Privacy Policy

Resilient Roots Therapeutic Services, PLLC Originally effective: 2025 | Last updated: November 2026

Who We Are

Resilient Roots Therapeutic Services, PLLC ("Resilient Roots," "we," "us," or "our") provides outpatient therapy to clients in North Carolina, in person and through telehealth. Our website is https://resilientrootsmh.com.

Reaching out for therapy takes courage, and protecting your privacy is part of how we care for you. This Privacy Policy explains how we collect, use, share and protect information when you visit our website, contact us, or receive services from us.

Once you become a client, your health information is also protected by federal and North Carolina law, and our Notice of Privacy Practices explains those protections in full. Our Notice of Privacy Practices is available on our website and in our client portal, and we provide a copy before or at your first appointment. If anything in this Privacy Policy differs from our Notice of Privacy Practices regarding your health information, the Notice of Privacy Practices controls.

1. The Laws and Standards We Follow

We handle your information in line with:

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules (45 CFR Parts 160 and 164).
- Federal confidentiality rules for substance use disorder records (42 CFR Part 2), when we receive records from a program covered by those rules.
- North Carolina confidentiality law for mental health services (N.C. Gen. Stat. 122C-51 through 122C-56), as it applies to our practice.
- The North Carolina Identity Theft Protection Act, including its security breach notification and secure disposal requirements (N.C. Gen. Stat. 75-60 through 75-66).
- The professional ethics codes and licensing rules that govern our clinicians, including the NASW Code of Ethics, the ACA Code of Ethics, the North Carolina Social Work Certification and Licensure Board, and the North Carolina Board of Licensed Clinical Mental Health Counselors.

2. Information We Collect

Information you give us

- **When you contact us or request a free 15 minute consultation:** your name, email address, phone number, preferred way to be contacted, and a brief note about what you are looking for.
- **When you become a client:** contact and demographic details, emergency contact, insurance and payment information, health and mental health history, and information you share in sessions and in our secure client portal.
- **When you communicate with us:** the content of your emails, messages, voicemails and portal messages.

> **A gentle request:** please do not share detailed personal or clinical information through our website contact form. Save that for your consultation or our secure client portal, where it is better protected.

Information collected automatically

Like most websites, ours automatically collects limited technical information, such as your IP address, browser and device type, the pages you visit, the site that referred you, and the date and time of your visit. This is collected through cookies and similar tools used by our website host and any analytics service we use (see Section 6).

Information from others

With your permission or as allowed by law, we may receive information from referral sources, other health care providers, and your insurance company.

3. How We Use Your Information

- To respond to your inquiry and schedule your consultation.
- To provide therapy and coordinate your care (treatment).
- To bill your insurance or process your payment (payment).
- To run our practice responsibly, including clinical supervision of associate licensed clinicians, quality improvement, training, licensing, compliance and legal needs (health care operations).
- To send appointment reminders and administrative messages, using the contact methods you approve.
- To operate, secure and improve our website.
- To meet our legal and ethical obligations.

Payments. Card payments are handled by a secure, PCI compliant payment processor. We do not store your full card number on our own systems.

We do not sell your personal information. We do not use client health information for marketing or advertising, and we do not share it with advertising companies.

4. How We Share Your Information

What you share in therapy is confidential. We share information only as described here and in our Notice of Privacy Practices.

- **With your written authorization.** You may revoke an authorization in writing at any time, except for anything already shared in reliance on it.
- **For treatment, payment and health care operations,** as permitted by HIPAA and North Carolina law, using only the minimum information needed. For example, we send required information to your insurance company to process a claim.
- **With family or others you involve in your care,** if you agree or do not object, limited to what is relevant to their involvement. Adult clients choose who we may speak with.
- **With trusted service providers** who help us run the practice, such as our electronic health record and client portal, telehealth platform, billing support, and secure communication tools. Each one signs a Business Associate Agreement requiring it to protect your information.

When we may share information without your consent

North Carolina and federal law allow, and in some cases require, us to share limited information without your consent, including:

- **Imminent danger.** When your clinician believes there is an imminent danger to your health or safety or to another person, or a likelihood that a felony or violent misdemeanor will be committed, we may share information with those who need it to prevent harm (N.C. Gen. Stat. 122C-55(d)).
- **Abuse or neglect.** We must report suspected abuse, neglect or dependency of a child (N.C. Gen. Stat. 7B-301), and suspected abuse, neglect or exploitation of a disabled adult (N.C. Gen. Stat. 108A-102), to the county Department of Social Services.
- **Legal proceedings.** When we receive a valid court order or as otherwise required by law. We review any legal request carefully and will let you know when we are permitted to.
- **Medical emergencies,** to the extent needed to get you appropriate care.
- **Oversight and compliance,** such as reviews by licensing boards or the U.S. Department of Health and Human Services.
- **Other limited situations** permitted or required by law, such as public health activities, workers' compensation, or responding to law enforcement as allowed by law. Our Notice of Privacy Practices lists these in full.

Extra protections

- **Psychotherapy notes,** if your clinician keeps them, are stored separately from your record and are shared only with your specific written authorization, except in the narrow cases the law allows.
- **Substance use disorder records** we receive from programs covered by 42 CFR Part 2 will not be used or shared in any civil, criminal, administrative or legislative proceeding against you without your written consent or a court order that meets the requirements of those rules.
- **Redisclosure.** Once information is properly shared with someone outside our practice, such as another provider or your insurance company, it may no longer be protected by HIPAA in their hands.

