GUIDE DE RÉFÉRENCE

Cybersécurité & nLPD

Protéger les données de vos patients.

Sécuriser votre infrastructure informatique.

Comprendre vos obligations légales.

DentalSystems Sàrl

Thomas Alvino, Technicien IT

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

Mars 2026. Conforme à la nLPD (RS 235.1)

TABLE DES MATIÈRES

Introduction

Ce guide s'adresse aux médecins-dentistes, aux responsables de cabinets et à leurs équipes. Il a été rédigé à la suite de la conférence organisée par la Société Suisse d'Odontostomatologie, Section Neuchâtel (SSO-NE), le 12 mars 2026, consacrée à la cybersécurité et à la conformité à la nouvelle Loi fédérale sur la Protection des Données (nLPD).

La nLPD, entrée en vigueur le 1er septembre 2023, impose aux cabinets dentaires des obligations concrètes en matière de protection des données patients. Ces données (radiographies, diagnostics, numéros AVS, plans de traitement) sont classées comme données sensibles et bénéficient du niveau de protection le plus élevé prévu par la loi.

Ce document couvre l'ensemble des thématiques abordées lors de la conférence, approfondies et complétées par deux sujets supplémentaires : la formation du personnel et les assurances cyber. Il est conçu comme un ouvrage de référence durable, à conserver et à consulter au quotidien.

À propos de ce guide

Ce document est fourni à titre informatif et éducatif. Il ne constitue pas un avis juridique. Pour toute question spécifique à votre situation, consultez un juriste spécialisé en protection des données.

Chapitre 1. Le cadre légal : la nLPD

1.1 Qu'est-ce que la nLPD ?

La nouvelle Loi fédérale sur la Protection des Données (nLPD, RS 235.1) est entrée en vigueur le 1er septembre 2023. Elle remplace intégralement l'ancienne loi qui datait de 1992, une époque où les dossiers patients étaient encore sur papier et où Internet n'existait pas dans les cabinets médicaux.

La nLPD modernise le cadre juridique suisse pour l'adapter aux réalités numériques actuelles. Elle s'aligne sur les standards européens du RGPD tout en conservant des spécificités suisses, notamment en matière de sanctions et de délais de notification.

Point essentiel : c'est le responsable du cabinet (le médecin-dentiste) qui est personnellement responsable de la protection des données de ses patients. Pas le prestataire informatique, pas le logiciel de gestion, pas l'hébergeur cloud.

1.2 Quelles données sont concernées ?

Un cabinet dentaire traite quotidiennement des données qui entrent dans la catégorie des données sensibles au sens de l'Art. 5 let. c nLPD :

- Données de santé : radiographies panoramiques, clichés rétro-alvéolaires, CBCT / scans 3D, photos intra-orales et extra-orales, diagnostics, plans de traitement, prescriptions, antécédents médicaux (allergies, maladies chroniques, traitements en cours), comptes-rendus opératoires, notes cliniques, historique complet des soins, correspondances médicales avec d'autres praticiens, laboratoires ou spécialistes
- Données biométriques : empreintes dentaires numériques, empreintes optiques issues de scanners intra-oraux, modèles 3D numériques
- Données génétiques : certains examens dentaires peuvent révéler des informations à caractère génétique, explicitement protégées par l'Art. 5 let. c ch. 3 nLPD
- Données administratives sensibles : numéros AVS, dates de naissance, coordonnées, formulaires d'anamnèse, consentements signés, données d'assurance (LAMal, complémentaires)
- Données financières : factures, relevés d'assurance, modes de paiement, historique de facturation
- Correspondance : échanges avec les patients par e-mail ou messagerie, échanges avec les assurances, bons de commande aux laboratoires dentaires contenant des données patient

Ces données bénéficient du niveau de protection le plus élevé prévu par la loi. Leur traitement requiert des mesures de sécurité renforcées.

1.3 Les trois obligations fondamentales

1. Savoir où sont vos données et comment elles sont protégées. Sur le serveur du cabinet, sur un portable qui rentre à la maison le soir, dans un logiciel cloud dont vous ignorez où se trouvent les serveurs, dans votre messagerie non chiffrée, sur une clé USB dans un tiroir, dans un ancien disque dur jamais effacé, sur le téléphone personnel d'une assistante, dans les e-mails envoyés à un laboratoire via Gmail, dans les sauvegardes que personne n'a vérifiées depuis des mois. Souvent, ces données sont protégées par un mot de passe Windows "1234", un antivirus gratuit périmé, ou rien du tout.

2. Notifier le PFPDT en cas d'incident. L'Art. 24 nLPD impose au responsable du traitement d'annoncer dans les meilleurs délais toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les droits des personnes concernées. L'annonce doit indiquer au minimum la nature de la violation, ses conséquences et les mesures prises ou envisagées (Art. 24 al. 2). Le sous-traitant (votre prestataire IT, par exemple) a l'obligation de vous informer sans délai de toute violation qu'il détecte (Art. 24 al. 3). Si la protection des patients l'exige, ou si le PFPDT le demande, vous devez également informer les personnes concernées directement (Art. 24 al. 4).

3. Démontrer votre conformité à tout moment. Sur demande du PFPDT, vous devez pouvoir prouver que vous avez pris les mesures techniques et organisationnelles nécessaires (Art. 8 nLPD). Concrètement, cela signifie disposer d'une documentation à jour : registre des activités de traitement, contrat de sous-traitance signé avec votre prestataire IT, politique interne de sécurité, preuve de formation du personnel, procédure de réponse aux incidents, journal des sauvegardes et de leurs tests de restauration. L'absence de documentation ne signifie pas nécessairement une sanction, mais elle rend votre position indéfendable en cas d'incident.

1.4 Notification des violations (Art. 24 nLPD)

La loi suisse impose une notification « dans les meilleurs délais », une formulation volontairement souple, contrairement au RGPD européen qui fixe un délai strict de 72 heures. Le PFPDT recommande d'agir le plus rapidement possible après la découverte de la violation.

Le portail officiel de notification est accessible à l'adresse databreach.edoeb.admin.ch. Le PFPDT peut, avec l'accord du responsable du traitement, transmettre l'annonce à l'Office fédéral de la cybersécurité (OFCS) pour analyse de l'incident.

Important

Une annonce fondée sur l'Art. 24 ne peut pas être utilisée contre la personne qui l'a faite dans le cadre d'une procédure pénale, sauf avec son consentement (Art. 24 al. 6 nLPD). Notifier ne vous expose pas. Ne pas notifier, en revanche, vous expose.

1.5 Droits des patients (Art. 25 nLPD)

Tout patient peut demander au cabinet si des données personnelles le concernant sont traitées. Le cabinet doit alors fournir, dans un délai de 30 jours et gratuitement :

- L'identité et les coordonnées du responsable du traitement
- Les données personnelles traitées en tant que telles
- La finalité du traitement
- La durée de conservation ou les critères pour la déterminer
- L'origine des données si elles n'ont pas été collectées auprès du patient
- L'existence éventuelle d'une décision individuelle automatisée et sa logique
- Les destinataires auxquels des données sont communiquées, y compris à l'étranger

Communication des données de santé (Art. 25 al. 3)

Les données de santé peuvent être communiquées au patient par l'intermédiaire d'un professionnel de la santé qu'il aura désigné, avec son consentement. Cette disposition protège le patient contre des informations médicales difficiles à interpréter sans accompagnement.

Responsabilité en cas de sous-traitance (Art. 25 al. 4)

Si le cabinet utilise un sous-traitant (hébergeur de données, prestataire informatique), le cabinet reste responsable de fournir les renseignements au patient. Vous ne pouvez pas renvoyer le patient vers votre prestataire IT.

Caractère impératif du droit d'accès (Art. 25 al. 5)

Aucun patient ne peut renoncer par avance à son droit d'accès. Toute clause contractuelle allant en ce sens est nulle et non avenue.

Gratuité et délai (Art. 25 al. 6 et 7)

Les renseignements sont fournis gratuitement, dans un délai de 30 jours. En cas d'impossibilité de respecter ce délai (complexité, volume de données), le responsable doit en informer le patient et justifier la prolongation.

Recours du patient en cas de non-respect

Si le cabinet refuse de répondre ou ne respecte pas les délais, le patient dispose de plusieurs voies de recours :

- Rappel par lettre recommandée au cabinet

- Plainte auprès du PFPDT
- Action civile devant le tribunal (Art. 32 nLPD)
- Plainte pénale si les renseignements fournis sont intentionnellement faux (Art. 60 nLPD)

Attention aux formulations ambiguës

Un juriste d'entreprise a été condamné à 600 CHF d'amende en mars 2025 (Statthalteramt Bezirk Zürich, décision ST.2024.1046/ZM) pour avoir répondu qu'une société « n'avait trouvé aucune donnée » alors qu'elle en détenait. La formulation trompeuse suffisait à constituer l'infraction. Même une réponse partiellement exacte mais donnant une fausse impression d'exhaustivité peut être sanctionnée.

1.6 Registre des activités de traitement (Art. 12 nLPD)

Le registre est obligatoire pour les entreprises de plus de 250 collaborateurs ou dont le traitement présente un risque élevé. En raison de la nature sensible des données de santé traitées par un cabinet dentaire, il est fortement recommandé d'en tenir un, même pour les petites structures.

Le registre doit contenir au minimum : l'identité du responsable, la finalité des traitements, les catégories de personnes et de données concernées, les destinataires, les durées de conservation et une description des mesures de sécurité en place.

1.7 Sanctions (Art. 60 à 66 nLPD)

Les violations intentionnelles de la nLPD sont passibles d'amendes pouvant atteindre 250'000 CHF. Ces sanctions visent les personnes physiques responsables, et non l'entreprise. Dans un cabinet dentaire, c'est le praticien titulaire qui est directement concerné.

