone. The same principle as a bank card: the number alone is not enough, you also need the PIN.

VPN: an encrypted connection between a remote device and the practice network. It protects data in transit like a private tunnel.

RMM: professional remote maintenance software that logs every connection, applies updates and monitors computers continuously. A secure alternative to free tools such as TeamViewer.

EDR: advanced protection that analyses the behaviour of programs in real time and blocks suspicious actions, even unknown ones. It goes beyond conventional antivirus, which only detects threats that have already been listed.

Art. 9 FADP: the article of law governing processors. A third party may process patient data for the practice (IT provider, cloud hosting provider, laboratory, accountant) only if an agreement or the law provides for it, and the practice must ensure that it is able to guarantee data security. Writing is not required, but it is the surest way to prove the agreement.

Intentionally entrusting data without meeting these conditions is punishable, on complaint, by a fine of up to CHF 250,000 (Art. 61 let. b).

FOCS: Federal Office for Cyber Security. The body to contact in the event of a cyberattack. Contact: incidents@ncsc.ch or report.ncsc.admin.ch.

FDPIC: Federal Data Protection and Information Commissioner. The authority to which a high-risk data security breach must be reported (Art. 24 FADP). Contact: +41 58 462 43 95 or databreach.edoeb.admin.ch.

Useful contacts and resources

Emergency contacts

- **FOCS:** Federal Office for Cyber Security: incidents@ncsc.ch / report.ncsc.admin.ch
- **FDPIC:** Federal Data Protection and Information Commissioner: +41 58 462 43 95
(Mon-Fri 10:00-12:00) / databreach.edoeb.admin.ch
- **Cantonal police:** 117

Legal texts

- **FADP (SR 235.1):** www.fedlex.admin.ch
- **Data Protection Ordinance (DPO):** www.fedlex.admin.ch
- **FDPIC guide on data breaches:** www.edoeb.admin.ch
- **SME data protection guide:** www.kmu.admin.ch

Further resources

- **FMH:** tools and templates for medical practices: www.fmh.ch
- **HIN:** information security for the medical field: www.hin.ch
- **No More Ransom (decryption help):** www.nomoreransom.org

Frequently asked questions

The following questions are the ones practitioners ask most often. They come from real situations encountered in dental practices in French-speaking Switzerland.

Is an accidental loss of data a breach within the meaning of the FADP?

Yes. Art. 5 let. h FADP defines a data security breach as any loss, modification, deletion or destruction of personal data, whether accidental or unlawful. Deleting patient files by mistake, losing a hard drive or suffering a server failure with no backup: all of this falls within this definition. If the risk for patients is high, notifying the FDPIC is mandatory.

My IT provider deleted data. Who is responsible?

You, the dentist, as the controller (Art. 9 and Art. 25 para. 4 FADP). You cannot refer the patient to your IT provider. Your recourse against the provider is much stronger with a compliant data processing agreement; without one, it remains possible under the Code of Obligations, but harder to enforce. You delegate the technical side, never the responsibility.

I retired 3 years ago and a leak dating back 4 years has been discovered. Am I still concerned?

Yes. Art. 66 FADP sets the limitation period for criminal prosecution at 5 years. Retirement or ceasing to practise does not remove liability for acts committed while practising. The exact starting point (date of the leak or date of discovery) requires a lawyer's opinion, but the 5-year period is confirmed by law.

My iMacs run Windows 10 via Boot Camp: can we go back to macOS?

No, and that would not solve anything. Dental software (Sidexis, Romexis, DBSWin, Cliniview, DTX Studio) runs exclusively on Windows. In addition, these Intel iMacs often can no longer be upgraded either to Windows 11 or to the latest versions of macOS. They are at the end of their life on both sides. The solution: replace them with dedicated Windows 11 PCs.

Which dental software should I choose?

This guide does not publicly recommend or advise against any specific software. On the other hand, here are the security criteria to check: does the software offer two-factor authentication (2FA) natively? Does the vendor publish regular security updates? Where is the data hosted?

Does the development team have documented security skills? Critical medical software is an IT product: ask yourself whether the vendor has the means to keep developing it over time.

A dental assistant sends an X-ray on WhatsApp. Who is responsible?

Both, but not for the same reasons. The dental assistant may incur personal criminal liability if sending it amounts to intentional disclosure of data covered by secrecy: Art. 62 FADP (breach of the duty of confidentiality) and Art. 321 of the Swiss Criminal Code (professional secrecy, which also covers dentists' assistants), on complaint. A mistake through mere negligence is not punishable under these articles. The dentist, for their part, is the one who notifies the FDPIC and answers to the patients. Their own exposure depends on the measures they had put in place: a written internal policy, training given, access management. If none of this existed, they share the exposure for failing to prevent the risk.

