DentiPro Privacy Policy

Privacy practices for the DentiPro website, clinic portal, professional portal, and mobile application

Effective date	October 7, 2026
Document version	2026-10-07

DentiPro Solutions LLC ("DentiPro," "we," "us," or "our") operates a technology marketplace that connects dental practices ("Clinics") with independent Registered Dental Hygienists ("Professionals"). This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information when you use our websites, portals, mobile application, support channels, or related services (collectively, the "Platform").

This Policy applies to Clinic owners and staff, Professionals, prospective users, website visitors, and people who contact us. It does not govern patient records maintained by Clinics, Checkr's candidate portal, Stripe's services, or another third party's independent practices. Those services have their own privacy notices.

1. Information We Collect

1.1 Account and identity information

- Name, email address, phone number, mailing or service address, account type, verification status, electronic signatures, consents, and account credentials. Passwords are stored using one-way password hashing rather than as readable passwords.
- Government identification images, extracted identity fields, legal name, date of birth, address, document type, partial document identifiers, expiration date, extraction confidence, and review status.
- Profile photo and other images you choose to upload.

1.2 Professional, Clinic, and credential information

- RDH license information, license jurisdiction and expiration, credential verification, professional experience, education, biography, preferences, availability, ratings, Merit Points, cancellation history, and compliance status.
- Professional malpractice insurance information and proof of coverage. CPR or BLS information is optional for onboarding but may be required for a particular shift.
- Clinic legal and display names, office locations, contacts, supervising dentists, dentist license and title information, shift requirements, and operational settings.
- Background-screening readiness, candidate and report references, status, notices, consents, and compliance decisions. Checkr generally collects highly sensitive screening data such as Social Security number directly through its hosted flow; DentiPro does not intend to store full Social Security numbers in its application database.

1.3 Shift, attendance, and marketplace information

- Shift postings, applications, counteroffers, confirmations, cancellations, schedules, rates, planned and actual breaks, clock-in and clock-out events, timesheets, corrections, disputes, reviews, and support history.
- A Professional's confirmed profile address and a Clinic's verified location coordinates, used to display approximate distance and sort open shifts.
- Attendance action, server-recorded time, booking and account identifiers, and whether the Clinic's shift code was verified through manual entry or QR scanning. Current attendance does not collect device GPS coordinates. Historical location records collected under earlier policy versions remain subject to the retention practices described below.

1.4 Payment, tax, and professional insurance information

- Stripe customer and connected-account identifiers, billing or payout readiness, payment-method type and limited display details, charges, refunds, disputes, transfers, payouts, invoices, and transaction status.
- Tax classification, taxpayer name, last four digits or provider reference for a tax identifier, Form W-9 status, and tax-reporting records. Stripe may collect full payment, bank, and tax details directly.

- Professional malpractice insurance policy, carrier, coverage, expiration, document, and verification information supplied by a Professional. DentiPro does not currently operate a platform-funded occupational accident insurance program.

DentiPro does not intentionally store complete payment-card numbers or complete bank-account numbers in its application database. Stripe processes those details under its own terms and privacy policy.

1.5 Device, usage, and communications information

- IP address, user-agent, device and browser type, operating system, app version, authentication and security events, error logs, request identifiers, and cookie or local-storage information needed to operate the Platform.
- First-party product analytics such as page visits, screen views, clicks, workflow completion, referral page, and timestamps. We use this information to understand and improve the Platform.
- Messages, email delivery and verification events, notification activity, demo or support requests, attachments, and feedback.

1.6 Information from other sources

We may receive information from Clinics and Professionals, Stripe, Checkr, professional licensing authorities, credential and sanctions sources, Amazon Web Services tools used for address selection and document extraction, public records, and service providers that help us verify, secure, or operate the Platform.