Infraction	Amende maximale	Condition
Renseignements intentionnellement inexacts ou incomplets	250'000 CHF	Sur plainte
Omission intentionnelle d'informer la personne concernée	250'000 CHF	Sur plainte
Sous-traitance sans contrat conforme (Art. 9)	250'000 CHF	Sur plainte
Communication de données à l'étranger sans garanties	250'000 CHF	Sur plainte
Renseignements inexacts au PFPDT lors d'une enquête	250'000 CHF	Sans plainte
Refus de collaborer avec le PFPDT	250'000 CHF	Sans plainte

Délai de prescription : 5 ans (Art. 66 nLPD). La retraite ou la cessation d'activité ne supprime pas la responsabilité pour des faits commis pendant l'exercice professionnel.

Seules les violations intentionnelles sont punissables pénalement

La négligence n'est pas sanctionnée pénalement par la nLPD, mais elle peut entraîner des recours civils de la part des patients lésés. La bonne foi et la réactivité sont toujours des facteurs atténuants.

1.8 Différences majeures avec l'ancien droit (LPD 1992)

La nLPD de 2023 constitue une révision complète de la loi de 1992. Voici les principales différences :

Ancienne LPD (1992)	Nouvelle nLPD (2023)
Protège personnes physiques et morales	Protège uniquement les personnes physiques
Pas d'obligation de notification	Notification obligatoire au PFPDT en cas de violation
Amendes limitées et rares	Amendes jusqu'à 250'000 CHF (responsabilité individuelle)
Pas d'obligation d'analyse d'impact	Analyse d'impact obligatoire pour traitements à risque élevé
Registre des traitements facultatif	Registre obligatoire (sauf exceptions limitées)
Pas de Privacy by Design	Privacy by Design et Privacy by Default obligatoires (Art. 7)
Données biométriques non protégées spécifiquement	Données biométriques et génétiques dans les données sensibles

1.9 Privacy by Design et Privacy by Default (Art. 7 nLPD)

L'Art. 7 impose deux principes fondamentaux qui doivent guider toute décision informatique dans le cabinet :

Privacy by Design (protection dès la conception) : les mesures de protection des données doivent être intégrées dès le choix d'un logiciel, d'un équipement ou d'un processus. Il ne s'agit pas de corriger après coup, mais de prévoir la sécurité dès le départ.

Privacy by Default (protection par défaut) : les réglages par défaut de tout système doivent limiter le traitement des données au strict minimum nécessaire. Un logiciel dentaire ne devrait pas, par défaut, partager les données patients avec des tiers ou stocker plus d'informations que nécessaire.

En pratique, ces principes s'appliquent lors du choix d'un logiciel de gestion, de la configuration d'un réseau, de la mise en place d'un nouveau poste de travail ou de l'adoption d'un outil cloud. Chaque décision doit intégrer la question : « est-ce que cette solution protège les données patients par défaut ? »

1.10 Analyse d'impact relative à la protection des données (Art. 22 nLPD)

L'analyse d'impact (AIPD) est obligatoire lorsqu'un traitement envisagé est susceptible d'entraîner un risque élevé pour les droits des personnes concernées. L'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement.

Exemples nécessitant une AIPD

- Mise en place d'un système de reconnaissance faciale dans le cabinet
- Profilage à grande échelle des patients
- Traitement massif de données de santé avec intelligence artificielle
- Surveillance vidéo extensive du cabinet

Contenu de l'analyse d'impact

L'AIPD doit contenir une description du traitement envisagé, une évaluation des risques pour les droits des personnes concernées, et les mesures prévues pour protéger ces droits. Si, malgré les mesures prévues, le risque reste élevé, le responsable doit consulter le PFPDT préalablement au traitement (Art. 23 nLPD).

En pratique pour un cabinet dentaire

La plupart des cabinets dentaires n'auront pas besoin de réaliser une AIPD dans leur activité courante. En revanche, l'introduction d'un nouveau logiciel traitant des données patients à grande échelle, d'un outil d'IA pour l'analyse de radiographies, ou d'un système biométrique d'accès pourrait déclencher cette obligation.

1.11 Jurisprudence récente

Bien que la nLPD soit encore récente, les premières décisions commencent à dessiner les contours de son application pratique.

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

Un juriste d'entreprise a été condamné à 600 CHF d'amende pour avoir répondu à une demande d'accès en affirmant qu'une société « n'avait trouvé aucune donnée » alors qu'elle en détenait. La formulation trompeuse suffisait à constituer l'infraction au sens de l'Art. 60 al. 1 let. a nLPD.

Ce cas illustre que même une réponse partiellement exacte mais donnant une fausse impression d'exhaustivité peut être sanctionnée. Pour un cabinet dentaire, cela signifie qu'une

demande d'accès d'un patient doit recevoir une réponse complète, précise et vérifiable dans les 30 jours.

1.12 Bonnes pratiques pour la gestion des demandes d'accès

- Répondre systématiquement dans les 30 jours
- Fournir une réponse complète dès la première fois
- Éviter les formulations ambiguës (ne jamais répondre « nous n'avons rien trouvé » si des données existent)
- Documenter chaque demande et chaque réponse dans un registre interne
- Former le personnel à traiter correctement ces demandes
- Désigner un responsable pour la gestion des demandes d'accès
- Vérifier l'identité du demandeur avant toute communication de données

Chapitre 2. Messagerie sécurisée

L'envoi de données patients par e-mail est l'une des pratiques les plus courantes, et les plus risquées, dans les cabinets dentaires. Une radiographie envoyée par Gmail, Bluewin ou Hotmail transite sans chiffrement de bout en bout, sur des serveurs souvent situés hors de Suisse.

2.1 Le problème

Les services de messagerie grand public ne sont pas conçus pour les données médicales :

- **Gmail / Hotmail / Yahoo :** serveurs hors de Suisse, pas de chiffrement de bout en bout. Doublement non conforme.
- **Bluewin :** serveurs en Suisse, mais pas de chiffrement de bout en bout. Swisscom peut techniquement accéder au contenu. Insuffisant pour des données médicales.
- **Infomaniak Mail :** mieux protégé que Gmail, mais pas de chiffrement natif de bout en bout. Convient pour les échanges internes non sensibles, pas pour les données patients.

2.2 Les solutions conformes

- **HIN Mail :** la référence dans le domaine médical suisse. Communication sécurisée entre professionnels de santé, compatible avec le réseau HIN national. Solution idéale pour les échanges avec médecins, laboratoires et spécialistes.
- **Proton** : fondé en 2014 au CERN à Genève par des scientifiques et ingénieurs préoccupés par la surveillance de masse révélée par Edward Snowden. L'objectif fondateur était de créer des outils de communication que personne, pas même Proton, ne peut lire. L'entreprise est basée à Genève et soumise au droit suisse, l'une des législations les plus strictes au monde en matière de protection de la vie privée. L'ensemble de l'infrastructure est hébergée en Suisse, y compris dans un ancien bunker militaire sous 1'000 mètres de roche granitique dans les Alpes.

  Proton ne se limite pas à la messagerie. L'écosystème complet comprend **ProtonMail** (messagerie chiffrée de bout en bout), **Proton Drive** (stockage cloud

chiffré, alternative conforme à Google Drive ou Dropbox), **Proton Pass** (gestionnaire de mots de passe chiffré), **Proton VPN** (réseau privé virtuel pour sécuriser les connexions à distance) et **Proton Calendar** (agenda chiffré). Pour un cabinet dentaire, cet écosystème permet de couvrir plusieurs besoins en une seule solution : messagerie sécurisée pour les échanges avec patients et fournisseurs hors réseau HIN, stockage cloud pour les documents administratifs sensibles, coffre-fort de mots de passe pour l'équipe, et VPN. Le tout avec un chiffrement de bout en bout, des serveurs en Suisse et une politique zéro accès : Proton ne peut techniquement pas lire vos données, même sur demande d'une autorité.

Règle pratique

Si le contenu de l'e-mail contient une radiographie, un diagnostic, un numéro AVS ou toute autre donnée patient identifiable, il doit transiter par une messagerie chiffrée de bout en bout. Sans exception.

Chapitre 3. Mises à jour

Les mises à jour corrigent les failles de sécurité et empêchent la majorité des attaques les plus courantes. Un système non mis à jour est un système vulnérable. Chaque jour qui passe sans correctif est une porte ouverte supplémentaire pour les attaquants.

3.1 Système d'exploitation

Windows et macOS doivent impérativement être maintenus à jour. Le support de Windows 10 a pris fin en octobre 2025 : les failles découvertes après cette date ne seront jamais corrigées par Microsoft.

Windows 11 est aujourd'hui le seul système Windows encore supporté. Tout poste sous Windows 7, 8 ou 10 doit être remplacé ou migré.

3.2 Applications et logiciels métier

Les logiciels dentaires, quelle que soit la solution utilisée dans votre cabinet, doivent être mis à jour régulièrement. Une ancienne version peut contenir des failles exploitables ou provoquer des corruptions de données. Cela concerne aussi bien les logiciels de gestion de cabinet que les logiciels d'imagerie et de radiologie.

Les navigateurs web, les lecteurs PDF et les suites bureautiques doivent également être maintenus à jour. Ce sont des vecteurs d'attaque fréquents et souvent négligés.

Vérifiez auprès de votre éditeur que la version installée est toujours supportée et qu'elle reçoit des correctifs de sécurité. Si ce n'est plus le cas, planifiez la migration vers une version récente ou une solution alternative.

Bonne pratique

Activez les mises à jour automatiques sur tous les postes. Planifiez un redémarrage hebdomadaire pour permettre l'installation des correctifs en attente. Un poste qui n'a jamais été redémarré accumule des failles de sécurité non corrigées.

Chapitre 4. Sauvegardes

La sauvegarde est votre dernière ligne de défense. En cas de ransomware, d'erreur humaine ou de panne matérielle, c'est elle qui détermine si vous perdez tout ou si vous reprenez l'activité en quelques heures.

4.1 La règle 3-2-1

3 copies de vos données, sur 2 supports différents, dont 1 copie immuable. Il s'agit d'une version que personne ne peut modifier ou supprimer, même un ransomware.

