

Privacy Policy

Last updated: October 28, 2026

1. Introduction & Scope

Lantern ABA, Inc. ("Lantern ABA," "we," "us," or "our") is a sole-practitioner Applied Behavior Analysis (ABA) practice located in California. This Privacy Policy describes how we collect, use, disclose, and protect personal information gathered through our website, our parent portal, and other general business communications with clients, prospective clients, and website visitors.

This Policy does not replace our Notice of Privacy Practices (NPP). The NPP governs how we use and disclose Protected Health Information (PHI) under HIPAA and the California Confidentiality of Medical Information Act (CMIA). Where clinical health information is concerned, the NPP and our Client Handbook & Services Agreement control.

We may update this Privacy Policy from time to time. The "Last updated" date above reflects the most recent changes. Material changes will be posted on our website. Your continued use of our website after changes are posted constitutes acceptance of the revised Policy.

2. Categories of Information We Collect

2.1 Information You Provide Directly

- Contact information: name, email address, phone number, mailing address.
- Intake and enrollment information: child's name, date of birth, emergency contacts, school information, referring provider information, insurance card details (for superbill purposes only, as described in our Client Handbook)
- Payment and billing information: billing contact details, payment method information (credit/debit card, Zelle, Venmo, check, or cash, as processed through our billing workflow).
- Correspondence: messages sent through our service inquiry form, Google Workspace business email, Google Voice for our managed Workspace account, or our secure parent portal.
- Forms and authorizations: signed consent forms, release-of-information forms, and financial agreements submitted during intake or throughout services.

2.2 Information Collected Automatically (Website)

- Device and usage information: IP address, browser type, operating system, pages viewed, time and date of visit, referring website, and general geographic location (e.g., city or region, derived from IP address).

- Cookies and similar tracking technologies (see Section 6 below).

2.3 Information Collected Through Our Clinical Systems and Parent Portal

- Login credentials and account activity for our secure parent portal and clinical systems (HiRasmus and AlohaABA).
- Session verification records, electronic signatures confirming service delivery, scheduling and billing information, clinical documentation, and communications exchanged through these systems.

2.4 Information Exchanged Through Our Communication Platforms

Lantern ABA uses Google Workspace business email, Google Voice for our managed Workspace account, and our secure parent portal to communicate with families. Depending on the channel and your communication preferences, we may collect or store the following information:

- SMS preferences and consent records: the phone number you authorize, your opt-in or withdrawal of consent, and the date and method used to document your choice.
- Scheduling requests, appointment confirmations, and calendar-related communications.
- Billing questions, invoices, and payment confirmations.
- Clinical updates, progress summaries, and treatment-related discussions, which should be exchanged through our secure parent portal or another secure method arranged with the family, rather than standard SMS.
- Attachments such as signed forms, superbills, or progress reports.

We use covered Google Workspace services subject to our Business Associate Agreement (BAA) with Google. Google Voice is used through our managed Workspace account. A BAA does not make ordinary SMS end-to-end encrypted or eliminate communication risks. See Section 7.2 for our SMS practices and your communication choices.

Clinical information such as diagnosis, treatment plans, session notes, and progress data is collected and governed separately under our Notice of Privacy Practices and is not the subject of this Policy.

3. How We Collect Information

- Directly from parents/guardians through intake forms, phone calls, email, or in-person conversation.
- Automatically through our website via cookies and similar tracking technologies.
- Through our secure clinical systems and parent portal (HiRasmus and AlohaABA).
- Through our Google Workspace business email, Google Voice, or secure parent portal when you correspond with us directly.
- From third parties such as referring physicians, schools, or other treatment providers, where authorized.

4. How We Use Information

- To respond to inquiries and provide information about our services.
- To process intake, enrollment, and billing.
- To coordinate care with other authorized providers, with consent.
- To schedule, confirm, and follow up on appointments through business email, our secure parent portal, or Google Voice SMS when you have agreed to receive texts.
- To comply with legal, regulatory, and licensing obligations, including mandated reporting requirements.
- To maintain and improve the functionality and security of our website and parent portal.
- To communicate with families regarding scheduling, billing, and general administrative matters.
- To maintain accurate business records, including correspondence retained within Google Workspace, Google Voice, and our secure parent portal for documentation purposes. We do not use personal information collected through our website for advertising or marketing purposes directed at children.

