

Privacy Policy & HIPAA Notice of Privacy Practices

Effective Date: January 1, 2025 | Last Reviewed: July 20, 2026

THIS NOTICE DESCRIBES HOW YOUR MEDICAL AND OTHER PERSONAL INFORMATION MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.

SculptorRx Medspa ("SculptorRx," "the Practice," "we," "us," or "our") is committed to protecting the privacy and security of the personal and health information entrusted to us by our clients and website/booking-portal visitors. This Privacy Policy and HIPAA Notice of Privacy Practices ("Notice") explains the categories of information we collect — including Protected Health Information ("PHI") and other personal information collected through our online booking portal — how we may use and disclose that information for medical and commercial purposes, your rights regarding your information, the safeguards we use to protect it, and what happens if a breach occurs.

This Notice is designed to comply with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (the "HIPAA Privacy Rule," 45 C.F.R. Parts 160 and 164), the HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400–414), Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), the FTC's Health Breach Notification Rule (16 C.F.R. Part 318), and applicable Texas law, including Texas Occupations Code Chapter 159 and the Texas Medical Records Privacy Act (Tex. Health & Safety Code Chapter 181).

This Notice applies to information we collect in person at the Practice and information collected through our public website and online booking portal, whether or not you have an existing treatment relationship with us.

TABLE OF CONTENTS

1. Definitions
2. Information We Collect
3. How We Use and Disclose Your Information
4. Minimum Necessary Standard
5. Your Rights Regarding Your Information
6. Data Security, Storage & Retention
7. Breach Notification Procedures
8. Business Associates & Third-Party Service Providers
9. Cookies, Analytics & Booking Portal Data Practices
10. Marketing Communications & Consent
11. Children's Privacy
12. Changes to This Notice
13. No Retaliation

14. Contact Us / Privacy Officer

Acknowledgment (Booking Portal Integration)

1. DEFINITIONS

- Protected Health Information (PHI). Individually identifiable health information — including demographic data, medical history, treatment records, photographs, consultation notes, Good Faith Exam findings, and billing information — that we create, receive, maintain, or transmit in any form (oral, written, or electronic) relating to your past, present, or future physical or mental health condition, the provision of aesthetic or medical services to you, or payment for those services, and that identifies you or could reasonably be used to identify you (45 C.F.R. § 160.103).
- Individually Identifiable Health Information. PHI that identifies the individual, or provides a reasonable basis to believe the information can be used to identify the individual.
- De-Identified Information. Information from which all required identifiers have been removed such that it cannot reasonably be used to identify an individual, per 45 C.F.R. § 164.514. De-identified information is not PHI and is not subject to this Notice's PHI-specific protections.
- Covered Entity. SculptorRx Medspa, as a health care provider that conducts certain transactions electronically, is a "Covered Entity" under HIPAA.
- Business Associate. A person or organization (other than a member of our workforce) that performs functions or services on our behalf involving the use or disclosure of PHI, such as our electronic health record vendor, payment processor, or booking/scheduling platform.
- Treatment, Payment, and Health Care Operations ("TPO"). The core purposes for which PHI may be used or disclosed without your written authorization, as defined at 45 C.F.R. § 164.501.
- Marketing. Under HIPAA, a communication about a product or service that encourages you to purchase or use it, other than certain treatment-related or operational communications. Marketing communications require your prior written authorization, which must disclose whether SculptorRx receives payment from a third party for making the communication.
- Sale of PHI. Any disclosure of PHI in exchange for direct or indirect remuneration. SculptorRx does not sell PHI; any exception requires your specific written authorization stating that the disclosure is a sale and identifying any remuneration.
- Personal Health Record / Consumer Health Information (FTC). Health-related information about you that you or our systems input, collect, or generate through our website or online booking portal, which may fall under the FTC Act and the FTC's Health Breach Notification Rule even if it is not PHI subject to HIPAA — for example, wellness information submitted through a public intake questionnaire before a treatment relationship exists.
- Breach. The acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the information (45 C.F.R. § 164.402), or, for information not subject to HIPAA, any acquisition of unsecured, individually identifiable health information without the individual's authorization, as defined by the FTC's Health Breach Notification Rule (16 C.F.R. § 318.2).

2. INFORMATION WE COLLECT

2.1 Health Information Collected as a Covered Entity (PHI)

- Identifying and demographic information: name, date of birth, address, phone number, email, and emergency contact.
- Health history: medical conditions, medications, allergies, pregnancy status, and prior aesthetic procedures, collected via intake and Good Faith Exam forms.
- Treatment records: consultation notes, procedure/treatment notes, provider assessments, clinical photographs (before/after), and lab or diagnostic information where applicable.
- Billing and payment records tied to treatment.
- Communications with our clinical staff regarding your care.