La copie immuable ne signifie pas nécessairement un disque dur à débrancher chaque soir. Des technologies comme les snapshots automatiques, le stockage cloud avec rétention immuable ou les sauvegardes versionnées permettent de protéger les données sans intervention humaine quotidienne. Votre prestataire informatique doit être en mesure de vous proposer et de mettre en place un système de sauvegarde adapté à votre cabinet, conforme à la règle 3-2-1 et documenté par écrit. Ce n'est pas au praticien de concevoir l'architecture de sauvegarde ; en revanche, c'est à lui de s'assurer qu'elle existe, qu'elle fonctionne et qu'elle est testée.

Un exemple concret de mise en œuvre : le serveur du cabinet conserve les données de travail (copie 1), une sauvegarde automatique est répliquée sur un NAS ou un disque dédié dans le cabinet (copie 2), et une troisième copie est envoyée chaque nuit vers un stockage cloud sécurisé en Suisse avec rétention immuable (copie 3). Si un ransomware chiffre les deux premières copies, la troisième reste intacte et permet une restauration complète.

La solution peut être personnalisée selon la taille du cabinet et le volume de données. Certains prestataires appliquent la règle 3-2-1-1-0, qui ajoute une copie immuable supplémentaire et vise zéro erreur lors des tests de restauration. L'important n'est pas la complexité du système, mais la garantie que vos données patients peuvent être récupérées en cas de sinistre, dans un délai compatible avec la continuité de votre activité.

Si votre prestataire IT actuel ne peut pas vous expliquer clairement votre stratégie de sauvegarde, où se trouvent vos copies, si elles sont immuables et quand elles ont été testées pour la dernière fois, c'est un signal d'alerte.

4.2 Pourquoi la copie immuable est essentielle

Les ransomwares modernes détectent et chiffrent toutes les sauvegardes connectées au réseau. Un disque dur externe branché en permanence sera également chiffré lors de l'attaque. Seule une copie physiquement déconnectée ou logiquement isolée (versioning immuable) restera intacte.

4.3 Tester la restauration

Une sauvegarde non testée est une illusion de sécurité

Testez chaque mois la restauration effective d'un échantillon de données, par exemple quelques dossiers patients ou quelques radiographies. Vérifiez que les fichiers s'ouvrent correctement et que les données sont exploitables. Sans test régulier, vous découvrirez trop tard que vos sauvegardes sont corrompues ou incomplètes.

Chapitre 5. Mots de passe et double authentification

5.1 Le problème des mots de passe faibles

Un mot de passe « 1234 », le nom du cabinet ou une date de naissance se devine en quelques secondes. Un compte partagé entre toute l'équipe empêche toute traçabilité en cas d'incident. L'absence de double authentification laisse un seul mot de passe comme unique barrière entre un attaquant et vos données patients.

5.2 Créer un mot de passe robuste

Minimum 12 caractères, combinant majuscules, minuscules, chiffres et symboles. Une méthode concrète : choisissez deux mots sans lien logique, ajoutez un chiffre mémorable et des caractères spéciaux consécutifs sur le clavier.

Exemple

CarmolTroppen91()=. Facile à retenir, Aucun lien avec votre cabinet ou vous-même.

5.3 Utiliser un coffre-fort de mots de passe

Un gestionnaire de mots de passe stocke tous vos identifiants de manière chiffrée. Vous n'avez qu'un seul mot de passe maître à retenir.

- Proton Pass : chiffré, serveurs en Suisse
- Bitwarden : open source, auto-hébergeable
- KeePass : stockage local, pas de cloud

5.4 Double authentification (2FA)

La 2FA ajoute une deuxième vérification après le mot de passe : un code temporaire sur votre téléphone, une notification push, ou une clé physique. Même si votre mot de passe est compromis, l'attaquant ne peut pas accéder au compte sans ce deuxième facteur.

À activer sur : messagerie professionnelle, logiciel dentaire (si disponible), sauvegardes cloud, accès à distance, comptes bancaires.

Chapitre 6. Chiffrement des disques et des archives

6.1 Chiffrement des postes de travail

Un ordinateur portable volé dans une voiture ou un serveur emporté lors d'un cambriolage donnent un accès immédiat à toutes les données si le disque n'est pas chiffré. Le chiffrement rend les données totalement illisibles sans la clé de déchiffrement.

- **Windows :** BitLocker, intégré dans Windows Pro et Enterprise, gratuit. À activer sur tous les postes.
- **macOS :** FileVault, intégré, gratuit. À activer dans les préférences système.
- **Serveurs :** chiffrement matériel (TPM), Bitlocker ou logiciel selon l'infrastructure.

6.2 Chiffrement de conteneurs pour archives sensibles

Pour les disques externes contenant des archives patients, de la comptabilité ou des sauvegardes anciennes, un conteneur chiffré fonctionne comme un coffre-fort numérique : accessible uniquement via un mot de passe fort.

- **Windows :** BitLocker To Go (disques externes), VeraCrypt (conteneurs chiffrés)
- **macOS :** FileVault pour disques externes
- **Multiplateforme :** VeraCrypt : open source, robuste, gratuit

Chapitre 7. Réseau WiFi

Un réseau WiFi unique partagé entre le personnel, les appareils médicaux et les patients est une faille de sécurité majeure. Un téléphone infecté connecté au réseau invité peut, sans séparation, atteindre le serveur du cabinet.

7.1 La configuration recommandée : trois réseaux séparés

- **Réseau principal :** postes de travail, serveur, imprimantes, isolé et protégé.
- **Réseau médical :** appareils de radiologie, capteurs, équipements connectés, si nécessaire selon l'infrastructure.
- **Réseau invité :** patients. Accès Internet uniquement, aucune visibilité sur le réseau interne du cabinet.

La séparation des réseaux est l'équivalent numérique de la cloison entre la salle d'attente et la salle de soins. Le protocole WPA3 est recommandé si le matériel le supporte, WPA2 étant le minimum acceptable.

Mot de passe WiFi

Ne jamais afficher le mot de passe du réseau principal en salle d'attente. Le réseau invité peut utiliser un portail captif avec un code journalier ou un code unique remis sur demande.

Chapitre 8. Accès à distance sécurisé

Les outils d'accès à distance sont indispensables pour la télémaintenance informatique, mais mal configurés, ils représentent une porte d'entrée majeure pour les attaquants.

8.1 Le risque des versions gratuites en veille permanente

Un cabinet dentaire romand a été victime d'une attaque par ransomware via TeamViewer laissé en veille permanente avec un mot de passe faible. Résultat : 3 jours d'activité perdue, rançon demandée de 15'000 CHF, récupération partielle des données uniquement.

Laisser TeamViewer, AnyDesk ou un autre outil d'accès distant actif 24h/24 sans sécurité renforcée équivaut à laisser une porte ouverte en permanence sur votre cabinet.

8.2 Solutions recommandées

Solution	Usage	Sécurité	Recommandation
TeamViewer / AnyDesk gratuit	Occasionnel	Faible	À éviter pour données médicales
TeamViewer Pro + 2FA	Ponctuel	Correct	Acceptable si bien configuré
VPN professionnel	Permanent	Élevé	WireGuard ou OpenVPN recommandé
RMM entreprise	Télémaintenance	Très élevé	NinjaOne, Datto, Atera

Règle d'or

Aucun accès distant ne doit être configuré en accès libre permanent. Chaque connexion doit être tracée, authentifiée et limitée dans le temps. Plus le niveau de privilège est élevé (accès serveur, données patients), plus la solution doit être sécurisée.

Chapitre 9. Phishing

Le phishing reste le vecteur d'attaque le plus courant contre les cabinets médicaux. L'attaquant se fait passer pour un contact de confiance (Swisscom, votre banque, votre prestataire IT) pour obtenir des identifiants ou faire ouvrir un fichier infecté.

9.1 Reconnaître un e-mail de phishing

- Adresse expéditeur suspecte (domaine inhabituel, fautes d'orthographe)
- Urgence artificielle : « Votre compte sera bloqué dans 24h »
- Demande de cliquer sur un lien ou d'ouvrir une pièce jointe inattendue
- Fautes d'orthographe ou formulation inhabituelle
- Demande d'identifiants, de mots de passe ou de données bancaires

9.2 Protection avancée : le filtrage par label

Les e-mails provenant d'expéditeurs récurrents et de confiance peuvent être automatiquement filtrés et étiquetés. Tout e-mail prétendant provenir de l'un de ces contacts mais non reconnu par le filtre doit immédiatement éveiller les soupçons.

Cette configuration est possible via des règles de filtrage intégrées à votre messagerie ou via des solutions anti-phishing professionnelles. Si vous optez pour un outil tiers de filtrage des e-mails, vérifiez impérativement où sont situés les serveurs qui analysent le contenu de vos messages.

Une solution qui fait transiter vos e-mails par des serveurs situés hors de Suisse peut poser problème au regard de l'Art. 16 nLPD, en particulier si ces e-mails contiennent des données patients. Privilégiez des solutions dont le traitement des données s'effectue en Suisse ou, à défaut, dans un pays reconnu par le Conseil fédéral comme offrant un niveau de protection adéquat. Votre prestataire informatique doit être en mesure de vous confirmer la localisation des serveurs et les garanties de protection applicables.

Chapitre 10. Gestion des accès utilisateurs

Définir qui peut accéder à quoi réduit fortement les risques internes et limite les dégâts en cas de compromission d'un compte.

10.1 Principe du moindre privilège

Chaque utilisateur ne doit avoir accès qu'aux données strictement nécessaires à sa fonction. Ce principe, largement reconnu en sécurité informatique, est directement lié à l'Art. 8 nLPD qui impose des mesures organisationnelles appropriées pour assurer la sécurité des données.

Dans un cabinet dentaire, les rôles sont clairement distincts et les accès doivent refléter cette réalité. Une assistante dentaire doit pouvoir consulter les dossiers patients et prendre des rendez-vous, mais n'a pas besoin d'accéder à la comptabilité du cabinet, aux données RH ou aux paramètres d'administration du serveur. Un hygiéniste a besoin de l'historique de soins de ses patients, pas des factures impayées. Un comptable externe a besoin des données financières, pas des radiographies.

