Regener8 Health & Wellness

Privacy Policy

Last updated: July 1, 2025

1. Purpose & Scope

This Privacy Policy explains how we collect, use, disclose, and safeguard personal information—including protected health information ("PHI")—obtained through any Regener8 Health & Wellness or telemedicine platform, laboratory, wellness program, website, email, or other channel (collectively, "Services"). It applies to patients, prospective patients, caregivers, and any person who submits data to us.

2. Information We Collect

Category	Examples & Sources	Basis for Collection
Personal Identifiers	Name, date of birth, address, phone, email, emergency contacts (via intake/HQ forms, phone calls, secure portals).	Contractual necessity (providing care); legitimate interest (patient identification).
Clinical & Wellness Data	Medical history, medications, allergies, vitals (InBody scans, BP, HR), physical-exam notes, symptom questionnaires.	Provision of treatment; legal/ethical obligation.
Laboratory & Diagnostic Results	Hormone panels, blood chemistry, metabolic profiles (drawn in-clinic or via third-party labs).	Provision of treatment; legal/ethical obligation.
Telemedicine & Communications	Audio/video consult recordings, secure messages, emailed forms ("What to Expect"), PCC follow-up notes.	Provision of treatment; quality assurance; regulatory compliance (HIPAA).
Device & Usage Data	IP address, browser type, referring pages (if you access patient portals or websites).	Site functionality; security; analytics.

NOTE: We do not request or store credit-card data within clinical systems; payment details are processed separately per our Credit-Card Authorization Form.

3. How We Use Your Information

- Diagnose, treat, and monitor hormone-replacement and wellness conditions.

- Develop custom therapy protocols, medication/supplement schedules, and detox recommendations.
- Schedule appointments, lab work, and follow-up calls (e.g., Week 1, Day 21, Week 6, etc.).
- Communicate lab results, care plans, shipping notices, and tracking numbers.
- Maintain legal medical records, submit insurance claims (when applicable), and satisfy regulatory reporting.
- Improve quality of care, perform internal audits, training, and protocol refinement.
- De-identified data may be aggregated for research or statistical analysis; no patient will be personally identifiable in such reports.

4. Disclosures & Sharing

We disclose PHI only as allowed under HIPAA and related state privacy laws:

Recipient	Purpose	Safeguards
Network Physicians & Licensed Providers	Direct care, consults, prescription authority.	Role-based EMR access; secure telehealth platform.
Laboratories & Diagnostic Facilities	Collection, testing, and result reporting.	HIPAA-compliant lab portals; encrypted interfaces.
Patient-Care Coordinators (PCCs)	Scheduling, protocol coaching, ongoing wellness check-ins.	Signed confidentiality agreements; audit logs.
Order Processors / Pharmacies / Supplement Vendors	Fulfillment of medications, NAD IVs, supplements.	Minimum necessary data; tracking shared via secure email/portal.
Insurance Payers (if elected)	Eligibility verification, claims, prior authorization.	HIPAA EDI standards.
Regulators & Law-Enforcement	When required by subpoena, court order, or statute.	Legal review before disclosure.

We never sell or lease patient information to third-party marketers.

5. Patient Rights

- Access & Copies – Inspect or obtain a copy of your medical record.
- Amend – Request corrections to incomplete or inaccurate information.
- Request Restrictions – Limit disclosures to family, insurance, or others.
- Confidential Communications – Specify preferred contact methods or addresses.
- Accounting of Disclosures – Receive a log of non-treatment-related disclosures.
- Revoke Authorization – Withdraw any prior consent prospectively.
- File a Complaint – With our Privacy Officer or HHS without retaliation.

6. Data Security

- Encryption – All EMR data at rest and in transit uses industry-standard encryption.

- Access Controls – Multi-factor authentication and role-based permissions restrict staff access.
- Audit Trails – Automatic logging of chart access, edits, and disclosures.
- Secure Disposal – Paper records shredded; electronic data wiped per NIST SP 800-88.
- Incident Response – Breach-notification plan consistent with HIPAA/HITECH requirements.

7. Data Retention

Medical records are retained for at least seven (7) years from the last date of service—or longer if required by state law—after which they are securely destroyed or archived.

8. Telemedicine & Electronic Communications

By engaging in telehealth visits or receiving emailed materials, you acknowledge:

- Electronic communications may carry inherent security risks; we use HIPAA-compliant platforms to mitigate these risks.
- You may opt out of unencrypted email or SMS reminders at any time by notifying your PCC.

9. Third-Party Links & Portals

Our websites or emails may link to external labs, pharmacies, or wellness resources. We are not responsible for the privacy practices of those sites. Review each third party's policy before providing personal data.

10. Policy Updates

We may revise this Privacy Policy to reflect operational, legal, or regulatory changes. Updated versions will be posted on our website and effective on the "Last updated" date. Material changes affecting your rights will be communicated via email or during your next visit.

11. Contact Us

Regener8 Health & Wellness, LLC
2901 NW Commerce Park Drive Suite 1
Boynton Beach FL, 33426
Email: admin@regener8now.com

Acknowledgment

By continuing to engage with Regener8 Health & Wellness, you acknowledge that you have read and understood this Privacy Policy.