2. How We Use Information

- Create and secure accounts; verify email; resume onboarding; authenticate users; prevent unauthorized access; and provide role-appropriate features.
- Verify identity, address, professional licenses, malpractice insurance, credentials, supervising dentists, and Clinic locations.
- Run or facilitate background screening after a Professional first requests a shift; allow the Clinic to negotiate and accept while screening is pending; restrict additional shift requests when a result requires human review; and administer individualized compliance, pre-adverse, and adverse-action processes where required.
- Display, search, sort, negotiate, accept, schedule, perform, and administer shifts, including approximate distance calculations and shift-specific requirements such as CPR.
- Verify attendance with the Clinic's shift code, track breaks, prepare and correct timesheets, resolve disputes, calculate Merit Points, and prevent fraud.
- Process Clinic payments and calculate applicable marketplace fees under the Marketplace Service Agreement; pay Professionals through Stripe Connect; manage cancellation compensation; generate invoices; administer billing risk controls; and support tax reporting.
- Send email and in-app notifications—and push notifications when enabled—about verification, applications, bookings, attendance, timesheets, payments, policy changes, security, support, and other service events.
- Operate, measure, debug, maintain, and improve the Platform; develop new features; conduct internal analytics; and protect users, DentiPro, and the public.
- Comply with law, legal process, professional-board obligations, tax and accounting rules, contracts, audits, and enforceable requests, and establish, exercise, or defend legal claims.

3. When We Disclose Information

3.1 Between marketplace users

We disclose information needed to evaluate and perform shifts. A Clinic may see a Professional's name, profile photo, credentials, rating, Merit Points, application or counteroffer, screening and insurance eligibility status, attendance, and timesheet information. A Professional may see the Clinic name, verified location, supervising dentist, requirements, rating, shift details, and instructions. We limit disclosure to information reasonably relevant to the marketplace relationship.

3.2 Service providers and business partners

- Stripe for Clinic billing, Checkout, connected accounts, payouts, payment-risk controls, and tax functions.
- Checkr for consumer-report and background-screening workflows. Checkr may collect sensitive candidate information directly through its hosted experience.

- Amazon Web Services, including S3 for encrypted document storage, Textract for identity-document extraction, Location Service for address search and geocoding, and hosting, database, delivery, monitoring, security, and backup services.
- Email, notification, customer-support, professional-services, fraud-prevention, audit, and infrastructure providers that process information for us under appropriate contractual or legal restrictions.

3.3 Legal, safety, and corporate events

We may disclose information to comply with law, subpoena, court order, tax or licensing authority requests, or other valid legal process; protect safety and rights; investigate fraud, abuse, or security events; enforce agreements; or obtain professional advice. We may transfer information in a merger, financing, reorganization, bankruptcy, sale of assets, or similar transaction, subject to applicable law and appropriate confidentiality protections.

3.4 No sale or targeted-advertising sharing

DentiPro does not sell personal information for money and does not share personal information for cross-context behavioral advertising or use it for targeted advertising as those terms are defined by applicable U.S. state privacy laws. If our practices change, we will update this Policy and provide legally required choices before the change applies.

4. Background Screening and Automated Tools

Professionals upload identity documents during onboarding and confirm extracted information, but a Checkr candidate and hosted invitation are generally created only after the Professional first requests a shift and separately authorizes screening. The Clinic may negotiate and accept that application while screening is pending. Checkr and DentiPro compliance administrators—not the applying Clinic—administer the screening workflow. A result requiring review restricts additional shift requests but does not by itself cancel an accepted shift, block attendance, or hold earned compensation. DentiPro does not make a final adverse eligibility decision solely through an automated status.

Amazon Textract may extract fields from identity documents. Extraction confidence and geocoding results help prefill forms but do not by themselves make a legal or eligibility decision. You must confirm extracted information, and support-assisted correction is available for verified legal identity information.

5. Location Information

We use address coordinates selected through address autocomplete to calculate approximate mileage between a Professional and a Clinic. This distance is an estimate and may differ from driving distance or route conditions.

Attendance requires the Clinic's shift-specific code, entered manually or scanned as a QR code in the mobile application. Camera access is used only when the Professional chooses to scan; manual entry remains available without camera access. Attendance does not require location permission or enforce a GPS boundary. A valid code confirms access to that code, not physical proximity or identity. Profile and Clinic addresses and their geocoded coordinates remain in use for matching, approximate distance, directions, and other disclosed purposes.