En cas de compromission d'un compte (phishing réussi, mot de passe volé), le principe du moindre privilège limite les dégâts : l'attaquant ne peut accéder qu'aux données autorisées pour ce compte. Si tout le monde partage le même identifiant avec accès total, une seule compromission expose l'intégralité du cabinet.

10.2 Règles de gestion des comptes

Un compte par personne, jamais de compte partagé. Les comptes génériques comme « cabinet », « admin », « accueil » ou « compta » empêchent toute traçabilité. En cas d'incident, il est impossible de déterminer qui a effectué quelle action et à quel moment. Chaque collaborateur doit disposer de son propre identifiant, avec un mot de passe personnel qu'il ne partage avec personne.

Les comptes administrateurs doivent être réservés aux opérations techniques (installation de logiciels, configuration réseau, maintenance) et ne jamais être utilisés pour le travail quotidien. Si votre prestataire IT utilise un compte administrateur, ce compte doit être distinct de ceux du personnel, protégé par une double authentification et soumis à une journalisation des connexions.

10.3 Gestion des arrivées et des départs

L'arrivée d'un nouveau collaborateur doit déclencher la création d'un compte nominatif avec des droits correspondant strictement à sa fonction. Le collaborateur doit recevoir une formation sur les règles d'utilisation des systèmes informatiques du cabinet, y compris la politique de mots de passe et les interdictions (WhatsApp, clés USB personnelles, transfert de données vers des équipements non autorisés).

Le départ d'un collaborateur, qu'il soit volontaire ou non, doit entraîner la désactivation immédiate de tous ses accès : compte utilisateur, messagerie, logiciel de gestion, accès à distance, stockage cloud. Ne pas le remettre au lendemain, ne pas le reporter à la fin du mois. Un ancien employé mécontent disposant encore de ses accès représente un risque réel, tant pour la sécurité des données que pour la responsabilité du cabinet vis-à-vis de la nLPD.

10.4 Revue périodique des droits d'accès

Les droits d'accès ne sont pas figés. Un collaborateur peut changer de fonction, un stagiaire peut terminer son stage, un prestataire externe peut ne plus intervenir. Sans vérification régulière, des accès obsolètes s'accumulent et créent des failles invisibles.
Planifiez une revue trimestrielle : passez en revue la liste des comptes actifs, vérifiez que chaque compte correspond à une personne toujours en poste, que les droits attribués correspondent à la fonction actuelle, et que tous les comptes inutilisés sont désactivés.
Documentez cette revue par écrit : elle fait partie des mesures organisationnelles que le PFPDT peut demander à consulter.

10.5 Outils facilitant la gestion des accès

Certains équipements et technologies permettent de centraliser et de simplifier la gestion des comptes et des droits d'accès dans un cabinet. Un serveur NAS professionnel (par exemple de type Synology) offre une gestion des utilisateurs et des dossiers partagés avec des permissions granulaires : chaque collaborateur n'accède qu'aux répertoires autorisés pour sa fonction, avec une journalisation des connexions et des modifications. C'est une solution adaptée aux cabinets de petite et moyenne taille qui ne disposent pas d'un serveur dédié.

Pour les cabinets disposant d'une infrastructure Windows plus avancée, un annuaire centralisé de type Active Directory permet de gérer l'ensemble des comptes, mots de passe, groupes de sécurité et politiques d'accès depuis un point unique. Il facilite la création et la suppression de comptes, l'application automatique de règles de sécurité (complexité des mots de passe, verrouillage après tentatives échouées, expiration des sessions) et la restriction des accès par groupe fonctionnel (praticiens, assistantes, comptabilité, administration). Votre prestataire informatique doit être en mesure de vous conseiller sur la solution la mieux adaptée à la taille et à l'organisation de votre cabinet.

Chapitre 11. Malwares polymorphiques et protection EDR

Un malware polymorphique est un programme malveillant capable de modifier son propre code à chaque infection pour ne pas être reconnu par les antivirus classiques. Ce n'est pas une menace nouvelle ; ces techniques existent depuis les années 90, mais l'intelligence artificielle a considérablement accéléré leur sophistication. Ce qui prenait des semaines de développement à un attaquant se génère désormais en quelques minutes.

11.1 Pourquoi l'antivirus classique ne suffit plus

Un antivirus traditionnel fonctionne par signature : il compare chaque fichier à une base de données de menaces connues. Si le malware change de forme à chaque infection, il n'est jamais reconnu. C'est comme un garde de sécurité qui reconnaît uniquement les criminels fichés. Si le criminel change de visage, il passe inaperçu.

Ce modèle de détection reste utile contre les menaces connues et largement diffusées, mais il est insuffisant face aux attaques ciblées ou aux malwares récents qui n'ont jamais été catalogués. Or, c'est précisément ce type d'attaque qui touche les cabinets médicaux : des ransomwares déployés sur mesure, souvent après une phase de reconnaissance du réseau de la victime.

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

Un EDR ne cherche pas un visage connu ; il observe un comportement. Si un programme commence à ouvrir massivement des fichiers patients et à les chiffrer un par un, l'EDR le détecte, le stoppe et le met en quarantaine en temps réel, avant qu'il n'ait terminé. Peu importe l'apparence du programme ou s'il a déjà été répertorié.

Au-delà de la détection comportementale, un EDR offre des capacités que l'antivirus classique ne possède pas : isolation automatique du poste compromis pour éviter la propagation au reste du réseau, journalisation complète de l'incident (quels fichiers ont été touchés, à quelle heure, par quel processus), possibilité de restauration des fichiers modifiés (rollback), et alertes en temps réel destinées à votre prestataire informatique.

Parmi les solutions EDR reconnues sur le marché, on trouve SentinelOne, CrowdStrike, Sophos Intercept X, Microsoft Defender for Endpoint ou encore ESET Inspect. Chacune propose des niveaux de fonctionnalités et de tarification différents ; le choix doit être fait en

concertation avec votre prestataire informatique en fonction de la taille de votre cabinet et de votre infrastructure existante.

11.3 EDR, EPP, antivirus : comprendre les différences

Un antivirus classique détecte les menaces connues par signature. Un EPP (Endpoint Protection Platform) combine l'antivirus avec des couches supplémentaires : pare-feu local, contrôle des périphériques USB, filtrage web. Un EDR va plus loin en ajoutant l'analyse comportementale, la réponse automatisée et la visibilité complète sur ce qui se passe sur chaque poste. Pour un cabinet dentaire traitant des données sensibles, un EDR managé par votre prestataire informatique est le niveau de protection recommandé.

À titre d'exemple, un antivirus classique comme Windows Defender (inclus gratuitement dans Windows) offre une protection de base par signature. Un EPP comme Bitdefender GravityZone ou ESET Protect ajoute des couches de prévention supplémentaires. Un EDR comme SentinelOne ou CrowdStrike Falcon ajoute la détection comportementale et la réponse automatisée. Le coût augmente avec le niveau de protection, mais les conséquences financières d'une attaque réussie dépassent largement l'investissement dans une solution adaptée.

11.4 Le rôle du prestataire informatique

Un EDR ne se configure pas seul. Il nécessite un paramétrage adapté à votre environnement (exclusion des logiciels dentaires légitimes, seuils d'alerte, politique de réponse automatique) et une surveillance régulière des alertes générées.

Votre prestataire informatique doit être en mesure de déployer, configurer et superviser cette solution. Demandez-lui s'il utilise un EDR sur les postes qu'il gère, s'il reçoit les alertes en temps réel et quel est son temps de réaction en cas de détection d'une menace active. Si votre prestataire se contente d'installer un antivirus gratuit sans supervision, le niveau de protection est insuffisant pour des données médicales soumises à la nLPD.

Chapitre 12. Modernisation du parc informatique

Ne jamais laisser un ou deux anciens postes de travail dans un cabinet moderne. Un seul ordinateur obsolète ou non mis à jour suffit pour compromettre tout le réseau. Dans un cabinet dentaire, cela signifie un risque réel de fuite ou de rançon portant sur des radiographies, diagnostics, données administratives ou comptables. Un seul maillon faible suffit pour mettre en danger l'ensemble du cabinet.

12.1 Pourquoi un poste obsolète est dangereux

Un poste Windows dépassé ou jamais redémarré accumule des failles de sécurité connues et publiquement documentées. Les attaquants disposent de bases de données répertoriant ces failles et des outils automatisés pour les exploiter. Si l'une d'elles est exploitée, la chaîne d'attaque est prévisible : obtenir un accès initial au réseau local via le poste vulnérable, contourner les protections des postes récents en se déplaçant latéralement sur le réseau, atteindre le serveur de stockage, accéder au logiciel métier ou aux sauvegardes, puis voler ou chiffrer les données sensibles. Tout cela peut se produire en quelques heures, souvent la nuit ou le week-end lorsque personne ne surveille.

Le problème ne concerne pas uniquement les postes de travail visibles. Les équipements souvent oubliés sont tout aussi critiques : un ancien serveur qui tourne encore "en attendant", une imprimante réseau dont le firmware n'a jamais été mis à jour, un routeur WiFi d'ancienne génération, un NAS dont le système d'exploitation est obsolète. Chacun de ces équipements constitue un point d'entrée potentiel.

12.2 Cycle de renouvellement recommandé

La règle pratique est de renouveler les postes de travail tous les 5 ans maximum. Ce délai n'est pas arbitraire : il correspond à la durée moyenne pendant laquelle un fabricant garantit la compatibilité avec les mises à jour de sécurité du système d'exploitation et des composants matériels (pilotes, firmware, module TPM).

Ce qui compte réellement, ce n'est pas l'âge du poste en soi, mais sa capacité à recevoir les dernières mises à jour de sécurité. Un poste de 4 ans compatible Windows 11 avec un module TPM 2.0 est en meilleur état de sécurité qu'un poste de 2 ans bloqué sous un système en fin de support.

Windows 11 est aujourd'hui le seul système Windows encore supporté par l'éditeur. Tout poste sous Windows 7, 8 ou 10 ne reçoit plus aucun correctif de sécurité. Conserver un tel poste sur le réseau du cabinet revient à laisser une porte ouverte en permanence, quel que soit le niveau de protection des autres équipements.