5. How We Share Information

We do not sell personal information, and we do not share personal information with third parties for their own marketing purposes.

SMS consent is not shared with third parties or affiliates. Mobile phone numbers collected for SMS are not sold or shared with third parties or affiliates for their own marketing or promotional purposes.

We may share information with the following categories of parties, only as necessary to operate our practice:

- Google Workspace: used as our business email provider for all professional correspondence, including scheduling, billing, and clinical communication. Google Workspace is covered under a signed Business Associate Agreement with Lantern ABA.
- Google Voice (managed Workspace account): used for business calls and, with your consent, standard SMS about scheduling and general administrative matters. Ordinary SMS is not a secure clinical messaging channel.
- HiRasmus: our electronic documentation and parent portal system, used to record session data, progress notes, and session verifications.
- AlohaABA: our practice-management system, used for scheduling, billing, administrative records, and other practice operations.
- Payment processors: used solely to process billing transactions (e.g., card processing, Zelle, Venmo), limited to the information necessary to complete payment.
- Other treatment providers, with your written authorization, to coordinate care.

- Legal and regulatory authorities, when required by law, court order, or mandatory reporting obligations.
- Successors, in the event of a change in business ownership or structure, subject to the same privacy commitments described here.

Each of these vendors is contractually limited to using information only to provide the applicable service to Lantern ABA and is prohibited from using it for their own independent purposes, such as advertising. A complete description of how Protected Health Information is shared, including circumstances that do not require prior authorization, is provided in our Notice of Privacy Practices.

6. Cookies & Tracking Technologies

Our website may use the following types of cookies and similar technologies:

- Essential/functional cookies: required for basic website operation.
- Analytics cookies: help us understand how visitors use our website (e.g., aggregated, non-identifying usage statistics).

We do not use cookies for third-party advertising or behavioral ad targeting. Most web browsers allow you to control cookies through browser settings, including blocking or deleting cookies. Because there is not yet a uniform standard for how businesses should respond to "Do Not Track" browser signals, our website does not currently respond differently to such signals. You may still manage cookie preferences directly through your browser.

7. Data Security

7.1 General Safeguards

We take reasonable administrative, technical, and physical measures designed to protect personal information against unauthorized access, use, or disclosure, including:

- Use of HIPAA-compliant, encrypted platforms for clinical and sensitive communications.
- Restricted access to personal and clinical information, limited to those with a legitimate need.
- Secure, access-controlled storage of records, whether physical or electronic.
- Confidentiality obligations for anyone assisting in the operation of the practice.
- Regular review of our data-handling practices as our practice and technology evolve.

7.2 Communication Platforms & SMS Consent

We select communication channels based on the sensitivity of the information and the family's documented preferences. Our secure parent portal or another arranged secure method should be used for detailed clinical discussions. Our email and SMS practices are described below:

- Google Workspace (business email): Used for professional correspondence with families. Covered services are subject to our Business Associate Agreement (BAA) with Google. Families may request a secure alternative for sensitive information.
- Google Voice (managed Workspace account): Used for business calls and optional standard SMS about scheduling and general administrative matters. We ask families to use our secure parent portal or another arranged secure method for diagnoses, treatment details, behavior descriptions, progress reports, and other sensitive clinical information.

Standard SMS text messaging is not end-to-end encrypted and carries a risk of interception, misdelivery, or access by others who can use your device, account, or message previews. Even a client name or appointment message may reveal a relationship with a health care practice. Using Google Voice through Workspace does not remove these risks.