6. Cookies, Local Storage, and Analytics

The web and mobile applications use cookies, device storage, tokens, and similar technologies needed for login, security, preferences, session continuity, and core functionality. We also maintain limited in-house analytics for page or screen visits, clicks, and feature usage. We do not currently use third-party advertising cookies for cross-site behavioral advertising. Browser or device controls may limit storage, but disabling necessary storage can prevent login or other features.

7. Data Retention

We retain information for the period reasonably necessary to provide the Platform, maintain transaction and audit integrity, resolve disputes, enforce agreements, protect safety and security, satisfy tax, accounting, professional-insurance verification, licensing, consumer-report, and other legal obligations, and preserve evidence of consent. Retention varies by record and context.

- Account and profile data is generally retained while the account is active and for a reasonable period after closure.
- Agreements, electronic signatures, consents, shift, timesheet, payment, payout, tax, audit, and dispute records may be retained for applicable limitation, reporting, and recordkeeping periods.

- Raw government-ID images are generally scheduled for deletion 30 days after identity confirmation or completed compliance review, unless a longer period is reasonably necessary for an active investigation, legal hold, unresolved verification, fraud prevention, or legal obligation. DentiPro may retain derived identity fields, masked identifiers, verification status, and audit evidence longer.
- Background-report information is retained and disposed of consistent with applicable consumer-reporting and recordkeeping requirements. Checkr independently controls retention of information in its systems under its policies and legal obligations.
- Backups and disaster-recovery copies may persist for a limited period before routine overwrite or deletion.

When retention is no longer justified, we delete, de-identify, or securely dispose of information, subject to technical and legal limitations.

8. Security

We use administrative, technical, and organizational safeguards designed to protect personal information, including encryption in transit, encryption at rest for sensitive data and documents, access controls, password hashing, field-level encryption for selected identity information, audit logging, private object storage for user-uploaded documents, network controls, monitoring, and backups. Public legal documents are intentionally available through our web delivery service. No security program can guarantee absolute protection, and users should maintain strong credentials and promptly report suspected misuse.

9. Your Choices and Privacy Rights

You may update many profile fields in the Platform, control device permissions, choose whether to apply for a shift, and manage communication settings where available. Certain verified legal-name, credential, tax, payment, and compliance fields require support-assisted correction to preserve audit integrity.

Depending on where you live and applicable law, you may have rights to request access, confirmation, correction, deletion, or portability of personal information; obtain information about categories of collection and disclosure; opt out of a sale, targeted advertising, or certain profiling; limit certain uses of sensitive information; appeal a denied request; and receive equal service without unlawful discrimination for exercising a right. DentiPro does not currently sell personal information or use it for targeted advertising.

Submit privacy or account-deletion requests to support@mydentipro.com. We may verify identity and authority before acting, may deny or limit a request where an exception applies, and will explain available appeal options when required. An authorized agent may submit a request where permitted, but we may require proof of authority and direct identity verification.

10. Communications

Service communications—including verification codes, security alerts, booking and attendance events, screening notices, timesheets, payments, policy updates, and support responses—are part of operating the Platform and may not be fully optional while an account is active. Marketing communications, if introduced, will include legally required unsubscribe choices. Carrier, internet, or data charges may apply.

11. Children

The Platform is intended for adults and is not directed to children under 18. We do not knowingly create accounts for or collect personal information directly from children. Contact us if you believe a child has provided personal information.

12. U.S. Processing and State-Specific Notices

DentiPro currently operates in the United States. Information may be processed in states other than the one in which you live. Federal, state, and local laws may provide additional rights or impose different rules, particularly for consumer reports, criminal-history information, precise geolocation, professional records, and biometric information. DentiPro or Checkr will provide separate notices where required. This Policy does not replace a standalone background disclosure, screening authorization, or state-specific consumer-report notice.

13. Changes to This Policy

We may update this Policy to reflect changes in the Platform, law, vendors, or data practices. We will post the updated version with a new effective date and provide additional notice or request renewed acceptance when required. Material changes will not be applied retroactively where prohibited.

14. Contact Us

Questions, privacy requests, account-deletion requests, and security reports may be sent to:

DentiPro Solutions LLC
Email: support@mydentipro.com