12.3 Cas particulier : iMacs sous Boot Camp

Certains cabinets utilisent encore des iMacs Intel avec Windows installé via Boot Camp. Cette configuration pose un double problème : ces iMacs ne peuvent souvent plus monter ni sur Windows 11 (en raison de l'absence de module TPM 2.0), ni sur les dernières versions de macOS (Apple ayant cessé le support des modèles Intel les plus anciens). Ces machines se trouvent en fin de vie des deux côtés simultanément.

La solution est de les remplacer par des PC sous Windows 11 dédiés. Les logiciels de gestion et d'imagerie dentaire tournent exclusivement sous Windows ; un Mac n'apporte donc aucun avantage fonctionnel dans ce contexte et complique la maintenance, les mises à jour et la compatibilité matérielle.

12.4 Planifier la migration

Le remplacement du parc informatique ne doit pas se faire dans l'urgence le jour où un poste tombe en panne ou devient la cible d'une attaque. Il doit être planifié de manière anticipée, en concertation avec votre prestataire informatique. Voici les étapes recommandées :

Commencez par un inventaire complet du parc : chaque poste de travail, chaque serveur, chaque équipement réseau, avec le système d'exploitation installé, la date d'achat ou de mise en service, et la compatibilité avec les mises à jour actuelles. Identifiez les postes en fin de vie ou en fin de support. Établissez un calendrier de remplacement réaliste, étalé si nécessaire sur plusieurs mois pour répartir l'investissement. Prévoyez la migration des données et des logiciels métier, la reconfiguration des accès réseau et la vérification du bon fonctionnement de chaque poste avant mise en production.

Documentez cet inventaire et ce calendrier par écrit. Il fait partie des mesures organisationnelles démontrant votre conformité à l'Art. 8 nLPD.

12.5 Destruction sécurisée des anciens équipements

Le remplacement d'un poste ne s'arrête pas à l'installation du nouveau. L'ancien équipement contient potentiellement des données patients sur son disque dur, même si vous pensez avoir tout effacé. Un simple formatage ne suffit pas : des outils de récupération permettent de retrouver des données effacées de manière conventionnelle.

Deux options conformes à la nLPD : l'effacement sécurisé par logiciel spécialisé (écrasement multiple des données rendant toute récupération impossible) ou la destruction physique du support de stockage (broyage, démagnétisation). Dans les deux cas, demandez un certificat de destruction à votre prestataire informatique et conservez-le dans votre documentation de conformité. Ce certificat constitue une preuve que les données patients n'ont pas été abandonnées sur un support non sécurisé.

Chapitre 13. Le contrat de sous-traitance (Art. 9 nLPD)

L'Art. 9 de la nLPD encadre strictement la sous-traitance du traitement de données personnelles. En pratique, cela concerne directement la relation entre un cabinet dentaire et tout tiers qui accède, stocke, traite ou transporte des données personnelles de vos patients pour votre compte.

Sans contrat de sous-traitance conforme, vous n'avez aucun recours contre votre prestataire en cas de problème. Et en cas d'incident, c'est vous, le responsable du cabinet, qui répondez devant le PFPDT et devant vos patients. La sous-traitance sans contrat conforme est elle-même une infraction passible de 250'000 CHF d'amende (Art. 61 let. b nLPD).

13.1 Conditions préalables à toute sous-traitance

Avant même de rédiger un contrat, l'Art. 9 al. 1 pose deux conditions que le responsable du traitement doit vérifier. Premièrement, le sous-traitant ne peut effectuer que les traitements que le cabinet serait en droit d'effectuer lui-même. Si un traitement vous est interdit, vous ne pouvez pas le confier à un tiers pour contourner l'interdiction. Deuxièmement, aucune obligation légale ou contractuelle de garder le secret ne doit interdire cette sous-traitance. Dans le contexte médical, le secret professionnel (Art. 321 du Code pénal) impose une vigilance particulière sur les données auxquelles le sous-traitant pourra réellement accéder.

L'Art. 9 al. 2 ajoute une obligation active de vérification : le responsable du traitement doit s'assurer que le sous-traitant est en mesure de garantir la sécurité des données. Ce n'est pas une formalité. Vous devez pouvoir démontrer que vous avez vérifié les compétences, les outils et les pratiques de sécurité de votre prestataire avant de lui confier l'accès à votre infrastructure.

13.2 Qui est concerné par le contrat de sous-traitance ?

Le contrat de sous-traitance ne concerne pas uniquement votre prestataire informatique. Toute personne ou entreprise qui accède à des données personnelles de vos patients pour votre compte est un sous-traitant au sens de la nLPD. Voici les cas les plus fréquents dans un cabinet dentaire :

Votre prestataire informatique, qui accède aux postes, serveurs, sauvegardes et potentiellement aux données patients lors de ses interventions de maintenance. Votre hébergeur cloud, si vos données ou sauvegardes sont stockées chez un fournisseur externe. Un laboratoire dentaire, s'il reçoit des fichiers numériques contenant des données patient identifiables (empreintes optiques, radiographies avec nom du patient). Un comptable ou

fiduciaire externe, s'il accède aux données de facturation contenant des informations patient. Un éditeur de logiciel dentaire, si le logiciel fonctionne en mode cloud et que les données sont hébergées sur les serveurs de l'éditeur.

Pour chacun de ces sous-traitants, un contrat conforme à l'Art. 9 nLPD doit être en place.

13.3 Ce que le contrat doit contenir

Le contrat doit définir clairement le cadre dans lequel le sous-traitant est autorisé à traiter des données :

- La nature des données accessibles par le sous-traitant et les catégories de personnes concernées (patients, personnel, fournisseurs).
- La finalité du traitement, limitée aux instructions du cabinet. Le sous-traitant ne peut pas utiliser les données à d'autres fins, les revendre ou les communiquer à des tiers sans instruction préalable du responsable.
- La liste des outils utilisés et la localisation des serveurs. Ce point est directement lié à l'Art. 16 nLPD : si les outils du prestataire stockent ou font transiter des données sur des serveurs situés hors de Suisse, les garanties de protection adéquate doivent être documentées dans le contrat.
- Les mesures de sécurité techniques et organisationnelles mises en place par le sous-traitant (chiffrement, contrôle des accès, journalisation, antivirus ou EDR).
- La procédure de notification d'incident avec un délai défini. L'Art. 24 al. 3 nLPD impose au sous-traitant d'informer le responsable du traitement dans les meilleurs délais en cas de violation de la sécurité des données. Le contrat doit préciser un délai concret, par exemple 24 heures après la détection.
- La procédure de fin de contrat : suppression de tous les accès, restitution ou suppression des données détenues, confirmation écrite de l'exécution de ces mesures.
- L'interdiction de sous-traitance à des tiers sans accord préalable écrit du cabinet (Art. 9 al. 3 nLPD). Si votre prestataire informatique utilise lui-même des sous-traitants (par exemple un hébergeur cloud pour vos sauvegardes), cela doit être déclaré et encadré contractuellement.

- Une clause de confidentialité sans limite de durée, y compris après la fin du contrat.

Ce n'est pas un document de 40 pages. Un contrat bien rédigé tient en 9 articles, lisible en 5 minutes, signable en 2.

13.4 Vérifier les outils de votre prestataire

Le contrat doit inclure un tableau ou une annexe listant les outils utilisés par le prestataire dans le cadre de ses interventions, avec pour chacun la finalité et la localisation des données. Par exemple : l'outil de télémaintenance utilisé, la solution de monitoring, le gestionnaire de mots de passe, la solution de sauvegarde, la messagerie professionnelle. Pour chaque outil dont les serveurs sont situés hors de Suisse, vérifiez si le pays concerné est reconnu par le Conseil fédéral comme offrant un niveau de protection adéquat (Art. 16 al. 1 nLPD), ou si des garanties contractuelles supplémentaires sont en place (Art. 16 al. 2).

13.5 Responsabilité envers les patients (Art. 25 al. 4)

Même si un sous-traitant traite des données pour votre compte, vous restez le seul interlocuteur de vos patients. L'Art. 25 al. 4 nLPD est explicite : le responsable du traitement qui fait traiter des données par un sous-traitant demeure tenu de fournir les renseignements demandés par la personne concernée. Vous ne pouvez pas renvoyer un patient vers votre prestataire informatique en cas de demande d'accès à ses données. C'est à vous de répondre, dans les 30 jours, même si cela nécessite de solliciter votre sous-traitant pour obtenir les informations.

13.6 Mon prestataire actuel n'a pas de contrat : que faire ?

Si aucun contrat de sous-traitance n'est actuellement en place avec votre prestataire informatique ou vos autres sous-traitants, la démarche est simple. Contactez votre prestataire et demandez-lui s'il dispose d'un contrat conforme à l'Art. 9 nLPD. S'il en propose un, lisez-le attentivement et vérifiez qu'il couvre les points listés ci-dessus. S'il n'en propose pas, c'est un signal d'alerte sur son niveau de maturité en matière de protection des données. Vous pouvez lui fournir un modèle de contrat ou en faire rédiger un par un juriste spécialisé.

L'absence de contrat ne signifie pas que la collaboration doit cesser immédiatement, mais régulariser la situation doit être une priorité. En cas d'incident survenant sans contrat en place, votre position sera considérablement affaiblie, tant vis-à-vis du PFPDT que devant vos patients.

Vous déléguez la technique. Jamais la responsabilité.

Chapitre 14. Formation du personnel

La technologie ne suffit pas si les personnes qui l'utilisent ne sont pas formées. Les erreurs humaines (un e-mail de phishing ouvert, un écran non verrouillé, un dossier patient laissé à la réception, une radiographie envoyée par WhatsApp) représentent une part significative des violations de données. La plupart de ces incidents ne résultent pas d'une intention malveillante, mais d'un manque de sensibilisation et de règles claires.