2.2 Information Collected Through Our Online Booking Portal & Website

- Contact and scheduling information: name, phone, email, appointment preferences, and service selection.
- Payment card and billing details, processed via a secure third-party payment processor.
- Pre-visit questionnaire responses (e.g., skin concerns, treatment goals) submitted before an in-person provider relationship is established.
- Technical and device information: IP address, browser type, device identifiers, pages visited, and referral source.
- Cookies and similar tracking technologies (see Section 9).

2.3 Distinguishing Medical Use from Commercial Use

Information you provide during an active treatment relationship for the purpose of diagnosis, treatment, or payment is PHI governed by the HIPAA Privacy Rule. Information you provide through general website browsing, marketing sign-ups, promotional contests, or before a treatment relationship is established (e.g., a newsletter sign-up) is treated as commercial personal information governed by the FTC Act and, where applicable, the FTC Health Breach Notification Rule and Texas consumer privacy law. As a matter of practice, we apply HIPAA-equivalent safeguards to both categories of information, and this Notice describes our obligations for each.

3. HOW WE USE AND DISCLOSE YOUR INFORMATION

3.1 Permitted Uses/Disclosures Without Your Written Authorization

We may use and disclose your PHI without your written authorization for:

- Treatment — coordinating your care among our providers, injectors, and any referred specialists.
- Payment — billing, claims processing, and collecting payment for services.
- Health Care Operations — quality assessment, staff training, credentialing, business planning, and internal audits.
- As required by law.
- Public health activities (e.g., adverse event reporting for injectables).
- Health oversight activities, such as state licensing board inspections.
- Judicial and administrative proceedings, in response to a valid court order or subpoena.
- Law enforcement purposes, under limited circumstances defined by law.
- To avert a serious threat to health or safety.

- Workers' compensation claims.
- To family, friends, or others involved in your care, if you do not object and disclosure is in your best interest.
- Appointment reminders, treatment alternatives, and health-related benefits or services — these are permitted incidental communications, not “marketing” under HIPAA.

3.2 Uses/Disclosures That Require Your Prior Written Authorization

- Any marketing communication that promotes a product or service and is not related to your treatment or covered by the incidental-communications exception (e.g., using your before/after photos in advertising or on social media).
- Any sale of PHI.
- Disclosure of psychotherapy notes (not generally applicable to SculptorRx's aesthetic services).
- Any other use or disclosure not described in this Notice.

You may revoke a written authorization at any time, except to the extent we have already relied on it. To revoke, submit a written request to our Privacy Officer using the contact information in Section 14.

3.3 Medical Purposes vs. Commercial/Marketing Purposes — Our Commitment

SculptorRx maintains a clear operational distinction between using your information to provide and bill for aesthetic medical services (“Medical Purposes”) and using your information to promote our practice, products, or services (“Commercial Purposes”):

- We will never use your PHI, including clinical photographs, for advertising, social media, testimonials, or marketing without your separate, specific, written authorization.
- We will never sell, rent, or trade your PHI or your booking-portal personal information to third parties, data brokers, or advertisers.
- Promotional emails, text messages, or advertising communications are sent only if you have affirmatively opted in, and you may opt out at any time, consistent with the CAN-SPAM Act and the Telephone Consumer Protection Act.
- We make truthful, non-deceptive representations about our data practices in all client-facing materials, consistent with our obligations under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements about how consumer health data is collected, used, or shared.
- If our data practices change in a way that expands use of previously collected information, we will provide advance notice and, where required, obtain your renewed consent before applying the change.

4. MINIMUM NECESSARY STANDARD

In accordance with the HIPAA “minimum necessary” standard (45 C.F.R. § 164.502(b)), SculptorRx limits access to, and use and disclosure of, PHI to the minimum amount reasonably necessary to accomplish the intended purpose:

- Role-based access. Clinical staff (providers, injectors) may access full treatment records necessary for care. Front-desk and remote receptionist staff may access only scheduling, contact, and billing information necessary to book and confirm appointments — not clinical treatment notes or photographs — unless specifically required for their job function.

- Unique user credentials. Every workforce member accesses our electronic health record system (Aesthetic Record) and booking platform through individually assigned login credentials; shared logins are prohibited.
- Access logging and audit. System access to PHI is logged and periodically reviewed for appropriateness.
- Workforce training. All employees and contractors, including remote receptionist staff, complete HIPAA privacy and security training before accessing any client information and on a periodic basis thereafter.
- Business associate limits. Vendors and contractors (e.g., EHR provider, payment processor, booking platform, remote receptionist) receive access only to the PHI necessary to perform their contracted function, governed by a signed Business Associate Agreement.
- Sanctions. Workforce members who access, use, or disclose PHI beyond what is necessary for their role are subject to disciplinary action up to and including termination, and may be reported to appropriate authorities.