Does the FDPIC carry out inspections in practices?

The FDPIC can open an investigation on its own initiative or following a report, if there are sufficient indications that processing could breach data protection provisions (Art. 49 FADP). The real sources of risk for a dentist are a dissatisfied patient, an incident that becomes public, or a complaint from a former employee.

Does the FADP impose a 72-hour deadline like the GDPR?

No. Swiss law requires notification "as soon as possible", a deliberately more flexible wording than the European GDPR, which sets a strict deadline of 72 hours. The FDPIC recommends acting "as quickly as possible". In practice: act as soon as you become aware of the breach, and complete the documentation afterwards if necessary. There is no specific penalty for a delay, but responsiveness is a factor taken into account when assessing good faith.

Glossary

The following terms are used in this guide and in the FADP. This glossary defines them in language accessible to non-specialists.

Term	Definition
FADP	The new Federal Act on Data Protection (SR 235.1), which came into force on 1 September 2023.
FDPIC	Federal Data Protection and Information Commissioner. The independent supervisory authority responsible for ensuring compliance with the law.
FOCS	Federal Office for Cyber Security (formerly NCSC/MELANI). The Confederation's centre of expertise for cyber threats.
Personal data	All information relating to an identified or identifiable natural person (Art. 5 let. a).
Sensitive data	A category with enhanced protection: health data, religious/political opinions, genetic and biometric data, criminal proceedings, social assistance (Art. 5 let. c).
Controller	The person who determines the purposes and means of the processing. In a dental practice: the practice owner (Art. 5 let. j).
Processor	The person who processes data on behalf of the controller. Example: the practice's IT provider (Art. 5 let. k).
Security breach	Any loss, modification, deletion, destruction or disclosure of, or unauthorised access to, personal data, whether accidental or unlawful (Art. 5 let. h).
Privacy by Design	The obligation to build data protection into a system or process from the design stage (Art. 7 para. 1).
Privacy by Default	The obligation to limit processing by default to the strict minimum necessary (Art. 7 para. 3).

DPIA	Data protection impact assessment. Mandatory when processing presents a high risk (Art. 22).
2FA / MFA	Two-factor authentication / multi-factor authentication. A second check after the password (text message code, app, physical key).
EDR	Endpoint Detection and Response. A security solution that detects threats through real-time behavioural analysis rather than by signature.
Ransomware	Malicious software that encrypts data and demands a ransom to unlock it.
Phishing	A fraud technique using e-mail, text messages or the phone to obtain credentials or get someone to open an infected file.
BitLocker	An encryption tool built into Windows Pro/Enterprise. It makes data unreadable without the decryption key.
FileVault	The macOS equivalent of BitLocker. Built-in encryption of the system drive.
VPN	Virtual Private Network. An encrypted tunnel providing secure remote access to the practice network.
RMM	Remote Monitoring and Management. A professional remote maintenance solution with traceability (NinjaOne, Datto, Atera).
3-2-1 rule	Backup strategy recommended by the FOCS: 3 copies of the data, on 2 different media, 1 of them outside the practice. The 3-2-1-1-0 variant adds an offline or immutable copy (protected against modification) and aims for zero errors in restore tests.
WPA3 / WPA2	WiFi security protocols. WPA3 is the most recent and most secure version; WPA2 is the acceptable minimum.
HIN	Health Info Net. A secure Swiss network for exchanges between healthcare professionals.

DPO	Data Protection Ordinance. The implementing text of the FADP, setting out the technical and organisational details.
-----	---

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 guide (DS1) and the quick-reaction sheet (DS2) are made available free of charge. They may be freely downloaded, printed and distributed within a dental practice or a medical organisation, without modification and with mention of their author (DentalSystems Sàrl). The templates in the kit (DS3 to DS11) may be modified and used under the practice's name, including with its patients, staff and providers, without keeping the references to DentalSystems Sàrl.

Prohibited use

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

- Selling or marketing these documents in any form whatsoever, including in modified form.
- Distributing a modified version of the guide or the quick-reaction sheet, or presenting them as the work of another author.
- Removing, altering or concealing, in the guide and the quick-reaction sheet, the author's name, the logo or the contact details of DentalSystems Sàrl.
- Offering these documents for download to third parties (download sites, sharing platforms, resellers).

Any unauthorised commercial use constitutes a breach of copyright and may lead to legal proceedings. In the event of a discrepancy, the terms of use published on www.dentalsystems.ch prevail.

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 direct or indirect consequences of its use; this limitation does not apply in the event of intent or gross negligence (Art. 100 CO). Users remain solely responsible for adapting this information to their specific situation. This document 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.