14.1 Une obligation implicite de la nLPD

L'Art. 8 nLPD impose au responsable du traitement de prendre des mesures organisationnelles et techniques appropriées pour assurer la sécurité des données. La formation du personnel fait partie de ces mesures organisationnelles. Le Conseil fédéral, dans son rapport explicatif sur la nLPD publié par l'Office fédéral de la justice, souligne explicitement que la mise en œuvre efficace de la sécurité des données dépend de la formation correcte des personnes impliquées. Un manque de formation pourrait entraîner des violations de la sécurité des données, par exemple si un collaborateur ouvre un e-mail contenant un logiciel malveillant.

En droit du travail suisse (Art. 328 CO), l'employeur a un devoir de formation et de surveillance. Un licenciement prononcé suite à une violation de la politique de sécurité par un employé pourrait être considéré comme abusif si aucune formation n'avait été dispensée au préalable et si aucune règle écrite n'avait été remise.

14.2 Contenu recommandé d'une formation

La formation doit couvrir les situations réelles auxquelles le personnel est confronté au quotidien.

Reconnaître les tentatives de fraude. Le phishing par e-mail est le vecteur le plus courant, mais il ne s'agit pas du seul risque. La formation doit inclure les appels téléphoniques frauduleux (quelqu'un se fait passer pour le prestataire IT et demande un mot de passe, un prétendu collaborateur de l'éditeur du logiciel dentaire demande un accès à distance, un inconnu se présente comme un patient et demande des informations médicales par téléphone), les SMS et messages frauduleux, et les clés USB inconnues trouvées dans ou à proximité du cabinet. Des exemples concrets et des exercices pratiques renforcent la mémorisation.

Règles de verrouillage des postes. Verrouiller l'écran à chaque départ du poste, même pour quelques secondes. La combinaison Windows+L sous Windows ou Ctrl+Commande+Q sous macOS doit devenir un réflexe. Un écran non verrouillé dans une salle accessible aux patients constitue une violation potentielle de la confidentialité.

Politique de mots de passe. Utilisation obligatoire du coffre-fort de mots de passe du cabinet, activation de la double authentification sur tous les accès critiques, interdiction de noter les mots de passe sur des post-it ou dans des fichiers non chiffrés.

Utilisation de la messagerie sécurisée. Savoir distinguer quand utiliser la messagerie chiffrée (tout contenu contenant des données patient identifiables) et quand la messagerie standard est acceptable (échanges internes sans données sensibles, commandes de fournitures). Interdiction formelle d'utiliser des messageries grand public (Gmail, Hotmail, WhatsApp) pour toute communication contenant des données patients.

Procédure en cas d'incident

Chaque collaborateur doit savoir quoi faire en cas de suspicion d'attaque ou de fuite : qui appeler en premier (le praticien responsable, puis le prestataire IT), quoi faire immédiatement (débrancher le câble réseau, ne pas éteindre le poste), quoi ne pas faire (ne pas tenter de résoudre le problème soi-même, ne pas payer une rançon, ne pas supprimer les messages suspects avant documentation).

Gestion des données patients. Ne jamais envoyer de données patients via WhatsApp, SMS ou messagerie personnelle. Ne pas copier de données sur des clés USB personnelles, des disques durs personnels ou des services cloud non autorisés. Ne pas transférer de fichiers patients vers un ordinateur personnel, y compris pour « travailler à la maison ».

Sécurité physique et politique du bureau propre. Ne jamais laisser de dossiers patients, de radiographies imprimées ou de documents administratifs contenant des données personnelles visibles sur un comptoir, un bureau ou à proximité de l'accueil.

Les documents papier contenant des données patients doivent être détruits à l'aide d'une déchiqueteuse, jamais jetés à la poubelle. Les écrans visibles depuis la salle d'attente ou les zones de passage doivent être positionnés ou équipés de filtres de confidentialité.

Secret professionnel. Rappel des obligations pénales : l'Art. 321 du Code pénal suisse punit la révélation de secrets confiés dans le cadre de l'exercice professionnel. Cette obligation s'applique à l'ensemble du personnel du cabinet, pas seulement au praticien.

14.3 Appareils personnels et BYOD

L'utilisation d'appareils personnels (téléphones, tablettes, ordinateurs portables, clés USB) pour accéder aux données du cabinet doit être soit interdite, soit strictement encadrée par une règle écrite. Si un collaborateur utilise son téléphone personnel pour consulter des e-mails professionnels, les données patients présentes dans ces e-mails se retrouvent sur un appareil non contrôlé par le cabinet, potentiellement non chiffré, et susceptible d'être perdu, volé ou compromis. La politique du cabinet doit définir clairement quels appareils sont autorisés, quelles applications peuvent être utilisées, et quelles données peuvent y transiter.

14.4 Personnel temporaire et tiers

Les stagiaires, remplaçants, personnel de nettoyage, techniciens externes et tout autre intervenant ayant un accès physique aux locaux du cabinet doivent être pris en compte dans la politique de sécurité. Un stagiaire présent deux semaines peut voir les mêmes écrans qu'un employé permanent. Le personnel de nettoyage intervenant en dehors des heures d'ouverture a accès aux bureaux, aux imprimantes et potentiellement aux documents laissés visibles. Les techniciens externes (fournisseurs de matériel médical, installateurs) peuvent avoir besoin d'accéder temporairement au réseau.

Chaque personne ayant un accès physique ou numérique, même temporaire, doit recevoir un minimum d'information sur les règles de confidentialité du cabinet. Pour le personnel temporaire, un document synthétique d'une page rappelant les règles essentielles, signé à l'arrivée, est suffisant.

14.5 La politique interne de sécurité écrite

La formation orale ne suffit pas. Le cabinet doit disposer d'une politique interne de sécurité informatique formalisée par écrit, remise à chaque collaborateur lors de son arrivée et mise à jour au moins une fois par an. Ce document constitue la référence en cas de litige et protège le praticien en cas d'incident : il démontre que des règles existaient, qu'elles ont été communiquées et que le collaborateur en a pris connaissance.
La politique doit couvrir au minimum les règles d'utilisation des postes de travail, la politique de mots de passe, les règles relatives à la messagerie et aux communications, l'interdiction ou l'encadrement des appareils personnels, la procédure en cas d'incident, et les sanctions internes en cas de non-respect. Chaque collaborateur signe un exemplaire attestant qu'il a lu, compris et accepté les règles. Cette signature est conservée dans le dossier du personnel.

14.6 Fréquence, format et évaluation

La formation doit avoir lieu au minimum une fois par an pour l'ensemble du personnel, avec une session dédiée lors de l'arrivée de tout nouveau collaborateur, y compris les stagiaires et les remplaçants. Le format peut être une présentation interne de 30 à 60 minutes, complétée par la remise du document de politique interne.

Pour évaluer l'efficacité de la formation, des exercices pratiques sont recommandés : simulations de phishing (envoi d'un faux e-mail frauduleux pour vérifier la réaction du personnel), quiz rapides sur les bonnes pratiques, mises en situation (un collaborateur reçoit un appel demandant un mot de passe). Ces exercices ne visent pas à piéger le personnel mais à identifier les points faibles et à adapter la prochaine session de formation en conséquence.

Documentez chaque session : date, participants, sujets abordés, résultats des exercices le cas échéant. Cette documentation fait partie des mesures organisationnelles que le PFPDT peut demander à voir en cas de contrôle.

14.7 Responsabilité partagée

Si une assistante envoie une radiographie sur WhatsApp, elle engage sa responsabilité pénale personnelle (Art. 60 nLPD et Art. 321 CP). Mais le dentiste est celui qui notifie le PFPDT et qui répond devant les patients. Sa propre exposition dépend des mesures qu'il avait mises en place : politique interne écrite et signée, formation dispensée et documentée,

gestion des accès appropriée. Si rien n'était en place, il est co-exposé pour ne pas avoir prévenu le risque. Si tout était en place et documenté, sa position est considérablement renforcée.

Chapitre 15. Assurances cyber

Même avec un niveau de sécurité informatique excellent, le risque zéro n'existe pas. Une assurance cyber permet de transférer une partie du risque financier à un assureur et de bénéficier d'une aide professionnelle en cas de crise.

15.1 Ce que couvre une assurance cyber

Les assurances cyber proposées en Suisse couvrent généralement :

- Les frais d'intervention informatique d'urgence (forensique, restauration)
- La perte de chiffre d'affaires due à l'interruption de l'activité
- Les frais de notification obligatoire (PFPDT, patients concernés)
- La responsabilité civile en cas d'atteinte aux données de tiers
- Les frais de gestion de crise et de communication
- Les frais juridiques liés à l'incident

15.2 Principaux assureurs en Suisse

Plusieurs assureurs suisses proposent des formules spécialement conçues pour les PME :

- **Zurich :** formule modulaire en 4 variantes, incluant une formation cybersécurité gratuite pour les assurés.
- **Helvetia :** assurance cyber avec hotline 24h/24 et réseau de partenaires spécialisés, label cyber-safe pour 20% de rabais.
- **AXA :** protection à trois niveaux : prévention, aide d'urgence, réparation.
- **Baloise :** trois formules (ECO, SMART, TOP) avec couverture de la rançon sous conditions.
- **Allianz :** Cyber Risk avec couverture interruption d'exploitation sur 24 mois.

15.3 Points de vigilance

Avant de souscrire, vérifiez attentivement :

- Les exclusions (certaines polices excluent les attaques si les mises à jour n'étaient pas à jour)

- Le montant des franchises, parfois élevées pour les PME
- Les conditions préalables de sécurité exigées par l'assureur
- Le plafond de couverture et sa cohérence avec votre exposition réelle
- La couverture ou non du paiement de rançon (politique variable selon les assureurs)

Conseil

L'assurance cyber ne remplace pas les mesures de sécurité ; elle les complète. Un assureur exigera un niveau minimal de protection (antivirus, sauvegardes, mots de passe) pour accepter de vous couvrir. C'est un cercle vertueux : mieux vous êtes protégé, moins la prime est élevée.

Chapitre 16. Que faire en cas d'incident

Si ça arrive (et statistiquement, pour certains cabinets, ça arrivera), les premières minutes sont déterminantes.

