

Website and Marketing Privacy Policy

Epstein Plastic Surgery

Effective Date: April 27, 2026

1. Scope of this Policy

This Website and Marketing Privacy Policy explains how Epstein Plastic Surgery collects, uses, discloses, and protects information collected through our website, online forms, advertising landing pages, social media pages, email, phone, text messaging, and other marketing or general inquiry channels.

This policy is separate from our HIPAA Notice of Privacy Practices. Our HIPAA Notice of Privacy Practices explains how we may use and disclose protected health information in connection with consultations, treatment, payment, health care operations, medical records, and patient rights. If information you provide through a website or marketing channel is protected health information under HIPAA or other applicable law, we will handle that information in accordance with our HIPAA Notice of Privacy Practices and applicable law.

This policy does not apply to information collected through a secure patient portal, medical record system, billing system, or clinical communication system, except where this policy specifically says otherwise.

2. Medical Disclaimer and Emergency Notice

Do not use website forms, social media, email, or text messages for medical emergencies, urgent symptoms, post-operative complications, or time-sensitive clinical concerns. Call 911 in an emergency. For clinical questions or urgent post-operative issues, call our office or use the secure communication method provided to you.

Submitting a website form, sending a message, or receiving a response from us does not establish a provider-patient relationship and does not constitute medical advice. A formal consultation and appropriate clinical evaluation are required before medical advice, diagnosis, or treatment recommendations can be provided.

3. Information We Collect

We may collect the following categories of information, depending on how you interact with us:

- **Contact information:** name, email address, telephone number, mailing address, and communication preferences.
- **Inquiry information:** procedure interests, requested consultation dates, message content, referral source, and information you choose to provide in a form or message.
- **Communication records:** records of calls, emails, texts, appointment requests, opt-in or opt-out preferences, and related notes.
- **Files or photographs:** photos, documents, or other materials only if you choose to upload or send them. General marketing forms are not intended for sensitive medical information or photographs unless the form is specifically identified as secure and appropriate for that purpose.
- **Website and device information:** IP address, browser type, device identifiers, pages viewed, referring URLs, approximate location, clickstream data, cookies, pixels, tags, and similar technologies.
- **Social media and advertising information:** interactions with our pages, ads, or content on platforms such as Meta, Instagram, Facebook, Google, or other third-party platforms, subject to those platforms' own policies.

Please do not submit Social Security numbers, insurance cards, medical record documents, detailed medical histories, photographs, or other sensitive information through general website forms, social media messages, or unsecured email unless we specifically instruct you to use a secure channel for that purpose.

4. How We Use Information

We may use information collected through website, marketing, and general inquiry channels to:

- Respond to inquiries and requests for information.
- Schedule, confirm, reschedule, or follow up about consultations or appointments.
- Provide information about our practice, providers, services, policies, and patient experience.
- Send appointment-related, administrative, or service-related communications.
- Send marketing or promotional communications when you have consented or when otherwise permitted by law.
- Operate, maintain, secure, test, and improve our website, forms, communications, advertising, and user experience.
- Measure advertising performance and understand how users interact with our website and ads.
- Maintain records of communications, consent, opt-outs, and requests.
- Detect, investigate, or prevent fraud, misuse, security incidents, or unlawful activity.
- Comply with legal, regulatory, licensing, professional, insurance, reporting, or risk-management obligations.

5. Calls, Emails, and Text Messages

By providing your phone number or email address and submitting a form or otherwise consenting, you authorize Epstein Plastic Surgery and its service providers to contact you by phone, email, or text message, including through automated systems, about your inquiry, appointments, services, and related information. Message frequency may vary. Message and data rates may apply. Consent to marketing calls or text messages is not a condition of receiving services or making a purchase.

You may opt out of marketing text messages by replying STOP. You may request help by replying HELP. You may opt out of marketing emails by using the unsubscribe link in an email or contacting us. We may continue to send non-marketing, transactional, appointment-related, legally required, or clinical communications as permitted by law.

Email and text messaging may not be fully secure. Please do not include sensitive medical details in standard email or text messages unless we have provided a secure method and you understand the risks of the communication method you choose.

6. Cookies, Pixels, Analytics, and Advertising Technologies

Our website and advertising pages may use cookies, pixels, tags, analytics tools, call tracking tools, session measurement tools, and similar technologies. These technologies may collect information such as pages viewed, links clicked, IP address, device and browser information, referring website, approximate location, and interactions with ads or forms.

We may use platforms such as Meta, Instagram, Facebook, Google, or similar services for analytics, advertising, audience measurement, and campaign performance. These third parties may process information according to their own privacy policies and settings.

We do not knowingly configure third-party advertising pixels, session replay tools, or similar technologies to collect or disclose protected health information. We avoid placing third-party advertising trackers on patient portals, secure messaging systems, online appointment or request forms that collect health details, photo upload tools, payment pages, or other pages where protected health information may be entered, unless the use is permitted by law and appropriate agreements or authorizations are in place. A website cookie banner or this policy is not a HIPAA authorization.