5. YOUR RIGHTS REGARDING YOUR INFORMATION

- Right to Access and Obtain a Copy. You may inspect and obtain a copy of your PHI in our designated record set, in the form and format you request if readily producible, generally within 15 business days of a written request (Tex. Occ. Code § 159.006). See our Medical Record Request & Authorization form.
- Right to Request Amendment. You may request that we amend PHI you believe is incorrect or incomplete. We may deny the request in certain circumstances (e.g., if the record is accurate) and will provide our reasoning in writing.
- Right to an Accounting of Disclosures. You may request a list of certain disclosures of your PHI made in the six years prior to your request, excluding disclosures for treatment, payment, health care operations, and certain other categories.
- Right to Request Restrictions. You may ask us to limit how we use or disclose your PHI for treatment, payment, or health care operations, or to restrict disclosures to your health plan for services you paid for in full out-of-pocket. We are not required to agree to all requests but must honor a request to restrict disclosure to a health plan for services paid in full by you.
- Right to Request Confidential Communications. You may ask us to contact you in a specific way (e.g., a personal cell number) or at a different location.
- Right to a Paper Copy of This Notice. You may request a paper copy of this Notice at any time, even if you agreed to receive it electronically.
- Right to Be Notified of a Breach. You have the right to receive notification if a breach of your unsecured PHI (or, where applicable, your unsecured health information under the FTC Health Breach Notification Rule) occurs, as described in Section 7.
- Right to File a Complaint. You may file a complaint with our Privacy Officer, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR"), or the Federal Trade Commission for concerns related to our online booking portal and commercial data practices. We will not retaliate against you for filing a complaint. Contact details are in Section 14.

6. DATA SECURITY, STORAGE & RETENTION

6.1 Safeguards

- Administrative: written policies and procedures, workforce training, a designated Privacy and Security Officer, and periodic risk assessments.
- Physical: locked facilities and file storage, restricted access to areas where records are kept, and secure device management.
- Technical: encryption of PHI in transit and at rest where technically feasible, role-based access controls, multi-factor authentication, firewalls, and secure, PCI-compliant payment processing for booking-portal transactions.

6.2 Where Your Information Is Stored

- Clinical and treatment records are maintained in our electronic health record platform (Aesthetic Record) and, where applicable, in physical files at our practice location.
- Booking and scheduling information submitted through our online booking portal is transmitted via encrypted connection and stored by our booking platform and/or EHR vendor, each bound by a Business Associate Agreement where PHI is involved.
- Payment information is processed by a PCI-DSS compliant third-party payment processor; SculptorRx does not store full payment card numbers.

6.3 Retention

We retain PHI in accordance with Texas Medical Board recordkeeping requirements and Texas Occupations Code Chapter 159 — generally a minimum of seven (7) years from the date of last treatment for adult clients, and until a minor client's 21st birthday, whichever is longer, unless a longer period is required by law or by our professional liability insurer. Non-PHI commercial information collected through our website (e.g., marketing opt-in records) is retained only as long as necessary for the purpose collected or as required by law, after which it is securely deleted or de-identified.

7. BREACH NOTIFICATION PROCEDURES

7.1 HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400–414)

If we discover a breach of unsecured PHI, we will:

- Conduct a risk assessment to determine the probability that the PHI has been compromised.
- Notify each affected individual by first-class mail (or email if previously agreed) without unreasonable delay and in no case later than 60 calendar days after discovery.
- Provide substitute notice (website posting or media notice) if we have insufficient contact information for 10 or more affected individuals.
- Notify the U.S. Department of Health and Human Services Secretary — concurrently with individual notice if the breach affects 500 or more individuals, or annually if fewer than 500.
- Notify prominent media outlets if a breach affects 500 or more residents of Texas or another single jurisdiction.
- Require any Business Associate that experiences a breach to notify SculptorRx without unreasonable delay and no later than 60 days after discovery, so that we can in turn notify affected individuals.

7.2 FTC Health Breach Notification Rule (16 C.F.R. Part 318)

To the extent our online booking portal, wellness questionnaires, or related digital tools collect health information that falls outside HIPAA's coverage — for example, information submitted by a website visitor before any treatment relationship is established, or information handled by a technology vendor acting as a

"PHR-related entity" or "vendor of personal health records" — a breach of that information, including unauthorized disclosure or sharing without your consent, will be handled consistent with the FTC's Health Breach Notification Rule:

- Affected individuals notified without unreasonable delay and no later than 60 calendar days after discovery.
- The FTC notified within 10 business days if 500 or more individuals are affected, or via annual log if fewer than 500.
- Media notified if 500 or more residents of a state or jurisdiction are affected.
- Notices will describe what happened, the types of information involved, steps we are taking in response, and how to contact us.