16.1 Scénario A : attaque active (ransomware, intrusion)

Étape 1. ISOLER : débrancher le câble réseau, désactiver le WiFi. Ne pas éteindre le poste ; cela détruit les preuves utiles pour l'analyse.

Étape 2. APPELER L'IT : votre prestataire informatique en premier. Si indisponible, l'OFCS via incidents@ncsc.ch ou le formulaire sur report.ncsc.admin.ch.

Étape 3. NE PAS PAYER : recommandation officielle de la Confédération suisse. Payer ne garantit pas la récupération des données et finance les réseaux criminels.

Étape 4. DOCUMENTER : photographier les écrans d'erreur, noter l'heure exacte de découverte, conserver tout. Ces informations seront nécessaires pour l'assurance, la police et la notification légale.

Étape 5. ÉVALUER : des données patients sont-elles touchées ? Si oui ou en cas de doute, la notification au PFPDT est obligatoire.

Étape 6. NOTIFIER : databreach.edoeb.admin.ch, dans les meilleurs délais.

16.2 Scénario B : perte ou fuite accidentelle

Perte d'un support de données, envoi au mauvais destinataire, suppression accidentelle, accès non autorisé découvert : la procédure est similaire : documenter, évaluer le risque pour les patients, notifier le PFPDT si le risque est élevé, informer les patients si nécessaire.

16.3 Ce que fait le PFPDT concrètement

Ce n'est pas une descente dans votre cabinet. Le PFPDT lit votre annonce, vérifie que vous avez réagi correctement, peut demander des précisions ou prodiguer des conseils. Sur 293 annonces reçues entre septembre 2023 et novembre 2024, seulement 26 enquêtes ont été ouvertes.

Le PFPDT ne peut pas infliger d'amende directement. Les sanctions pénales passent par les autorités cantonales et visent les violations intentionnelles, pas les cabinets qui ont notifié de bonne foi.

La règle d'or : notifier tôt vaut mieux que ne pas notifier.

Chapitre 17. Cas réels en Suisse romande

Ces attaques ne sont pas théoriques. Elles ont touché des structures médicales en Suisse romande, dans des environnements comparables à un cabinet dentaire.

Groupe 3R, Réseau Radiologique Romand (avril 2025)

Vingt centres d'imagerie médicale répartis sur sept cantons. Ransomware, vol de données médicales et administratives, tentative d'extorsion. La rançon a été refusée. L'incident a été signalé à l'OFCS.

Vidymed, Lausanne (décembre 2024)

Plus d'un mois sans accès aux dossiers patients ni à l'agenda. Phishing ciblant médecins et patients. Une situation qui paralyserait n'importe quel cabinet dentaire.

Hôpital de Rolle, Canton de Vaud (2023)

Système paralysé plusieurs jours. Prise en charge des patients mise en péril. Un hôpital cantonal à 30 minutes de Neuchâtel.

La Suisse en chiffres

Plus de 59'000 délits numériques enregistrés en Suisse en 2024. Depuis 2020, le nombre a plus que doublé. En moyenne : un cyber-incident toutes les 8 minutes et 30 secondes sur le territoire national.

Scénarios types d'attaques dans le domaine médical

Au-delà des cas réels ci-dessus, voici quatre scénarios fréquents qui touchent régulièrement des cabinets médicaux en Suisse :

Ransomware via accès distant non sécurisé

Un cabinet dentaire romand utilisait TeamViewer avec un mot de passe simple (6 chiffres) en veille permanente pour faciliter les interventions du prestataire informatique. Un attaquant a deviné le mot de passe par force brute et a pris le contrôle du serveur pendant la nuit. Résultat : ransomware déployé sur l'ensemble du réseau, 3 jours d'arrêt d'activité, rançon de 15'000 CHF demandée. Récupération partielle des données uniquement.

Phishing par fausse facture opérateur télécom

Plusieurs cabinets ont reçu un e-mail imitant Swisscom ou Sunrise avec pour objet « Votre facture impayée ». En ouvrant la pièce jointe, un cryptolocker a chiffré l'ensemble du réseau, y compris les sauvegardes connectées. Le cabinet s'est retrouvé sans aucune copie exploitable de ses données.

Usurpation d'identité du prestataire IT

Un attaquant s'est fait passer pour le prestataire informatique du cabinet par e-mail et a demandé les identifiants « pour une mise à jour urgente ». Une assistante a transmis les accès. L'attaquant a accédé au serveur et exfiltré 5'000 dossiers patients avant d'être détecté.

Clé USB infectée

Une clé USB « oubliée » dans le parking du cabinet contenait un fichier « Salaires_2025.xlsx ». Une fois connectée à un poste, elle a installé un logiciel espion enregistrant tous les mots de passe saisis au clavier. Les identifiants du logiciel dentaire, de la messagerie et de la banque en ligne ont été compromis.

Coûts approximatifs d'une cyberattaque

Les conséquences financières d'une attaque peuvent être considérables, même pour un petit cabinet :

Poste de coût	Estimation
Rançon demandée	5'000 à 50'000 CHF
Perte d'activité	2 à 10 jours d'arrêt
Reconstitution des données	10'000 à 30'000 CHF
Intervention forensique et IT d'urgence	5'000 à 15'000 CHF

Notification PFPDT et patients	2'000 à 5'000 CHF
Amende PFPDT (violation intentionnelle)	Jusqu'à 250'000 CHF
Perte de confiance des patients	Inestimable

Checklist de conformité

Utilisez cette liste pour évaluer votre niveau de conformité actuel et améliorer ce qui est manquant dans votre infrastructure actuelle. Chaque point non coché représente un risque à traiter. Un lexique des termes techniques est disponible en fin de liste.

Communications

- Messagerie chiffrée utilisée pour toute donnée patient (HIN Mail, ProtonMail ou équivalent)
- Aucune donnée patient envoyée via Gmail, Hotmail, Bluewin, WhatsApp ou SMS
- Documents papier contenant des données patients détruits par déchiqueteuse

Infrastructure

- Tous les postes sous Windows 11 ou macOS à jour
- Aucun poste sous Windows 7, 8 ou 10 sur le réseau
- Mises à jour automatiques activées sur tous les postes, serveurs et applications
- Chiffrement des disques activé sur tous les postes et serveurs (BitLocker / FileVault)
- WiFi patients séparé du réseau du cabinet

Sauvegardes

- Stratégie 3-2-1 en place (3 copies, 2 supports, 1 immuable)
- Restauration testée mensuellement

Accès et authentification

- Un compte nominatif par collaborateur, aucun compte partagé
- Mots de passe de 12+ caractères, stockés dans un gestionnaire sécurisé
- 2FA activée sur messagerie, logiciel de gestion et accès à distance
- Comptes des anciens collaborateurs désactivés
- Accès à distance via VPN ou RMM professionnel uniquement

Conformité nLPD

- Contrat de sous-traitance Art. 9 signé avec le prestataire IT

- Contrat de sous-traitance en place avec tout tiers accédant aux données patients
- Politique interne de sécurité rédigée et signée par chaque collaborateur
- Formation du personnel réalisée dans les 12 derniers mois
- Plan de réponse incident documenté et accessible
- Contacts d'urgence affichés (prestataire IT, OFCS, PFPDT)

Protection et suivi

- Solution EDR déployée et supervisée
- Audit de sécurité annuel réalisé
- Assurance cyber souscrite et conditions vérifiées

Lexique de la checklist

Messagerie chiffrée : service d'e-mail dont le contenu est verrouillé à l'envoi et ne peut être lu que par le destinataire. Ni le fournisseur, ni un pirate interceptant le message ne peuvent y accéder. Exemples : HIN Mail, ProtonMail.

Sauvegarde 3-2-1 : 3 copies de vos données, sur 2 supports différents, dont 1 copie immuable (protégée contre toute modification ou suppression, même par un virus).

BitLocker / FileVault : outils de chiffrement intégrés gratuitement à Windows (BitLocker) et macOS (FileVault). Rendent le contenu du disque dur totalement illisible en cas de vol du poste.

2FA (double authentification) : deuxième vérification après le mot de passe, généralement un code temporaire affiché sur le téléphone. Même principe que la carte bancaire : le numéro seul ne suffit pas, il faut aussi le code.

VPN : connexion chiffrée entre un appareil distant et le réseau du cabinet. Protège les données en transit comme un tunnel privé.

RMM : logiciel professionnel de télémaintenance qui enregistre chaque connexion, applique les mises à jour et surveille les postes en continu. Alternative sécurisée aux outils gratuits comme TeamViewer.

EDR : protection avancée qui analyse le comportement des programmes en temps réel et bloque les actions suspectes, même inconnues. Va au-delà de l'antivirus classique qui ne détecte que les menaces déjà répertoriées.

Art. 9 nLPD : article de loi imposant un contrat écrit entre le cabinet et tout tiers accédant aux données patients (prestataire IT, hébergeur cloud, laboratoire, comptable). Son absence est une infraction passible de 250'000 CHF.

OFCS : Office fédéral de la cybersécurité. Organisme à contacter en cas de cyberattaque. Contact : incidents@ncsc.ch ou report.ncsc.admin.ch.

PFPDT : Préposé fédéral à la protection des données et à la transparence. Autorité à notifier en cas de violation de données patients (Art. 24 nLPD). Contact : +41 58 462 43 95 ou databreach.edoeb.admin.ch.

Contacts et ressources utiles

Contacts d'urgence

- **OFCS :** Office fédéral de la cybersécurité : incidents@ncsc.ch / report.ncsc.admin.ch
- **PFPDT :** Préposé fédéral à la protection des données : +41 58 462 43 95 (lu-ve 10h-12h) / databreach.edoeb.admin.ch
- **Police cantonale :** 117

Textes légaux

- **nLPD (RS 235.1)** : www.fedlex.admin.ch
- **Ordonnance sur la protection des données (OPDo)** : www.fedlex.admin.ch
- **Guide PFPDT sur les violations de données** : www.edoeb.admin.ch
- **Guide KMU protection des données** : www.kmu.admin.ch

Ressources complémentaires

- **FMH** : outils et modèles pour cabinets médicaux : www.fmh.ch
- **HIN** : sécurité de l'information pour le domaine médical : www.hin.ch
- **No More Ransom (aide au déchiffrement)** : www.nomoreransom.org

Questions fréquentes

Les questions suivantes sont celles qui reviennent le plus souvent de la part des praticiens. Elles sont issues de situations réelles rencontrées dans des cabinets dentaires en Suisse romande.