5. Email, Text, Phone and Telehealth

Regular email and text messages are not fully secure. We encourage you to use our secure client portal for anything personal or clinical. At the start of services we will ask how you would like us to contact you, and we will respect your choices.

Text messages. If you agree to receive texts from us, such as appointment reminders, message and data rates may apply. Reply STOP at any time to opt out, or HELP for help. We do not share or sell your mobile phone number or text messaging consent with third parties or affiliates for marketing or promotional purposes. Mobile information is shared only with the service providers who help us deliver these messages.

Telehealth. We use a HIPAA compliant video platform. We ask that you join from a private space. Sessions are not recorded by anyone without the written consent of everyone involved.

Voicemail. If you leave us a voicemail, we will return your call using the contact method you have approved. Please let us know if there are numbers where we should not leave a message.

Recording and AI tools. We do not use artificial intelligence tools to record, transcribe or summarize your sessions without your knowledge and written consent. Any tool we use for this purpose is HIPAA compliant and covered by a Business Associate Agreement.

Social media and online reviews. To protect your privacy, our clinicians do not connect with current or former clients on personal social media, and we will never confirm or deny that someone is our client in response to an online review or comment. Following or interacting with our public social media pages may make that interaction visible to others.

> **Our website, email, texts and voicemail are not monitored for emergencies.** If you are in crisis or in danger, call 911, or call or text 988 to reach the Suicide and Crisis Lifeline.

6. Cookies, Analytics and Tracking

Our website host uses cookies that are needed for the site to work properly. We may also use analytics tools to understand, in general, how visitors use our site so we can improve it.

We do not use advertising pixels or similar tracking tools on our contact or consultation pages, and we do not allow tracking technologies to send your health information to third parties. Our client portal is provided by our electronic health record vendor under a Business Associate Agreement and is not part of our public website tracking.

You can block or delete cookies through your browser settings, though some parts of the site may not work as well. Our website does not currently respond to "Do Not Track" browser signals.

Our site may link to other websites, such as social media or directories. We are not responsible for their privacy practices, and we encourage you to review their policies.

7. How We Protect Your Information

We use administrative, technical and physical safeguards to protect your information, including encryption, secure systems with access controls, HIPAA training for our team, Business Associate Agreements with our vendors, and secure disposal of records as required by North Carolina law. No method of electronic storage or transmission is completely secure, but we take every reasonable step to protect your information.

8. If a Breach Occurs

If your information is ever involved in a breach, we will notify you as required by HIPAA, without unreasonable delay and no later than 60 days after we discover it, and as required by North Carolina law (N.C. Gen. Stat. 75-65). When required, we will also notify the U.S. Department of Health and Human Services and the Consumer Protection Division of the North Carolina Attorney General's Office.

9. How Long We Keep Information

Client records are kept for the length of time required by North Carolina law and our licensing boards' rules, then securely destroyed. Information from people who contact us but do not become clients is kept only as long as needed to respond and for reasonable business purposes.

10. Your Privacy Rights

As a client, you have the right to:

- See and get a copy of your health record, in paper or electronic form. We will respond within 30 days, as HIPAA requires. We may charge a reasonable, cost based fee for copies as allowed by law.
- Ask us to correct information in your record that you believe is wrong or incomplete.
- Request a list of certain disclosures we have made of your information.
- Ask us to limit how we use or share your information. If you pay for a service in full out of pocket, you can ask us not to share information about that service with your health plan, and we will agree unless the law requires otherwise.
- Ask us to contact you in a specific way or at a specific place.
- Get a paper copy of our Notice of Privacy Practices at any time.
- Choose someone to act for you, such as a legal guardian or a person with power of attorney.
- Be notified if a breach affects your information.
- File a complaint without any retaliation (see Section 12).

If you are not a client and have contacted us through our website, you may ask what information we have about you, ask us to correct it, or ask us to delete it. Please note that health records for current and former clients cannot be deleted on request, because the law requires us to keep them for a set period.

11. Minors, Families and Couples

When we provide services to a minor, parents and legal guardians generally have the right to access the minor's information, consistent with North Carolina law and limited exceptions. We talk through confidentiality with both the young person and their parent or guardian at the start of services. When we work with couples or families, we explain at the start how information shared in joint sessions is handled.

Our website is not directed to children under 13, and we do not knowingly collect personal information online from children under 13.

12. Questions or Complaints

If you have a concern about your privacy, please contact our Privacy Officer using the information below. You may also file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, at www.hhs.gov/ocr/complaints, or with the licensing board for your clinician. We will never retaliate against you for filing a complaint.

13. Changes to This Policy

We may update this Privacy Policy as laws and our practices change. The current version will always be posted on this page with its effective date. If we make a material change to our Notice of Privacy Practices, we will make the new version available to clients.

14. Contact Us

If you have questions about this policy, would like to exercise any of your rights, or need this policy in another format or language, please contact us.

Privacy Officer: Dr. Aalih Hussein, PhD, LCSW, Founder and Executive Director

Email: contact@resilientrootsmh.com

Phone: (336) 863-3558

Mail: Resilient Roots Therapeutic Services, PLLC, 31 S. Talbert Blvd #123, Lexington, NC 27292