Before sending SMS, we ask the parent or legal guardian to acknowledge these risks and affirmatively request or permit text communication at a specified number. This choice is documented separately in a communication consent form or equivalent recorded opt-in; reading this Privacy Policy alone does not constitute SMS consent. SMS is optional, and declining it does not affect eligibility for services. You may withdraw SMS consent by replying STOP or contacting ethan@lanternaba.com, and request another communication method. Message frequency varies, and message and data rates may apply. SMS is not monitored continuously and must not be used for emergencies.

7.3 Limitations

No method of electronic transmission or storage is completely secure, even with vendor-level safeguards and signed Business Associate Agreements in place. While we work diligently to protect personal information using the measures described above, we cannot guarantee absolute security, and we encourage families to also take reasonable precautions, such as keeping portal login credentials confidential and avoiding transmission of sensitive information through unsecured channels.

8. Data Retention & Destruction

Clinical records are retained for a minimum of seven (7) years from the date of last service, or, for clients who are minors, for at least seven (7) years after the client turns 18, consistent with our Notice of Privacy Practices. General business and website-related information (such as contact form submissions or website analytics data) is retained only as long as reasonably necessary for the purposes described in this Policy, after which it is securely deleted or destroyed.

9. Your Privacy Rights

9.1 HIPAA / CMIA Rights (Clinical Information)

As described more fully in our Notice of Privacy Practices, you have the right to request access to, and correction of, your child's health records, request restrictions on certain uses or disclosures, receive an accounting of certain disclosures, and file a complaint if you believe your privacy rights have been violated.

9.2 California Consumer Privacy Rights (General Personal Information)

To the extent the California Consumer Privacy Act (CCPA), as amended, applies to personal information we collect outside of HIPAA-protected health information (for example, website or general contact information), you have the right to:

- Know what personal information we have collected, used, or disclosed about you.
- Request deletion of personal information we have collected, subject to certain legal exceptions.
- Correct inaccurate personal information.
- Opt out of the sale or sharing of personal information — we note that we do not sell or share personal information as defined under the CCPA.
- Not be discriminated against for exercising any of these rights.

To exercise any of these rights, please submit a written request using the contact information in Section 13 below. To help protect your information, we may need to verify your identity or your authority to act on a client's behalf before fulfilling certain requests. We will acknowledge your request and respond within the timeframe required by applicable law. If we are unable to fulfill a request in whole or in part (for example, because information is subject to a legal retention requirement or is part of a HIPAA-protected clinical record governed by our Notice of Privacy Practices instead), we will explain the applicable basis in our response.

We will not discriminate against you for exercising any of these rights, including by denying services, charging different rates, or providing a different level of service, except as otherwise permitted by law.

10. Children's Privacy

Our services are provided to children and adolescents exclusively through the consent, involvement, and account access of a parent or legal guardian. Our website is directed at parents, guardians, and other adults seeking information about our services, and is not directed at soliciting information directly from children.

Where a minor client interacts with the parent portal, access and account credentials are managed and controlled by the parent or legal guardian. We do not knowingly collect personal information directly from children through our website without parental involvement.

11. Third-Party Links

Our website may contain links to third-party websites, such as insurance provider portals or telehealth platforms. We are not responsible for the privacy practices or content of those third-party sites. We encourage you to review the privacy policy of any third-party website you visit.

12. Changes to This Policy

We may revise this Privacy Policy periodically to reflect changes in our practices, technology, or legal requirements. The "Last updated" date at the top of this Policy indicates when it was last updated. We encourage you to review this Policy periodically.

13. Contact Us

If you have questions about this Privacy Policy, wish to exercise a privacy right described above, or have a concern about how your personal information is handled, please contact:

- Ethan Lin, M.Ed., BCBA — Owner, Lantern ABA, Inc.
- Email: ethan@lanternaba.com For concerns specifically involving Protected Health Information under HIPAA, you may also contact the U.S. Department of Health and Human Services Office for Civil Rights at www.hhs.gov/ocr.

This Privacy Policy is provided for general informational purposes and does not constitute legal advice. Lantern ABA, Inc. encourages review by qualified legal counsel to ensure compliance with all applicable federal and state requirements.