Une perte accidentelle de données est-elle une violation au sens de la nLPD ?

Oui. L'Art. 5 let. h nLPD définit la violation de la sécurité des données comme toute perte, modification, effacement ou destruction de données personnelles, qu'elle soit accidentelle ou illicite. Supprimer par erreur des dossiers patients, perdre un disque dur ou subir une panne serveur sans sauvegarde : tout cela entre dans cette définition. Si le risque pour les patients est élevé, la notification au PFPDT est obligatoire.

Mon prestataire IT a supprimé des données. Qui est responsable ?

Vous, le dentiste, en tant que responsable du traitement (Art. 9 et Art. 25 al. 4 nLPD). Vous ne pouvez pas renvoyer le patient vers votre informaticien. Votre recours contre le prestataire n'existe que si vous avez un contrat de sous-traitance conforme. Sans contrat : aucun recours. Vous déléguez la technique, jamais la responsabilité.

Je suis retraité depuis 3 ans et une fuite datant de 4 ans est découverte. Suis-je encore concerné ?

Oui. L'Art. 66 nLPD fixe le délai de prescription de l'action pénale à 5 ans. La retraite ou la cessation d'activité ne supprime pas la responsabilité pour des faits commis pendant l'exercice professionnel. Le point de départ exact (date de la fuite ou date de découverte) nécessite l'avis d'un juriste, mais le délai de 5 ans est confirmé par la loi.

Mes iMacs sous Boot Camp Windows 10 : peut-on repasser sous macOS ?

Non, et cela ne résoudrait rien. Les logiciels dentaires (Sidexis, Romexis, DBSWin, Cliniview, DTX Studio) tournent exclusivement sous Windows. De plus, ces iMacs Intel ne peuvent souvent plus monter ni sur Windows 11, ni sur les dernières versions de macOS. Ils sont en fin de vie des deux côtés. La solution : les remplacer par des PC Windows 11 dédiés.

Quel logiciel dentaire choisir ?

Ce guide ne recommande ni ne déconseille publiquement un logiciel spécifique. En revanche, voici les critères de sécurité à vérifier : le logiciel propose-t-il la double authentification (2FA)

nativement ? L'éditeur publie-t-il des mises à jour de sécurité régulières ? Où sont hébergées les données ? L'équipe de développement dispose-t-elle de compétences en sécurité documentées ? Un logiciel médical critique est un produit IT : posez-vous la question de savoir si l'éditeur a les moyens de le faire évoluer dans la durée.

Une assistante envoie une radiographie sur WhatsApp. Qui est responsable ?

Les deux, mais pas pour les mêmes raisons. L'assistante engage sa responsabilité pénale personnelle au titre de l'Art. 60 nLPD (violation des obligations d'information) et de l'Art. 321 du Code pénal (secret professionnel). Le dentiste, de son côté, est celui qui notifie le PFPDT et qui répond devant les patients. Sa propre exposition dépend des mesures qu'il avait mises en place : politique interne écrite, formation dispensée, gestion des accès. Si rien n'existait, il est co-exposé pour ne pas avoir prévenu le risque.

Le PFPDT fait-il des contrôles dans les cabinets ?

Non, pas de rondes proactives. Le PFPDT peut ouvrir une enquête (Art. 49 nLPD), mais uniquement sur dénonciation ou suite à un incident signalé. Les sources de risque réelles pour un dentiste sont un patient mécontent, un incident qui devient public, ou une plainte d'un ancien employé. Sur 293 annonces reçues entre septembre 2023 et novembre 2024, seulement 26 enquêtes ont été ouvertes.

La nLPD impose-t-elle un délai de 72 heures comme le RGPD ?

Non. La loi suisse impose une notification « dans les meilleurs délais », une formulation volontairement plus souple que le RGPD européen qui fixe un délai strict de 72 heures. Le PFPDT recommande d'agir « le plus rapidement possible ». En pratique : agir dès la connaissance de la violation, compléter la documentation ensuite si nécessaire. Il n'existe pas de sanction spécifique en cas de retard, mais la réactivité est un facteur pris en compte dans l'évaluation de la bonne foi.

Glossaire

Les termes suivants sont utilisés dans ce guide et dans la nLPD. Ce glossaire les définit dans un langage accessible aux non-spécialistes.

Terme	Définition
nLPD	Nouvelle Loi fédérale sur la Protection des Données (RS 235.1), entrée en vigueur le 1er septembre 2023.
PFPDT	Préposé fédéral à la protection des données et à la transparence. Autorité de surveillance indépendante chargée de veiller au respect de la loi.
OFCS	Office fédéral de la cybersécurité (anciennement NCSC/MELANI). Centre de compétences de la Confédération pour les cybermenaces.
Données personnelles	Toutes les informations concernant une personne physique identifiée ou identifiable (Art. 5 let. a).
Données sensibles	Catégorie renforcée : données de santé, opinions religieuses/politiques, données génétiques, biométriques, poursuites pénales, aide sociale (Art. 5 let. c).
Responsable du traitement	La personne qui détermine les finalités et les moyens du traitement. Dans un cabinet dentaire : le praticien titulaire (Art. 5 let. j).
Sous-traitant	La personne qui traite des données pour le compte du responsable. Exemple : le prestataire informatique du cabinet (Art. 5 let. k).
Violation de la sécurité	Toute perte, modification, effacement, destruction, divulgation ou accès non autorisé à des données personnelles, de manière accidentelle ou illicite (Art. 5 let. h).
Privacy by Design	Obligation d'intégrer la protection des données dès la conception d'un système ou d'un processus (Art. 7 al. 1).

Privacy by Default	Obligation de limiter par défaut le traitement au strict minimum nécessaire (Art. 7 al. 3).
AIPD	Analyse d'impact relative à la protection des données personnelles. Obligatoire lorsqu'un traitement présente un risque élevé (Art. 22).
2FA / MFA	Double authentification / authentification multifacteur. Deuxième vérification après le mot de passe (code SMS, application, clé physique).
EDR	Endpoint Detection and Response. Solution de sécurité qui détecte les menaces par l'analyse comportementale en temps réel, et non par signature.
Ransomware	Logiciel malveillant qui chiffre les données et exige une rançon pour les débloquer.
Phishing	Technique de fraude par e-mail, SMS ou téléphone visant à obtenir des identifiants ou à faire ouvrir un fichier infecté.
BitLocker	Outil de chiffrement intégré à Windows Pro/Enterprise. Rend les données illisibles sans la clé de déchiffrement.
FileVault	Équivalent de BitLocker pour macOS. Chiffrement intégré du disque système.
VPN	Virtual Private Network. Tunnel chiffré permettant un accès distant sécurisé au réseau du cabinet.
RMM	Remote Monitoring and Management. Solution professionnelle de télémaintenance avec traçabilité (NinjaOne, Datto, Atera).
Règle 3-2-1	Stratégie de sauvegarde : 3 copies des données, sur 2 supports différents, dont 1 copie immuable (hors-ligne ou protégée contre la modification).
WPA3 / WPA2	Protocoles de sécurité WiFi. WPA3 est la version la plus récente et la plus sûre ; WPA2 est le minimum acceptable.

HIN	Health Info Net. Réseau sécurisé suisse pour les échanges entre professionnels de santé.
OPDo	Ordonnance sur la protection des données. Texte d'application de la nLPD, précisant les modalités techniques et organisationnelles.

Mentions légales et conditions d'utilisation

Ce document a été rédigé par **DentalSystems Sàrl** à des fins d'information et de sensibilisation. Il ne constitue pas un avis juridique et ne saurait engager la responsabilité de son auteur. Les informations contenues dans ce document sont à jour en date de mars 2026 et sont susceptibles d'évoluer en fonction des modifications législatives et réglementaires.

Pour toute question juridique relative à la nLPD, au RGPD ou à la protection des données dans le contexte médical, consultez un juriste spécialisé.

Propriété intellectuelle

Ce document est la propriété exclusive de DentalSystems Sàrl. L'ensemble de son contenu — textes, structure, mise en page et éléments graphiques — est protégé par le droit d'auteur conformément à la Loi fédérale sur le droit d'auteur et les droits voisins (LDA, RS 231.1).

Utilisation autorisée

Ce document est mis à disposition gratuitement et peut être librement téléchargé, imprimé et utilisé en interne au sein d'un cabinet dentaire ou d'une structure médicale, à condition que la mention de l'auteur (DentalSystems Sàrl) et le présent avis soient conservés intégralement.

Utilisations interdites

Sont strictement interdits, sauf accord écrit préalable de DentalSystems Sàrl :

- La revente ou la commercialisation de ce document, sous quelque forme que ce soit, y compris en version modifiée.
- La modification, l'adaptation ou la création d'œuvres dérivées présentées comme étant d'un autre auteur.
- La suppression, l'altération ou la dissimulation des mentions d'auteur, du logo ou des coordonnées de DentalSystems Sàrl.
- La redistribution à grande échelle par des tiers (sites de téléchargement, plateformes de partage, revendeurs) sans autorisation écrite.

Toute utilisation commerciale non autorisée constitue une violation du droit d'auteur et pourra faire l'objet de poursuites judiciaires.

Limitation de responsabilité

DentalSystems Sàrl décline toute responsabilité quant aux conséquences directes ou indirectes résultant de l'utilisation de ce document. L'utilisateur est seul responsable de l'adaptation de ces informations à sa situation spécifique. Ce document ne se substitue ni à un audit professionnel, ni à un conseil juridique.

DentalSystems Sàrl
Thomas Alvino, Technicien IT
www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44