You can adjust browser settings to refuse or delete cookies. Some advertising platforms also provide account-level privacy and ad preference controls. Blocking cookies may affect website functionality.

7. How We Share Information

We may share information as described below:

- **Service providers:** with vendors that help us operate our website, forms, scheduling tools, customer relationship management systems, email and text messaging, call tracking, advertising, analytics, hosting, cloud storage, IT, cybersecurity, payment processing, legal, compliance, and administrative services.
- **Business associates:** when a vendor creates, receives, maintains, or transmits protected health information on our behalf, we require appropriate HIPAA business associate agreements or other safeguards as required by law.
- **Legal and regulatory purposes:** when required or permitted by law, court order, subpoena, licensing board, regulatory inquiry, audit, investigation, insurance, risk-management process, or to protect rights, safety, and security.
- **With your direction or consent:** when you ask us to share information or authorize a disclosure.
- **Practice transitions:** in connection with a merger, acquisition, financing, reorganization, sale of assets, or transfer of practice operations, subject to applicable privacy laws and safeguards.

We do not sell or rent your personal information. We do not sell protected health information. We do not disclose protected health information to advertising platforms for their independent advertising purposes unless you have provided a valid written authorization or the disclosure is otherwise permitted by law. We may use or share information that has been de-identified or aggregated so that it does not identify you.

8. Social Media, Reviews, Testimonials, and Photographs

Information you post publicly on social media, review sites, or other public platforms may be visible to others and may be collected or used by those platforms according to their own policies. We generally will not respond publicly in a way that confirms patient status or discloses protected health information.

We will not use your protected health information, testimonial, story, image, video, or before-and-after photographs for marketing, advertising, website, social media, or promotional purposes without a separate written authorization when required by law. Do not submit photographs through public or unsecured channels unless we specifically provide a secure method and instruct you to do so.

9. Legal Requests and Sensitive Health Activities

If we receive a subpoena, court order, investigative demand, or other request for information, we will review the request under applicable federal and New York law before responding. For requests that may relate to reproductive health care, gender-affirming care, or other legally protected health activity under New York law, we will apply any required New York safeguards, notices, and restrictions before any disclosure.

10. Data Security and Retention

We maintain administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of personal information and protected health information. These safeguards may include access controls, workforce training, vendor review, secure disposal practices, system monitoring, and other measures appropriate to the nature of the information and our operations.

No website, email system, text system, or electronic storage system is completely secure. You should not submit confidential or sensitive information through general marketing forms or unsecured communication channels.

We retain information for as long as reasonably necessary for the purposes described in this policy, including to respond to inquiries, maintain communication and consent records, comply with legal and professional obligations, resolve disputes, maintain security, and preserve business records. Medical records and protected health information are retained according to applicable medical record, HIPAA, New York, professional, billing, insurance, and legal requirements. If a breach of personal information or protected health information occurs, we will investigate and provide notices as required by applicable law.

11. Your Choices and Rights

You may contact us to request access to, correction of, or deletion of personal information collected through website or marketing channels. We may need to verify your identity before responding. We may deny or limit a request where retention is required or permitted by law, including for medical records, billing records, consent records, legal obligations, security, fraud prevention, or legitimate business purposes.

For rights involving protected health information in medical, consultation, billing, or patient records, please review our HIPAA Notice of Privacy Practices. That Notice explains rights such as access to medical records, amendments, confidential communications, restrictions, accountings of disclosures, breach notifications, and complaint rights.

You may opt out of marketing communications as described in Section 5. You may manage cookies and advertising preferences as described in Section 6.

12. Children and Minors

Our website and marketing channels are not directed to children under 13. We do not knowingly collect personal information from children under 13 through general website forms. If you believe a child has submitted information to us through a general website form, please contact us so we can review and delete the information where appropriate.

For minor patients or prospective patients, a parent, guardian, or legally authorized representative should contact the practice through appropriate channels. Certain minors may have privacy rights under federal or New York law, and we will handle those situations in accordance with applicable law.

13. Third-Party Websites and Platforms

Our website, emails, ads, or social media pages may link to third-party websites or platforms. We are not responsible for the privacy, security, or content practices of third parties. Please review the privacy policies and settings of any third-party websites or platforms you use.

14. Changes to this Policy

We may update this policy from time to time. The updated policy will be posted on our website with a new effective date. Changes apply to information collected after the updated effective date and, where permitted by law, to information we already maintain.

15. Contact Us

For privacy questions, communication preferences, or requests involving website or marketing information, contact us at:

Practice	Epstein Plastic Surgery
Privacy Officer	Ruth Verspoor, Director of Operations / Privacy Officer
Address	200 Motor Parkway, Suite B12 Hauppauge, NY 11788

Phone / Fax	Phone: 631-689-1100 Fax: 631-751-0103
Email / Website	Email: rverspoor@epsteinplasticsurgery.com Website: www.epsteinplasticsurgery.com