7.3 Our Internal Response Protocol

- Immediate containment and investigation upon discovery of a suspected incident.
- Risk assessment and legal review to determine notification obligations.
- Notification to affected individuals, regulators, and media as required above.
- Documentation of the incident, our response, and any corrective action in a breach log retained for a minimum of six years.
- Remediation steps, including additional safeguards or workforce retraining, to prevent recurrence.

8. BUSINESS ASSOCIATES & THIRD-PARTY SERVICE PROVIDERS

We share PHI only with vendors who sign a Business Associate Agreement obligating them to safeguard PHI consistent with HIPAA, including our electronic health record and client-management platform, our online booking/scheduling platform, our payment processor, and our remote/virtual receptionist service. We remain responsible for ensuring these relationships are properly documented and that vendors report any breach to us as required by their Business Associate Agreement.

9. COOKIES, ANALYTICS & BOOKING PORTAL DATA PRACTICES

Our website and online booking portal may use cookies, pixels, and similar tracking technologies to operate the booking system, remember your preferences, and understand how visitors use our site. These technologies may collect non-health browsing data (e.g., pages viewed, device type) and, in limited cases, information you voluntarily submit through pre-visit questionnaires.

- We do not sell your personal information or health information to third parties or data brokers.
- We do not share health-related information collected through our booking portal with advertising networks or analytics providers for behavioral advertising purposes.
- You can control cookies through your browser settings; disabling cookies may affect booking portal functionality.
- Any third-party analytics or advertising tools we use are configured, to the extent possible, to avoid collecting or receiving sensitive health information, consistent with FTC guidance on unfair and deceptive practices involving consumer health data.

10. MARKETING COMMUNICATIONS & CONSENT

- We will only send you promotional emails, texts, or calls if you affirmatively opt in (e.g., by checking a consent box on the booking portal or intake form).
- Every marketing communication includes a clear, functioning method to opt out or unsubscribe, honored promptly and no later than required by the CAN-SPAM Act.
- Appointment reminders, confirmations, and other operational messages related to your scheduled care are not "marketing" and may be sent regardless of promotional opt-in status, unless you separately request otherwise.
- We do not use your clinical photographs, testimonials, or treatment details in any marketing material without your separate written authorization.

11. CHILDREN'S PRIVACY

Our services and booking portal are intended for adults. We do not knowingly collect personal information online from children under 13 without verifiable parental consent, consistent with the Children's Online Privacy Protection Act (COPPA). If a minor receives services with appropriate parental/guardian consent, all related health information is treated as PHI under this Notice and released only to the minor's parent or legal guardian, as permitted by Texas law, unless the minor independently consented to treatment under an applicable exception.

12. CHANGES TO THIS NOTICE

We reserve the right to change the terms of this Notice and to make the revised Notice effective for PHI we already maintain, as well as any information received in the future, consistent with 45 C.F.R. § 164.520(b)(1)(v)(C). If we make a material change, we will post the updated Notice on our website and booking portal, update the effective date, and, where required by the FTC Act for changes materially expanding use of previously collected commercial data, obtain your affirmative consent before applying the change retroactively. A current copy of this Notice is always available at our practice and on our booking portal.

13. NO RETALIATION

SculptorRx will not retaliate against you, deny you services, or otherwise treat you adversely for exercising any right described in this Notice or for filing a complaint with us, the U.S. Department of Health and Human Services, or the Federal Trade Commission.

14. CONTACT US / PRIVACY OFFICER

If you have questions about this Notice, wish to exercise any of the rights described above, or want to file a complaint, please contact:

Privacy Officer: Brandy Martinez Lopez, Owner
Practice: SculptorRx Medspa
Address: 536 W Randol Mill Rd, Suite 143, Arlington, TX 76011
Phone: 817-726-7042
Email: sculptorrx@icloud.com

Note: The email address above is a standard, unencrypted email account. Please do not send Protected Health Information (PHI), such as details about your treatment, diagnosis, or medical history, through this email address. Use our secure patient portal or call the office directly for any communication containing PHI.

You may also file a complaint with:

- U.S. Department of Health and Human Services, Office for Civil Rights — hhs.gov/ocr/privacy/hipaa/complaints
- Federal Trade Commission — reportfraud.ftc.gov

ACKNOWLEDGMENT — BOOKING PORTAL INTEGRATION

By checking the box below and submitting this form, I acknowledge that I have read and been given the opportunity to review the SculptorRx Medspa Privacy Policy and HIPAA Notice of Privacy Practices, and I understand how my medical and personal information may be used and disclosed as described above.

☐ I acknowledge and accept this Privacy Policy & Notice of Privacy Practices.

Template Disclaimer: This document is a customizable template provided for general informational purposes and does not constitute legal advice. Have this policy reviewed by a licensed Texas attorney before publishing it on your booking portal or website to ensure it reflects your practice's specific operations, vendor relationships, and any additional state law requirements.